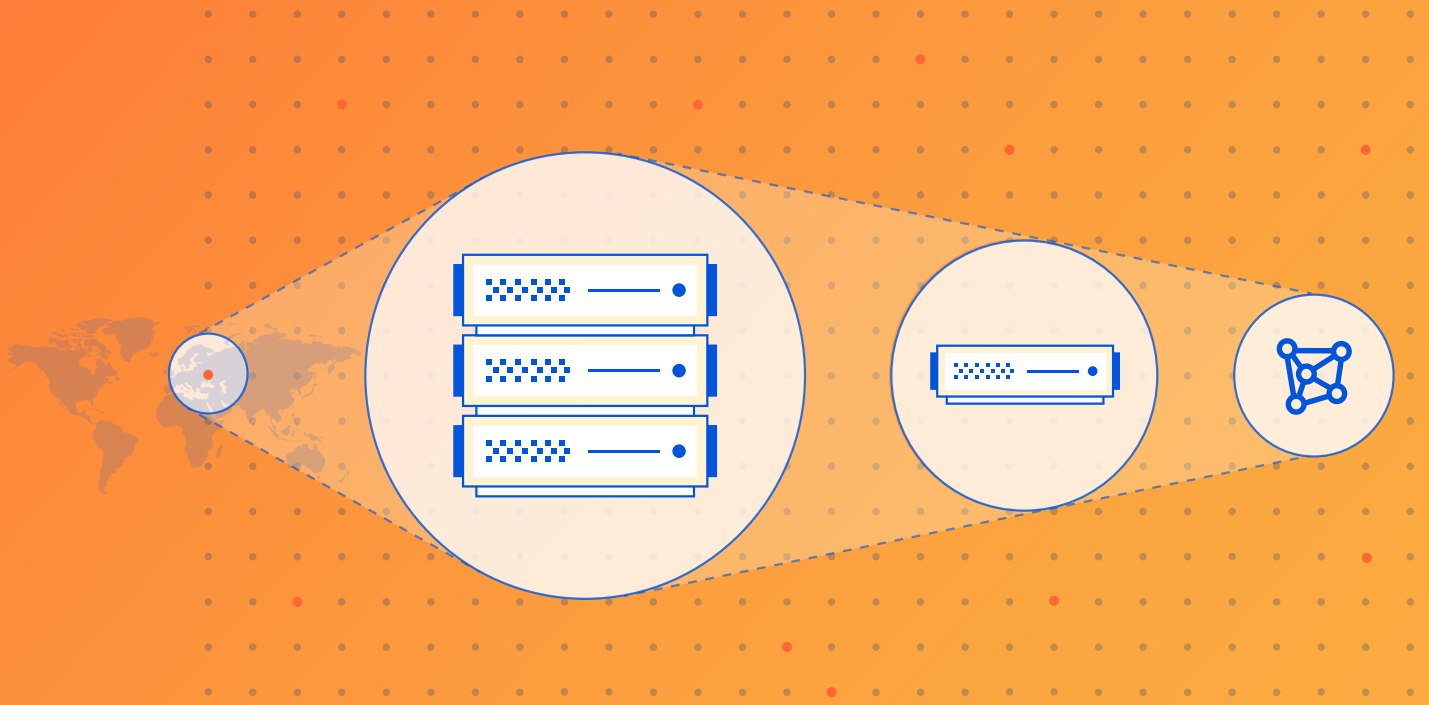
CLOUDFLARE

LIVRE BLANC

Les DNS et la menace des attaques DDoS



Contenu

Synthèse

Le DNS (Domain Name System) est l'une des principales innovations qui ont rendu l'Internet possible. Aujourd'hui, toutefois, d'immenses réseaux de zombies sont utilisés pour lancer des cyberattaques toujours plus vastes qui utilisent, et ciblent, l'infrastructure DNS.

Ces dernières années, les acteurs malveillants sont parvenus à provoquer des défaillances de services essentiels et d'immenses pans de l'Internet en lançant de vastes attaques par déni de service distribué (DDoS) contre les DNS. Un grand nombre de sites et d'organisations réputés ont ainsi été victimes d'interruptions de service et de pannes. Les solutions matérielles traditionnelles d'atténuation des attaques DDoS, qui recourent à des « scrubbing centers » (ou centres de nettoyage de données) pour éliminer le trafic malveillant, ne peuvent pas s'étendre suffisamment pour remporter la course aux armements contre des botnets distribués et fondamentalement gratuits.

Cloudflare considère que l'architecture est primordiale et qu'un réseau massivement distribué, associé à une approche sécurisée de la résolution DNS, est l'unique solution pour lutter contre les botnets massivement distribués. Cloudflare a fondé son service sur cette approche architecturale.

Les attaques de grande ampleur, toujours plus nombreuses, représentent un nouveau degré de menace pour les DNS

Le 21 octobre 2016, une attaque par déni de service distribué (DDoS), immense et soutenue, a affecté de vastes pans d'Internet, interrompant ou mettant hors service des dizaines de sites web et de services réputés. La cible directe de l'attaque était Dyn, un fournisseur de services DNS qui établit une correspondance entre les noms de domaine et leurs adresses IP (protocole Internet), afin de permettre l'acheminement du trafic vers un site spécifique. L'atténuation de l'attaque a demandé des heures.[1]

Toutefois, cet incident n'était que le début d'une vague croissante d'attaques DDoS de très grande ampleur. Dans les années qui ont suivi, les attaques ont gagné en ampleur et en portée, aboutissant à certaines des plus vastes cyberattaques jamais enregistrées. AWS a déclaré avoir atténué une immense attaque DDoS en février 2020. À l'apogée de l'attaque, le trafic entrant a atteint un débit de 2,3 térabits par seconde (Tb/s).[2] Et en juin 2022, Cloudflare a atténué une attaque de 26 millions de requêtes par seconde – la plus vaste attaque DDoS HTTPS jamais observée à l'époque.[3]

Comment les acteurs malveillants parviennent-ils à déployer des attaques d'une telle ampleur ?

D'immenses botnets basés sur l'IdO et sur des serveurs

L'une des principales tactiques utilisées pour lancer des attaques de grande ampleur consiste à prendre le contrôle d'appareils IdO (c'est-à-dire connectés à l'Internet des Objets) mal protégés. Le botnet Mirai est peut-être le plus célèbre exemple d'un réseau d'appareils IdO exploité à des fins malveillantes. Les créateurs de Mirai ont compromis plus de 100 000 appareils connectés (tels que des routeurs domestiques, des appareils domotiques intelligents, des caméras de sécurité et des enregistreurs vidéo) afin de créer un immense botnet, qu'ils ont ensuite utilisé pour lancer l'attaque Dyn (entre autres), avec un débit de trafic potentiel de 1,2 Tb/s.

Cet immense botnet a submergé Dyn, interrompant la résolution DNS pour tous les sites web et applications qui en dépendaient.

> **« Les chances qu'un appareil publiquement accessible soit piraté sont probablement de l'ordre de 100 %. L'espace d'adressage IPv4 n'est simplement pas très vaste. Vous pouvez désormais analyser l'intégralité de cet espace en quelques heures seulement, surtout si vous disposez d'un vaste botnet. Des analyses des vulnérabilités se déroulent continuellement, et se sont même accélérées au cours des deux dernières années. »**
>
> - Matthew Prince, CEO de Cloudflare

Le botnet a été créé avec un logiciel malveillant appelé Mirai. Mirai explore Internet à la recherche d'appareils dont le nom d'utilisateur et le mot de passe par défaut n'ont jamais été modifiés, ce qui les rend plus faciles à infecter, pirater et contrôler. Hormis une baisse occasionnelle des performances, les propriétaires de ces appareils ne se rendent même pas compte de leur compromission.

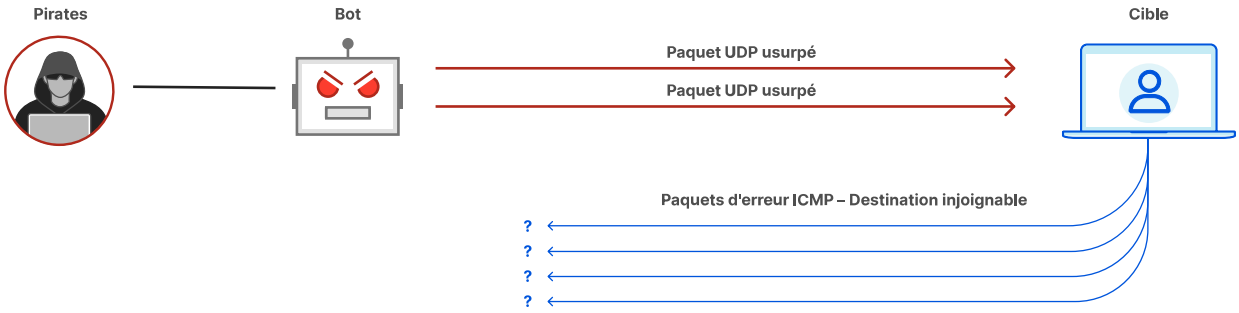
Le botnet Mirai, qui constitue toujours une menace aujourd'hui, est loin d'être le seul botnet activement utilisé pour lancer des attaques DDoS :

- Le **botnet Meris** a été détecté pour la première fois en juin 2021. Si les chercheurs ont identifié au moins 30 000 bots dans ce botnet, ils estiment que le nombre réel de bots est beaucoup plus élevé.[4]
- Le **botnet Mantis** utilise des machines virtuelles piratées et de puissants serveurs, au lieu d'appareils IdO. Chaque bot dispose donc de ressources de calcul considérablement supérieures à celles des appareils de Mirai ou Meris. Le botnet est capable de générer des attaques DDoS colossales, jusqu'à 26 millions de requêtes par seconde dans certains cas.[5]

Les deux méthodes les plus courantes d'exploitation du fonctionnement d'un DNS sont les attaques par amplification (ou « réflexion ») du DNS et les attaques UDP flood.

Submerger les serveurs DNS : les attaques UDP flood

Les attaques UDP flood transmettent un grand nombre de paquets UDP à un serveur cible dans le but de neutraliser la capacité de traitement et de réponse de cet équipement. Une attaque UDP flood peut également entraîner l'épuisement des ressources du pare-feu qui protège le serveur cible, provoquant un déni de service affectant le trafic légitime.



Ces attaques sont particulièrement pertinentes pour les résolveurs DNS, puisque tout le trafic DNS est généralement transmis par UDP (le protocole TCP n'est utilisé que dans certains scénarios d'utilisation spécifiques, tels que les transferts de zone). Puisque le protocole UDP ne nécessite pas de négociation lors de l'ouverture d'une connexion, de grands volumes de paquets UDP indésirables peuvent être transmis à la cible, qui répond ensuite à chacun d'eux dans la mesure du possible. (L'attaque de Mirai sur Dyn, par exemple, était une attaque UDP flood ; lorsqu'une attaque de ce type cible un DNS, elle peut être appelée « DNS flood »).

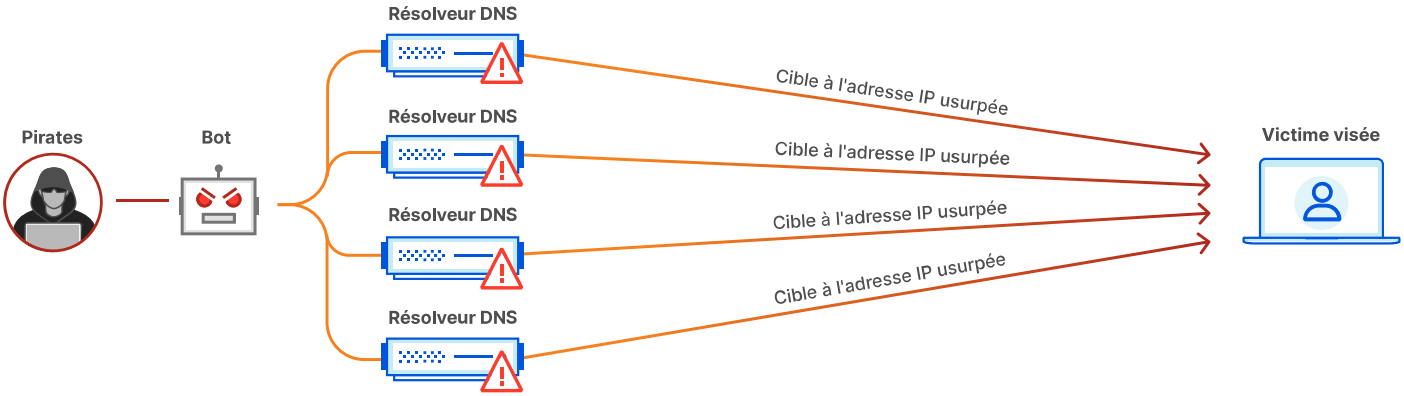
Le principe d'une attaque UDP flood consiste fondamentalement à exploiter les étapes qu'exécute un serveur répondant à un paquet UDP transmis à l'un de ses ports. Si aucun programme ne reçoit de paquets sur ce port, le serveur répond avec un paquet ICMP (ping) afin d'informer l'expéditeur que la destination est injoignable. Chaque nouveau paquet UDP reçu par le serveur suit une série d'étapes permettant le traitement de la requête, consommant des ressources du serveur. Puisque le serveur ciblé utilise des ressources pour vérifier, puis répondre à chaque paquet UDP reçu, ses ressources peuvent rapidement s'épuiser lorsqu'il est inondé d'un grand nombre de paquets UDP.

Exploiter le fonctionnement des DNS : l'amplification DNS

En plus de cibler directement les fournisseurs de services DNS, les acteurs malveillants peuvent également transformer leur infrastructure en arme et exploiter le mode de fonctionnement du DNS pour lancer des attaques DDoS dévastatrices contre d'autres cibles.

Les attaques par amplification DNS exploitent la fonctionnalité des résolveurs DNS ouverts afin de submerger un serveur ou un réseau cible avec une quantité amplifiée de trafic. Au lieu de cibler directement la victime, chaque bot impliqué dans l'attaque transmet des requêtes aux résolveurs DNS ouverts depuis une adresse IP usurpée, remplacée par l'adresse IP source réelle de la victime. La cible reçoit ensuite une réponse des résolveurs DNS.

L'acteur malveillant structure la requête de manière à générer une réponse aussi vaste que possible de la part des résolveurs DNS et, par conséquent, la cible reçoit une amplification du trafic initial de l'auteur de l'attaque. L'agence Cybersecurity & Infrastructure Security Agency (CISA) estime que les attaques par amplification DNS peuvent permettre à un acteur malveillant de transmettre un volume de trafic jusqu'à 54 fois supérieur à la largeur de bande des paquets usurpés qu'il a envoyés.[6]



L'amplification DNS était une composante cruciale de l'attaque qui, en 2013, a mis Spamhaus hors ligne,[7] et a également été utilisée dans de nombreuses autres attaques « dans la nature ».

Bien que les résolveurs DNS ne soient pas directement responsables de ces attaques, ces formes d'exploitation de leurs systèmes peuvent et doivent être évitées. Les organisations disposant d'un système DNS auto-hébergé risquent également de voir leur système être retourné contre elles dans le but de provoquer une défaillance de leurs réseaux internes.

L'impact des attaques DDoS de grande ampleur sur les résolveurs DNS et les victimes en aval

Les organisations qui ont subi des attaques DDoS sont bien conscientes de leur impact négatif considérable, qui inclut notamment des temps d'arrêt, des pertes d'activité, des atteintes à la réputation et de lourdes charges financières. Une source a déterminé que le coût total moyen d'une attaque DDoS s'élevait à 2 millions de dollars pour les sociétés, et à 120 000 dollars pour les petites et moyennes entreprises. Le coût de la réaction à une attaque DDoS pourrait s'élever 2,3 millions de dollars pour les sociétés (mesures effectuées en 2017).[8]

Les attaques ciblant directement les fournisseurs de DNS peuvent avoir des répercussions encore plus importantes, tant pour les organisations qui en dépendent que pour les fournisseurs eux-mêmes : en cas de défaillance de leur DNS, les organisations peuvent chercher un nouveau fournisseur.

Les sites web et les applications ne sont pas les seules cibles des attaques DDoS. Les acteurs malveillants ciblent également souvent les réseaux sur site. Les organisations utilisant un système DNS auto-hébergé peuvent se trouver paralysées pendant que l'attaque se poursuit, tandis que les appareils des clients ne parviennent plus à charger les ressources nécessaires. Une telle attaque peut grever considérablement les activités d'une organisation, voire entraîner leur arrêt complet.

Comment mettre un terme aux futures menaces ciblant l'infrastructure DNS

En fin de compte, seule une architecture adaptée permet d'arrêter les attaques DDoS, dont l'ampleur ne cesse de croître d'année en année.

Atténuation matérielle traditionnelle des attaques DDoS ou atténuation logicielle évolutive

Traditionnellement, pour arrêter une attaque, il était nécessaire d'acheter ou de construire un boîtier physique imposant, qui permettait ensuite de filtrer le trafic entrant. La plupart des fournisseurs de services traditionnels d'atténuation des attaques DDoS s'appuient sur des équipements d'entreprises telles que Cisco, Arbor Networks et Radware, qu'elles regroupent dans des « scrubbing centers » (centres de nettoyage de données).

Il existait des astuces permettant de faire fonctionner ensemble ces gigantesques équipements d'atténuation des attaques, mais ces solutions relevaient du bricolage. Les limites physiques relatives au nombre de paquets que pouvait absorber un boîtier unique sont devenues la limite réelle définissant le volume total qu'était en mesure de traiter un fournisseur de service. En cas d'attaque DDoS très importante, la majorité du trafic hostile n'atteignait même jamais le centre de nettoyage, car avec seulement quelques sites d'implantation, les FAI en amont constituaient un goulet d'étranglement.

Le coût de l'équipement était tel qu'il n'était pas rentable de déployer du matériel de nettoyage à grande échelle. De nombreux fournisseurs de solutions d'atténuation DDoS traditionnelles ne provisionnaient donc leurs services que

lorsque leurs clients subissaient une attaque. Il ne semblait jamais utile de disposer d'une capacité dépassant d'une certaine marge la plus vaste attaque précédemment observée.

Il paraissait rationnel de considérer tout investissement réalisé au-delà de cette limite comme du gaspillage. Cependant, cette conclusion signait en définitive la fin du modèle traditionnel.

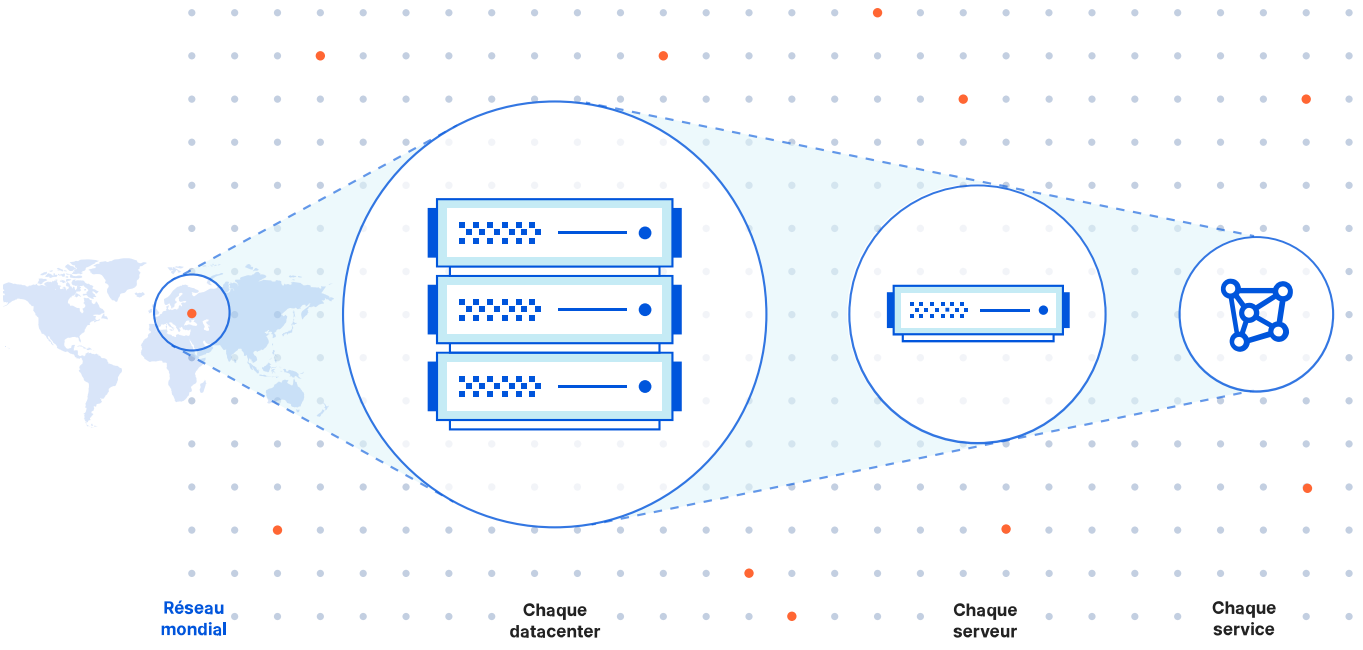
L'avenir ne se présente pas dans un boîtier

Au lieu d'investir dans des boîtiers matériels dédiés à l'atténuation des attaques DDoS, Cloudflare a commencé dès le début avec une architecture très simple. Les premiers racks de Cloudflare n'étaient composés que de trois éléments : un routeur, un switch et un serveur. La composition de ces racks se révèle encore plus simple de nos jours. Elle abandonne souvent complètement le routeur et s'appuie sur des switches capables de traiter une portion suffisamment importante de la table de routage pour assurer l'acheminement des paquets dans la région géographique desservie par le datacenter.

Plutôt que de mettre en œuvre des équipements physiques dédiés d'équilibrage de charge ou d'atténuation dédiés, susceptibles de se transformer en goulets d'étranglement lors d'une attaque, Cloudflare a développé un logiciel utilisant BGP (Border Gateway Protocol), le protocole de routage fondamental d'Internet, afin de répartir les charges de manière géographique, ainsi que dans chaque datacenter présent sur le réseau. Chaque serveur dans chaque rack est capable de répondre à n'importe quel type de requête. Le logiciel de Cloudflare assure la répartition dynamique de la charge de trafic en fonction des besoins d'un client donné à un instant précis ; cela signifie qu'en cas d'attaque de grande ampleur, Cloudflare répartit la charge de trafic sur des dizaines de milliers de serveurs.

Ce modèle permet également à Cloudflare de continuer d'investir de manière rentable dans son réseau. Par exemple, si le datacenter d'une ville donnée a besoin d'accroître sa capacité de 10 %, Cloudflare peut allouer 10 % de serveurs supplémentaires à celui-ci, plutôt que de prendre la décision étagée d'acheter ou de construire un autre boîtier de nettoyage de données.

Puisque chaque processeur dans chaque serveur dans chaque datacenter peut contribuer à l'atténuation des attaques, chaque nouveau datacenter mis en ligne par Cloudflare améliore le service et sa capacité à arrêter les attaques, toujours plus près de la source. Autrement dit, la solution à un botnet massivement distribué consiste à lui opposer un autre réseau massivement distribué. C'est sur ce principe qu'Internet a été fondé : une puissance distribuée et décentralisée, plutôt qu'une force de frappe concentrée sur quelques sites de nettoyage de données.



Comment Cloudflare renforce facilement la sécurité DNS

Toutefois, Cloudflare utilise non seulement un réseau distribué pour bloquer et absorber efficacement le trafic malveillant, mais fournit également un DNS de référence et un service de résolution DNS depuis chacun de ces sites. La capacité de servir des réponses DNS depuis n'importe quel datacenter permet de résoudre les requêtes DNS avec une latence minimale, et signifie également que le DNS de Cloudflare bénéficie de la capacité de l'ensemble du réseau et de sa configuration distribuée.

L'utilisation efficace des ressources du réseau de Cloudflare s'accompagne à la fois d'une réduction des dépenses d'investissement, mais également des frais de fonctionnement. Puisque Cloudflare utilise les mêmes équipements et les mêmes réseaux pour proposer l'ensemble de ses fonctionnalités, le blocage d'une attaque par Cloudflare n'entraîne que rarement des coûts de bande passante supplémentaires.

À mesure que Cloudflare continue d'étendre ses services, sa capacité à arrêter les attaques augmente, elle aussi, de manière proportionnelle. Cloudflare est en mesure d'offrir à ses clients un service d'atténuation des attaques DDoS à un coût fixe, quelle que soit l'ampleur de l'attaque, car les attaques n'entraînent pas d'augmentation plus importants coûts unitaires de Cloudflare.

Ce vaste réseau distribué de serveurs possédant tous les mêmes capacités permet également à Cloudflare de proposer des fonctionnalités à très grande échelle, avec une latence minimale. L'un des services les plus importants est le DNS de référence et secondaire ; Cloudflare est le résolveur DNS le plus rapide du monde.[9]

Le réseau mondial Anycast de Cloudflare permet la résolution DNS à la périphérie du réseau dans chacun des datacenters, présents dans plus de 275 villes, offrant une redondance inégalée et une disponibilité de 100 %. La capacité du réseau de Cloudflare permettant amplement d'absorber les attaques DDoS, il en résulte un DNS résilient face aux attaques de toute taille et de tout type.

Remporter la course aux armements et préserver la résilience face aux attaques DDoS

- Capacité du réseau de Cloudflare au 4e trimestre 2022 : **172 Tb/s** (et ce nombre augmente)
- La plus importante attaque DDoS jamais enregistrée : moins de **2,5 Tb/s**

L'ampleur des attaques DDoS pourrait continuer à croître rapidement, voire exponentiellement, dans les années à venir ; toutefois, Cloudflare est positionnée pour continuer à remporter la course aux armements dans les décennies à venir.

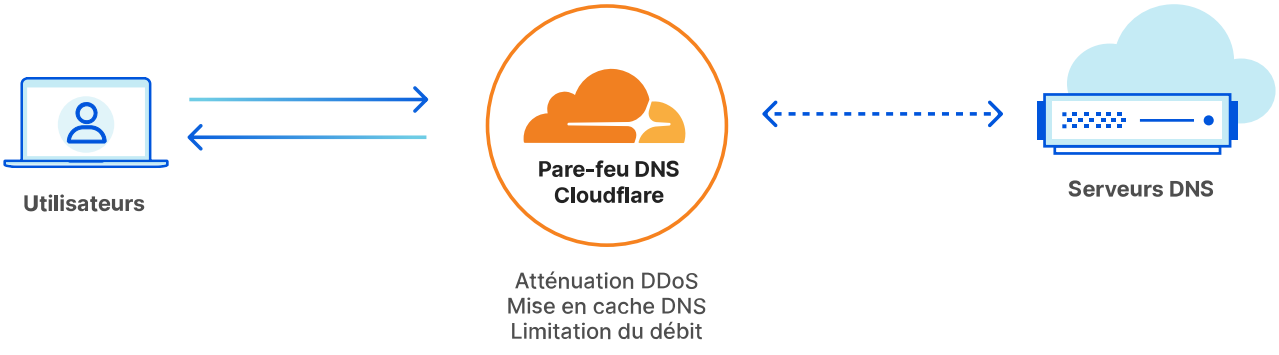
Cloudflare est le seul fournisseur DNS fondamentalement conçu pour atténuer les attaques DDoS de grande ampleur. À l'instar des attaques DDoS, distribuées par nature, le système d'atténuation des attaques DDoS de Cloudflare est, lui aussi, distribué sur l'ensemble de son immense réseau mondial.

Les acteurs malveillants disposent d'un avantage contre la plupart des fournisseurs de service traditionnels : les coûts auxquels font face ces derniers sont particulièrement élevés, car ils doivent acheter des équipements coûteux et de la bande passante. À l'inverse, les coûts encourus par les acteurs malveillants sont faibles, puisqu'ils se servent d'un nombre impressionnant d'appareils piratés pour générer un volume de trafic asymétrique contre leurs cibles. La recette secrète de Cloudflare repose donc sur son logiciel, qui permet de répartir la charge sur l'ensemble du réseau massivement distribué d'équipements informatiques standard de Cloudflare.

Protéger les DNS contre toutes sortes d'attaques et d'exploitations

Au quatrième trimestre 2022, Cloudflare traite environ 22,6 millions de requêtes DNS par seconde (requêtes de référence et requêtes de résolution), tout en atténuant un volume croissant d'attaques DDoS. Cloudflare DNS préserve sa résilience contre les attaques DDoS et de bots de toute ampleur, des importantes attaques DDoS actuelles aux attaques de type « water torture » et aux autres formes d'exploitation des DNS.

Pour les fournisseurs de services DNS et les organisations qui hébergent elles-mêmes leur infrastructure DNS, le pare-feu DNS de Cloudflare offre une solution qui les aide non seulement à protéger leur infrastructure et leurs utilisateurs contre les attaques DDoS de grande ampleur, mais améliore également leurs performances en gérant la mise en cache des enregistrements DNS et les réponses en leur nom.



L'intégration native des solutions DNS et de pare-feu DNS de Cloudflare à la fonctionnalité d'atténuation des attaques DDoS garantit que vos applications sont toujours protégées et disponibles, même face à certaines des plus vastes attaques DDoS jamais enregistrées.

Conclusions

Cloudflare continue à s'étendre, ajoutant régulièrement de nouvelles villes et de nouveaux pays à son réseau. Cloudflare demeure extrêmement vigilante quant aux futures attaques, mais reste convaincue que son architecture constitue en définitive la meilleure approche pour arrêter les menaces à venir, quelles qu'elles soient. Associez-vous au réseau construit pour arrêter les attaques contre les DNS, aujourd'hui comme dans les années à venir :

- Déployez Cloudflare pour vous protéger contre toutes les attaques DDoS, notamment les attaques DDoS lancées par l'intermédiaire de vastes botnets et les attaques par amplification
- Fiez-vous à Cloudflare en tant que fournisseur de DNS de référence pour protéger le bon fonctionnement de votre DNS, malgré les attaques
- Protégez votre infrastructure DNS et les victimes potentielles d'attaques DDoS en utilisant le pare-feu DNS de Cloudflare pour limiter le taux de requêtes et défléchir les attaques

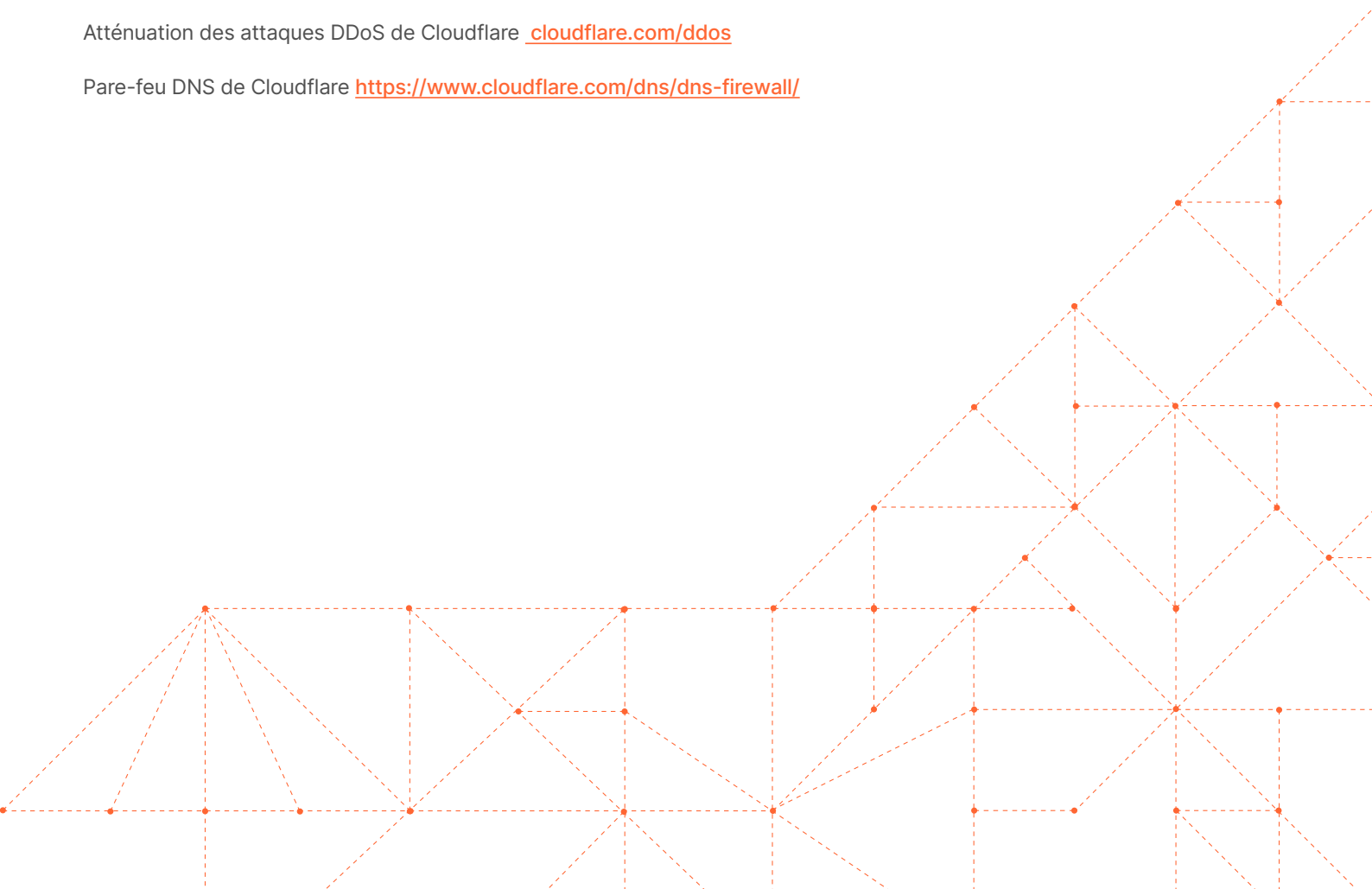
La mise en œuvre est très simple et demande généralement moins de 5 minutes. Consultez les offres, de l'offre gratuite à l'offre Entreprise, sur cloudflare.com/plans.

Pour en savoir plus sur les solutions Cloudflare, consultez :

Cloudflare DNS https://www.cloudflare.com/dns/

Atténuation des attaques DDoS de Cloudflare cloudflare.com/ddos

Pare-feu DNS de Cloudflare https://www.cloudflare.com/dns/dns-firewall/



Références

1. « DDoS Attack Against Dyn Managed DNS ». Dyn Statue Updates, 21 octobre 2016, https://www.dynstatus.com/incidents/nlr4yrr162t8. Consulté le 3 octobre 2022.
2. Cimpanu, Catalin. « AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever ». ZDNET, 17 juin 2020, https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/. Consulté le 3 octobre 2022.
3. Yoachimik, Omer. « Cloudflare atténue une attaque DDoS de 26 millions de requêtes par seconde ». Cloudflare, 14 juin 2022, https://blog.cloudflare.com/26m-rps-ddos/. Consulté le 3 octobre 2022.
4. Ganti, Vivek and Omer Yoachimik. « A Brief History of the Meris Botnet ». Cloudflare, 9 novembre 2021, https://blog.cloudflare.com/meris-botnet/. Consulté le 3 octobre 2022.
5. Yoachimik, Omer. « Mantis - the most powerful botnet to date ». Cloudflare, 14 juillet 2022, https://blog.cloudflare.com/mantis-botnet/. Consulté le 3 octobre 2022.
6. « Alert (TA14-017A): UDP-Based Amplification Attacks ». CISA, 18 décembre 2019, https://www.cisa.gov/uscert/ncas/alerts/TA14-017A. Consulté le 24 octobre 2022.
7. Prince, Matthew. « The DDoS That Knocked Spamhaus Offline (And How We Mitigated It). » Cloudflare, 20 mars 2013, https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/. Consulté le 24 octobre 2022.
8. Kobialka, Dan. « Kaspersky Lab Study: Average Cost of Enterprise DDoS Attack Totals $2M ». MSSP Alert, 25 février 2018, https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/. Consulté le 3 octobre 2022.
9. « DNS Performance Analytics and Comparison ». DNSPerf, https://www.dnsperf.com/. Consulté le 24 octobre 2022.

CLOUDFLARE

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES/3855.20221104