LIVRE BLANC

Un DNS conçu pour garantir une disponibilité optimale et une résilience maximale face aux attaques DDoS

Introduction

Edge DNS fournit aux entreprises un service DNS fiable pour connecter les utilisateurs finaux à leurs sites Web et à leurs autres applications. Si les entreprises concentrent toute leur attention sur les performances, c'est bien souvent au détriment de la disponibilité et de la résilience du DNS, notamment face aux attaques DDoS visant à perturber le service et empêcher la connexion des utilisateurs finaux. Akamai a conçu Edge DNS de façon à garantir la disponibilité même pendant les attaques DDoS les plus virulentes, grâce à une envergure mondiale inégalée, une architecture IP Anycast segmentée et de nombreux contrôles DDoS, notamment la possibilité d'exploiter d'autres services Akamai si nécessaire. Proposé en tant que service DNS géré, Edge DNS offre une combinaison optimale de performances et de disponibilité pour que les entreprises restent toujours connectées à leurs utilisateurs finaux.

Remarque sur les statistiques

Initialement, Akamai a créé Edge DNS dans le but de fournir des services DNS fiables pour promouvoir ses solutions de réseau de diffusion de contenu (CDN) mondial. Au fil des années, Akamai a tiré de nombreuses leçons quant aux meilleures méthodes pour assurer l'évolutivité et maintenir la disponibilité d'une infrastructure DNS aussi importante. Les statistiques globales présentées à droite donnent une idée générale de l'ampleur de la plateforme. Toutefois, les statistiques à elles seules ne suffisent pas pour renseigner précisément sur la disponibilité et la résilience. Elles doivent être rapprochées de l'architecture de plateforme, des capacités spécifiques d'atténuation des attaques DDoS et de la capacité globale mise à disposition d'Akamai pour protéger la plateforme contre les attaques.

Statistiques relatives à la plateforme

- Des milliers de serveurs de noms
- Plus de 1 000 points de présence
- Plus de 140 villes
- Plus de 40 pays

Notez que, pour des raisons de sécurité, Akamai ne divulgue pas de détails spécifiques au sujet du nombre de serveurs de noms ou du nombre, des emplacements ou de la taille de nos points de présence. Cette politique protège à la fois Akamai et nos clients des pirates qui pourraient tenter d'utiliser ces informations pour planifier des attaques.

Architecture

Comme le montrent les statistiques ci-dessus, la portée de Edge DNS est bien plus importante que celle de la plupart des autres services DNS fiables actuellement disponibles sur le marché. Toutefois, les statistiques globales relatives au nombre de serveurs et de points de présence ou à la capacité réseau totale sont insuffisantes pour comprendre le niveau de disponibilité et de résilience d'une plateforme mondiale. Contrairement à d'autres solutions DNS qui sont traditionnellement axées sur les performances à l'exclusion de tout le reste, Akamai a spécifiquement conçu Edge DNS dans un souci de disponibilité et de résilience contre les attaques DDoS, outre les performances, avec des redondances architecturales à plusieurs niveaux, y compris les serveurs de noms, les points de présence, les réseaux et même les clouds IP Anycast segmentés.

IP Anycast

Edge DNS comprend des milliers de serveurs de noms déployés dans plus de 1 000 points de présence utilisant un modèle IP Anycast pour répondre aux requêtes DNS. IP Anycast dirige les requêtes des utilisateurs finaux vers le point de présence le plus proche pour qu'elles soient résolues. Outre des performances plus rapides, IP Anycast offre plusieurs avantages fondamentaux en matière de disponibilité et de résilience, ce qui explique que la plupart des services DNS fiables l'utilisent :

- **Disponibilité** : IP Anycast permet aux serveurs de noms à différents emplacements du réseau de répondre aux requêtes dirigées vers une seule adresse IP. Grâce à IP Anycast, Edge DNS fournit non seulement aux entreprises une résolution DNS dans plusieurs centres de données, mais améliore également la disponibilité en répartissant la charge à l'échelle mondiale. En outre, des serveurs physiques individuels ou des points de présence entiers peuvent être hors ligne sans pour autant que cela n'affecte la capacité globale de résolution d'un domaine.

- **Portée** : comprenant de nombreux serveurs physiques sur de nombreux points de présence, l'infrastructure Edge DNS fournit aux entreprises d'importantes ressources informatiques sur lesquelles elles peuvent compter pour répondre à un volume important de requêtes DNS. Edge DNS a également accès à une capacité réseau supplémentaire significative dans de nombreux points de présence, car il partage souvent de la capacité avec d'autres services Akamai. Cela confère à Edge DNS une portée bien plus vaste pour répondre aux attaques DNS par inondation et aux autres formes d'attaques DDoS, comparé à un service DNS autonome.

- **Répartition** : en plus d'augmenter la portée, IP Anycast permet à Edge DNS de répartir le trafic sur plusieurs points de présence et divers emplacements réseau. Examiner attentivement les emplacements géographiques et les déploiements réseau pour ces points de présence peut aider à limiter l'impact d'attaques plus petites sur des zones géographiques ou des réseaux spécifiques, et contribuer à préserver la disponibilité des systèmes clients dans d'autres zones.

Akamai n'est pas seul à tirer parti d'IP Anycast. En permettant à plusieurs serveurs de noms de résoudre les requêtes DNS des utilisateurs finaux, IP Anycast améliore la disponibilité de la résolution de noms pour tous les services DNS. Mais même avec IP Anycast, la résilience reste limitée par la portée totale d'une plateforme, et des attaques DDoS de grande envergure peuvent encore submerger une plateforme basée sur le cloud. De plus, sans architecture diversifiée, même de plus petites attaques peuvent potentiellement anéantir l'organisation des services DNS dans des régions géographiques spécifiques, en les rendant indisponibles pour un grand nombre d'utilisateurs finaux, voire en influant négativement sur la disponibilité de sites Web auxquels ces utilisateurs se connectent.

Clouds Edge DNS

Pour optimiser davantage leur résilience en cas d'attaque, Edge DNS segmente ses serveurs de noms et ses points de présence entre plusieurs clouds IP Anycast. Un cloud Edge DNS se compose de points de présence et de serveurs de noms dédiés, associés à une capacité et une connectivité réseau. Chaque cloud fonctionne indépendamment des autres, et Edge DNS peut être équivalent à plusieurs fournisseurs DNS autonomes en termes de disponibilité, de portée et de répartition.

Les clouds IP Anycast Edge DNS représentent un ensemble diversifié d'architectures. Bien que deux clouds ne soient jamais identiques, ils respectent tous dans une large mesure deux principes de conception : performances et disponibilité.

- **Performances** : un cloud hautes performances peut avoir plus de 100 points de présence répartis dans le monde entier, chacun étant constitué d'un ensemble de serveurs de noms. Comme le montre la figure 1, un cloud hautes performances déploie de petits clusters de serveurs de noms dans de nombreux endroits proches des utilisateurs finaux et des fournisseurs d'accès Internet (FAI) locaux afin de minimiser les temps de recherche et d'améliorer les performances brutes. En contrepartie, les petits points de présence offrent moins de résilience face aux attaques DDoS par définition, car leurs ressources de calcul et leur capacité réseau sont moindres.
- **Disponibilité** : Edge DNS gère de nombreux clouds de disponibilité. Comme le montre la figure 1, les clouds de disponibilité ont moins de points de présence, mais incluent une ou plusieurs régions d'ancrage pouvant compter des centaines de serveurs de noms dans un centre de données centralisé avec une large capacité réseau dédiée et une excellente connectivité via plusieurs réseaux. La région d'ancrage fournit au cloud de disponibilité la portée nécessaire pour répondre aux pics importants de requêtes DNS et à d'autres parties du trafic réseau. Les clouds de disponibilité multiplient les régions d'ancrage avec quelques petits points de présence afin de maintenir un niveau de performances acceptable pour les utilisateurs du monde entier.

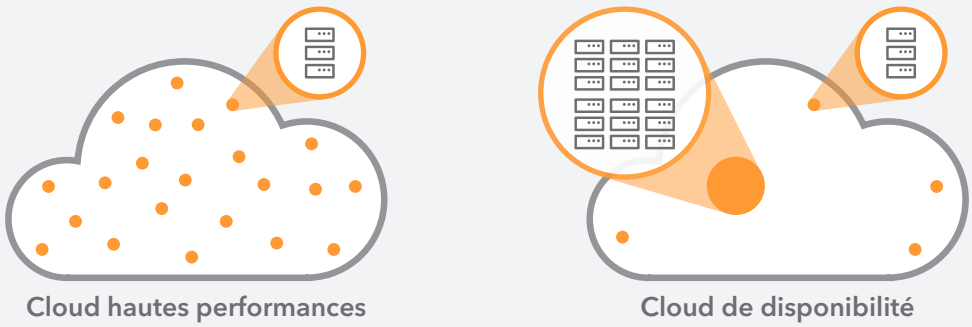

Figure 1 : Edge DNS combine plusieurs clouds DNS avec différentes architectures pour offrir une combinaison optimale de performances, de disponibilité et de résilience contre les attaques DDoS.

Architecture segmentée

Edge DNS offre un degré de disponibilité fondamentalement différent de celui des autres fournisseurs qui exploitent des services DNS fiables sur un seul et unique cloud IP Anycast. Pour tous les fournisseurs, IP Anycast offre un avantage certain en matière de disponibilité : grâce à lui, le service peut rester globalement disponible lorsqu'il est confronté à de petites attaques susceptibles de n'affecter que des zones géographiques spécifiques, et non l'ensemble de la plateforme. Cependant, même les pannes localisées auront un impact sur les utilisateurs finaux des zones géographiques affectées ainsi que sur les entreprises qui comptent sur ce service pour établir ou maintenir une connexion avec ces utilisateurs. En outre, les attaques DDoS de grande envergure combinées au trafic généré par les attaques de systèmes à travers le monde peuvent potentiellement provoquer une panne de toute la plateforme.

Grâce à des clouds IP Anycast nombreux et divers, Edge DNS peut continuer à fonctionner même après avoir perdu un ou plusieurs clouds. Cette solution offre une disponibilité et une résilience accrues contre les attaques DDoS par comparaison à une architecture de cloud unique. En outre,

l'exploitation de plusieurs clouds IP Anycast offre l'avantage de segmenter le trafic entre des sous-sections de la plateforme globale, afin de réduire l'impact des attaques DDoS, même lorsque celles-ci sont massives. Par exemple, une attaque ciblant un seul cloud IP Anycast Edge DNS sera dirigée vers les points de présence et les serveurs de noms physiques qui composent ce cloud spécifique. L'architecture segmentée isole l'impact pour épargner les autres clouds IP Anycast. Edge DNS peut ainsi préserver la disponibilité de la plateforme dans toutes les zones géographiques, même si certains clients ou clouds subissent une attaque DDoS.

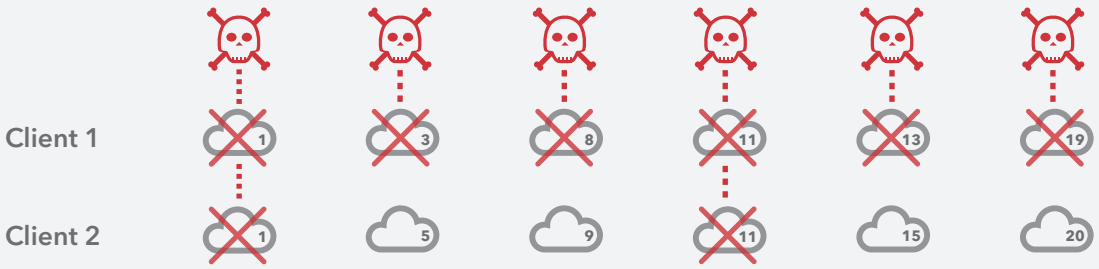

Figure 2 : chaque client Edge DNS reçoit des serveurs de noms avec une combinaison unique de clouds de performances et de disponibilité, ce qui réduit les dommages collatéraux causés par une attaque lancée contre d'autres clients.

Non seulement l'architecture segmentée Edge DNS accroît la résilience globale de la plateforme, mais elle réduit également le risque de dommages collatéraux infligés à des clients individuels en cas d'attaque de serveurs de noms utilisés par d'autres clients. Edge DNS attribue à chaque client plusieurs clouds Edge DNS, et cela dans une combinaison unique de clouds de performances et de disponibilité non partagée par un autre client. Comme le montre la figure 2, cette répartition réduit le chevauchement des serveurs de noms et des clouds IP Anycast entre deux clients. Cela garantit également que chaque client dispose de serveurs de noms disponibles même lorsque des clouds IP Anycast attribués à un autre client sont spécifiquement ciblés par une attaque DDoS de grande envergure.

Gestion des délégations de clients

Il arrive souvent qu'une même organisation soit visée par plusieurs attaques DDoS sur des périodes prolongées. Akamai a d'ailleurs déjà fait face à de vastes campagnes d'attaques qui se sont étendues sur plusieurs mois, voire encore plus longtemps. En pareil cas, l'architecture segmentée de Edge DNS offre à Akamai une plus grande flexibilité pour minimiser au mieux l'impact sur les clients non ciblés par l'attaque. Comme le montre la figure 3, Akamai peut réaffecter les clouds d'un client spécifique et isoler davantage les conséquences d'une attaque, si nécessaire.

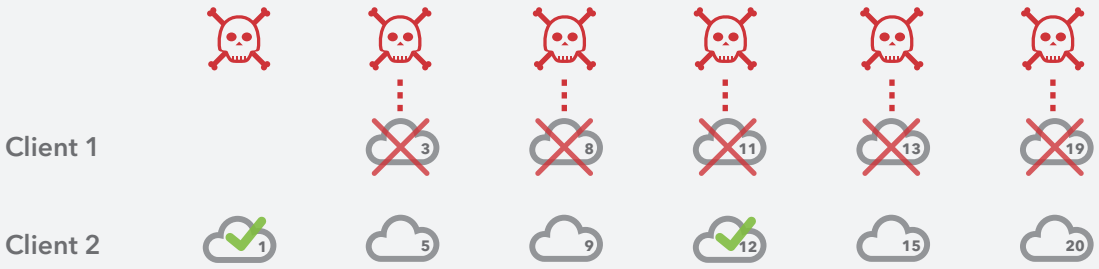

Figure 3 : Akamai peut gérer des délégations de serveurs de noms afin de minimiser davantage l'impact d'une attaque (comparativement à la figure 2 ci-dessus), par exemple en déplaçant un client ciblé hors d'un cloud individuel et en réduisant le chevauchement pour les clients non ciblés.

Par exemple, Akamai peut :

- **Déplacer un client ciblé hors d'un cloud spécifique** : chaque client Edge DNS partage des clouds IP Anycast avec d'autres clients. Par conséquent, une attaque visant tous les clouds Edge DNS d'un client particulier peut avoir des répercussions sur la disponibilité des clouds qui sont également affectés à d'autres clients. Dans des conditions normales, les programmes de résolution récursifs passent automatiquement à des clouds plus performants. Mais quand il s'agit de campagnes qui durent dans le temps, Akamai peut réattribuer les clouds IP Anycast du client ciblé de façon à rétablir la disponibilité pour les clients non ciblés.
- **Minimiser le chevauchement pour les clients non ciblés** : il arrive que plusieurs clients Edge DNS partagent plus de clouds Edge DNS que la normale. Dans ce cas, il est possible qu'une attaque massive contre un seul client induise des baisses de conséquences mesurables pour d'autres clients, bien que le service global reste disponible. Lorsque cela est nécessaire, Akamai peut réaffecter les clouds au profit des clients non ciblés afin de réduire ou d'éliminer le chevauchement avec le client ciblé et de restaurer les performances pour les utilisateurs finaux.

Diversification des déploiements de serveurs

Au sein de chaque cloud Anycast, Akamai déploie des serveurs de noms physiques dans différents emplacements conçus pour accroître la résilience globale de ce cloud. Divers emplacements de cloud Edge DNS apportent une couche supplémentaire de segmentation du trafic entre différents réseaux afin d'optimiser la disponibilité dans différentes circonstances. Par exemple :

- **Dans des centres de données dotés de plusieurs réseaux** : en matière de résilience contre les attaques DDoS, la diversité de la connectivité réseau peut être aussi importante que la capacité. Les attaques DDoS de grande envergure peuvent submerger les FAI en amont et d'autres réseaux avant d'atteindre un centre de données, entraînant ainsi une congestion du réseau et des pannes de service, même si le centre de données lui-même n'est pas affecté. Pour préserver la disponibilité et sa capacité à répondre aux requêtes DNS des utilisateurs finaux pendant des attaques, Edge DNS déploie des serveurs de noms dans de gros centres de données, avec non seulement de grandes capacités, mais également une connectivité via plusieurs réseaux.
- **Isolation des FAI** : dans de nombreux cas, Edge DNS déploie des clusters de serveurs de noms directement sur les réseaux des différents FAI. Souvent, ces serveurs de noms ne diffusent leur trafic IP Anycast qu'au sein de ces réseaux et ne résolvent les requêtes DNS que pour les utilisateurs finaux de ces FAI. Bien que cette disposition limite le nombre d'utilisateurs finaux qu'un cluster spécifique de serveurs de noms peut servir, elle préserve également la disponibilité pour ces utilisateurs lorsqu'un cloud IP Anycast est ciblé par une attaque externe à ce FAI. Pour pouvoir voir ces serveurs de noms, un pirate devra disposer de systèmes sur le réseau de ce FAI en question et, même lorsque cela est le cas, la capacité disponible suffit généralement à protéger ce cloud.
- **Diversité réseau** : les clients sont intentionnellement affectés à des clouds variés. Certains avec des emplacements de serveurs propres à des FAI spécifiques, d'autres avec un éventail plus large de machines de connexion. Cette architecture garantit que les serveurs de noms récursifs d'un client donné pourront toujours se connecter à un cloud Edge DNS disponible.

- **Dans des centres de données partagés avec d'autres services d'Akamai** : gérant de nombreux services au-delà d'un DNS fiable, Akamai peut déployer des serveurs de noms Edge DNS dans des centres de données prenant en charge plusieurs services. Comme l'explique plus en détail le paragraphe ci-dessous, cela permet à Edge DNS d'acquérir une capacité réseau supérieure en cas d'attaques DDoS d'envergure, aussi bien en matière de capacité réseau dédiée que pour les accords de peering publics déjà mis en place par Akamai pour d'autres services.

Contrôles DDoS

Au-delà de sa conception architecturale, Edge DNS inclut plusieurs contrôles pour aider à atténuer l'impact d'une catégorie d'attaques DDoS communément appelées « inondations DNS ». Bien que nombre d'attaques DDoS utilisent une grande quantité de trafic pour submerger les liaisons réseau, les inondations DNS génèrent de gros volumes de requêtes DNS légitimes pour consommer des ressources de traitement et de mémoire sur les serveurs de noms physiques, les empêchant ainsi de répondre aux requêtes des véritables utilisateurs finaux. Pour protéger la plateforme Edge DNS contre les inondations DNS, Akamai a recours à plusieurs méthodes :

- **Portée** : la portée du service DNS fiable d'Akamai peut être plusieurs fois supérieure à celle d'autres solutions DNS concurrentes. Edge DNS utilise des milliers de serveurs de noms déployés dans plus de 1 000 points de présence à travers le monde. Bien qu'il ne s'agisse pas spécifiquement d'un contrôle DDoS, IP Anycast répartit le trafic d'attaques sur l'ensemble des zones géographiques et des réseaux, tandis que le nombre de serveurs de noms physiques fournit à Edge DNS suffisamment de ressources de traitement et de mémoire pour absorber les pics importants de requêtes DNS.

- **Limitation du débit** : grâce à ses fonctionnalités de limitation du débit, Edge DNS peut automatiquement faire baisser le nombre de requêtes provenant de certaines adresses IP lorsque le volume de requêtes dépasse un seuil défini. Cette limitation du débit empêche les pics importants de requêtes DNS de consommer des ressources de traitement et de mémoire sur les serveurs de noms physiques, et peut être utile pour réagir aux attaques qui génèrent un volume élevé de requêtes, mais consomment relativement peu de bande passante. Notez que les fonctionnalités de limitation du débit sur Edge DNS ne peuvent pas être configurées par les clients. En revanche, elles peuvent être utilisées par des algorithmes propres à la plateforme Edge DNS.

- **Liste blanche DNS** : en raison de sa position sur Internet, Akamai dispose d'une visibilité unique sur le comportement des programmes de résolution récursifs qui sont responsables d'environ 95 % des recherches DNS légitimes sur Internet. Si nécessaire lorsque la charge est élevée, Edge DNS peut utiliser un modèle de sécurité positif et limiter les requêtes DNS à une liste de programmes de résolution DNS réputés.

À propos de la capacité

Bien que des contrôles DDoS puissent être utiles pour atténuer l'impact des inondations DNS, d'autres types d'attaques DDoS au niveau de la couche réseau nécessitent une capacité réseau disponible suffisante pour absorber la forte densité du trafic. Le risque d'attaques de très grande envergure a considérablement augmenté au cours des dernières années. Les attaques les plus importantes connues à ce jour dépassent même largement la barre de 1 Tbit/s en pic de bande passante.

Akamai ne divulgue pas la capacité de la plateforme Edge DNS afin d'éviter d'offrir aux pirates une cible quantifiable. Cependant, Akamai investit en permanence dans tous les aspects relatifs à la portée de la plateforme, en augmentant l'infrastructure Edge DNS de façon à suivre le rythme de l'arrivée de nouveaux clients et de la croissance du trafic sur Internet. En tant que fournisseur de services cloud, Akamai peut rapidement réutiliser des serveurs et déployer la capacité DNS dans de nouvelles régions. Akamai entretient une capacité disponible importante pour absorber les gros pics de trafic, le trafic normal sur la plateforme Edge DNS consommant moins de 1 % de sa capacité globale. Si nécessaire, Edge DNS peut également mettre à profit des ressources d'autres plateformes Akamai pour atténuer les attaques DDoS.

Exploitation d'autres plateformes Akamai

La méthode traditionnelle qui consiste à utiliser la capacité réseau pour estimer la capacité de résistance face à une attaque DDoS à large bande passante ne fonctionne pas avec Edge DNS, principalement parce que Edge DNS peut exploiter des ressources d'autres plateformes Akamai. Gérant de nombreux services en plus d'Edge DNS, Akamai n'est pas qu'une simple entreprise DNS. Parmi tous les services gérés par Akamai, un DNS fiable est essentiel au fonctionnement des autres services, mais il reste mineur pour ce qui est du trafic global. Cela offre plusieurs possibilités pour augmenter la capacité disponible pour Edge DNS en cas de nécessité :

- **Capacité d'emprunt au CDN** : dans de nombreux cas, Edge DNS déploie des serveurs de noms au sein des mêmes points de présence que les serveurs appartenant à d'autres services Akamai s'exécutant sur le CDN d'Akamai. Ces points de présence sont souvent beaucoup plus importants, puisqu'ils sont conçus pour prendre en charge des services qui consomment beaucoup plus de bande passante. Cela offre également à Akamai la flexibilité opérationnelle nécessaire pour emprunter de la capacité au CDN en cas de besoin, en détournant d'autres services via d'autres points de présence d'Akamai et en rendant une capacité réseau partagée disponible exclusivement pour Edge DNS de manière à pouvoir absorber les attaques DDoS de grande envergure.
- **Déploiement d'une capacité d'atténuation dédiée** : outre le CDN et le DNS fiable, Akamai utilise un service de protection DDoS distinct, doté de capacités et de fonctionnalités d'atténuation dédiées. Lorsqu'il convient d'atténuer des attaques DDoS de grande envergure, Akamai peut affecter des délégations de serveurs de noms individuels par l'intermédiaire de ses centres de nettoyage Prolexic afin d'exploiter cette capacité dédiée et les outils d'atténuation d'attaques DDoS. Cela déploie efficacement les fonctionnalités d'atténuation d'attaques DDoS de la plateforme Prolexic devant Edge DNS, préservant ainsi les ressources Edge DNS pour répondre aux requêtes légitimes des utilisateurs finaux.

Plusieurs fournisseurs DNS

Edge DNS offre un service DNS fiable avec une portée plusieurs fois supérieure à celle de nombreux services concurrents, une architecture résiliente dotée de nombreux clouds IP Anycast segmentés, ainsi que la possibilité d'exploiter la capacité et des fonctionnalités supplémentaires d'autres services Akamai pour offrir une protection face aux attaques DDoS. Grâce à ces avantages, Edge DNS peut fournir la disponibilité et la résilience nécessaires pour agir en tant qu'unique fournisseur DNS fiable d'une organisation. Certaines organisations peuvent néanmoins choisir de déployer Edge DNS en plus de leur solution existante. Un déploiement multi-fournisseur permet aux organisations de maintenir leurs pratiques de gestion d'enregistrements DNS existantes tout en renforçant leur solution DNS principale grâce à la disponibilité et la redondance supplémentaires offertes par Edge DNS.

Options de déploiement

Edge DNS prend en charge plusieurs options pour déployer Edge DNS dans un environnement multi-fournisseur :

- **Secondaire traditionnel** : les organisations qui disposent d'un fournisseur DNS existant peuvent déployer Edge DNS en tant que service secondaire pour renforcer leur solution DNS principale. Les organisations continuent de gérer leurs enregistrements DNS avec leur fournisseur principal et utilisent des transferts de zone ou des API Edge DNS pour mettre automatiquement à jour Edge DNS. Les solutions principale comme secondaire peuvent répondre aux requêtes des utilisateurs finaux, offrant ainsi une disponibilité supplémentaire.
- **Maître masqué** : Akamai recommande cette option de déploiement aux entreprises qui souhaitent continuer à gérer les enregistrements DNS au moyen d'une solution DNS interne. L'option « maître masqué » permet à Edge DNS (en tant que seul fournisseur DNS secondaire ou parmi plusieurs fournisseurs) de répondre aux requêtes des utilisateurs finaux sans risquer d'exposer la solution interne à des attaques DDoS. Les organisations continuent de gérer leurs enregistrements DNS avec leur fournisseur principal et utilisent des transferts de zone ou des API Edge DNS pour mettre automatiquement à jour Edge DNS.
- **Principal double** : variante du concept « maître masqué ». Certains fournisseurs de services cloud n'adhèrent plus à la fonctionnalité de transfert de zone traditionnelle et exigent que les clients utilisent leurs API ou d'autres interfaces utilisateur pour les modifications d'enregistrement de zone. Edge DNS peut également être exploité de cette façon, en le configurant en mode principal et en s'assurant que les clouds Edge DNS soient ajoutés et reconnus comme fiables.

Maintien de la disponibilité en tant que solution secondaire

Lorsqu'il est déployé en tant que solution DNS secondaire, Edge DNS s'appuie sur la solution DNS principale pour être informé au sujet des zones, afin de s'assurer de répondre correctement aux requêtes des utilisateurs finaux. En général, les fichiers de zones restent valides sur une solution DNS secondaire pendant une durée de vie déterminée par le champ d'expiration dans l'enregistrement SOA. Une attaque DDoS qui provoque une panne de la solution principale peut aussi empêcher la solution secondaire de répondre aux requêtes lorsque la durée de la panne dépasse la valeur de durée de vie. Edge DNS écarte ce scénario en (1) conservant le fichier de zone même après l'expiration de la durée de vie et en (2) continuant à répondre aux requêtes DNS tant que le registre DNS les dirige vers Edge DNS. Cela permet de fournir une disponibilité supplémentaire en tant que solution DNS secondaire, même lorsque la solution principale n'est pas disponible.

Conclusion

L'attaque DDoS la plus virulente connue à ce jour a dépassé 1 Tbit/s en pic de bande passante. À cette échelle, le calcul de la bande passante totale disponible pour un service basé sur le cloud ne fournit plus d'indication précise quant à sa résilience face à des attaques de ce genre, et même les attaques plus petites peuvent provoquer des pannes au niveau régional. Edge DNS utilise une approche multi-couche pour fournir 100 % de disponibilité aux clients. Pour ce faire, il combine les atouts suivants :

- Une grande portée grâce à une empreinte mondiale, notamment des serveurs de noms et des points de présence plusieurs fois supérieurs à ceux de nombreux services concurrents
- Une immense portée grâce à une empreinte mondiale, notamment des serveurs de noms et des points de présence plusieurs fois supérieurs à ceux de nombreux services concurrents
- Une réponse encadrée face aux attaques DDoS avec, entre autres, la possibilité de déployer des contrôles DDoS ou de réaffecter des délégations de clients si nécessaire
- La possibilité d'exploiter d'autres services Akamai, notamment le CDN d'Akamai et la protection Prolexic contre les attaques DDoS, pour augmenter sa capacité et résister aux attaques DDoS de toute envergure

Un DNS fiable est un service essentiel qui établit et maintient le contact entre les utilisateurs finaux aux quatre coins du monde et la présence en ligne des organisations. Qu'il soit déployé en tant que seul fournisseur DNS fiable ou aux côtés d'une solution DNS existante, Edge DNS offre aux organisations la disponibilité dont elles ont besoin pour maintenir l'accès mondial à leur site Web et à d'autres applications Internet.