CLOUDFLARE®

Cinq bonnes pratiques pour mitiger les attaques DDoS

Comment vous défendre contre des attaques par déni de service distribué rapidement changeantes et remédier aux vulnérabilités de chaque couche

+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

CLOUDFLARE

I. Résumé

Les attaques par déni de service distribué (DDoS, « Distributed Denial of Service ») restent l'une des méthodes les plus efficaces employées par les cybercriminels pour causer d'importants dommages financiers et opérationnels et porter atteinte à la réputation d'entreprises du monde entier. Bien que ces attaques revêtent différentes formes, l'objectif demeure toujours de provoquer l'arrêt des serveurs, services ou réseaux ciblés en les inondant de trafic provenant de dispositifs ou de réseaux compromis.

À mesure que les organisations ont renforcé leurs défenses, les cybercriminels ont réagi en lançant de nouveaux types d'attaques, ciblant différents services et applications. Certaines de ces attaques ciblent les couches 3 et 4 du modèle OSI (Open Systems Interconnection) de manières nouvelles, générant des pics de trafic réseau pouvant atteindre 1,3 Tb par seconde, voire plus. D'autres sont des attaques couche 7, à bas débit et à faible intensité, conçues pour passer inaperçues et cibler une ou plusieurs passerelles de services et couches d'application.

Relever les défis liés aux attaques DDoS exige d'adopter une approche globale, capable de répondre à toutes les menaces, à tous les niveaux. Cependant, la mise en œuvre d'une sécurité renforcée ne doit pas s'effectuer au détriment des performances. Si des solutions sur site peuvent constituer une partie de la réponse, une solution plus fiable devra intégrer les performances à une mitigation évolutive dans le Cloud, avec une exécution en périphérie de réseau pour offrir une agilité maximale et une capacité illimitée.

1ÈRE PARTIE

Qu’est-ce qu’une attaque DDoS ?

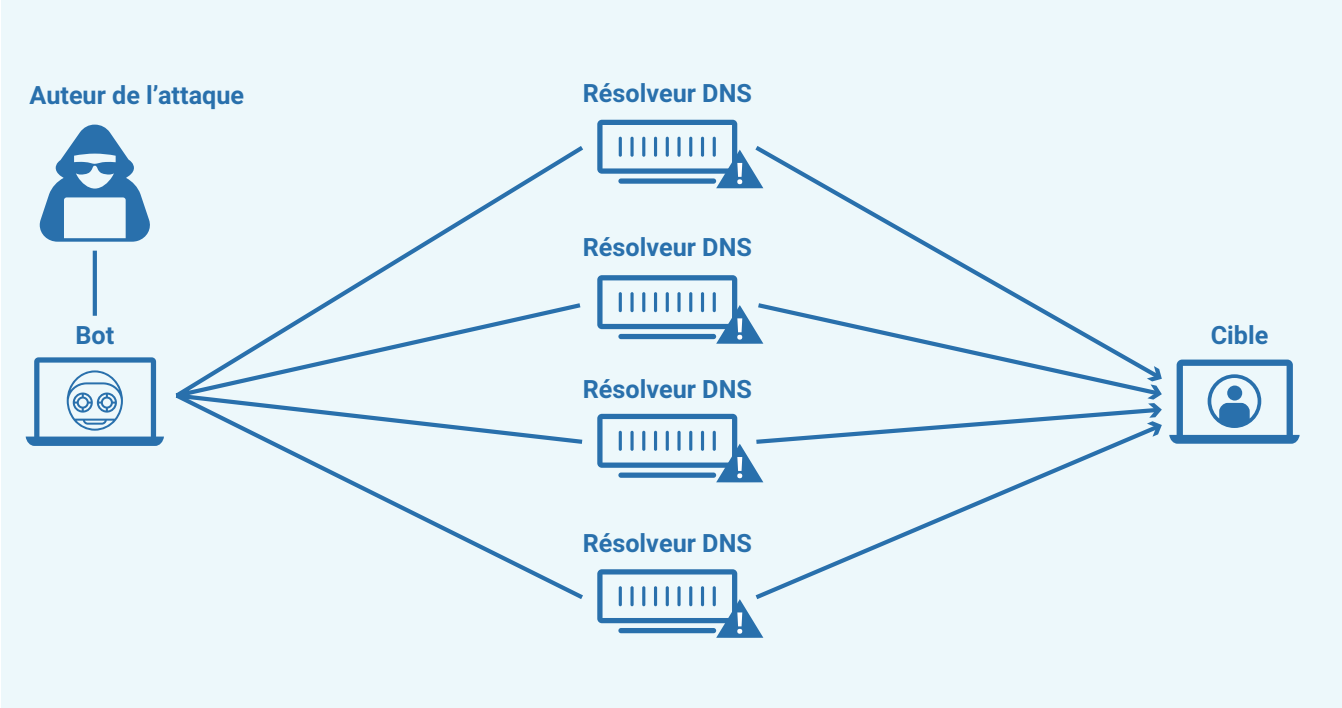
Une attaque par déni de service distribué (DDoS, « Distributed Denial of Service ») est une tentative malveillante de perturber le trafic normal d'un serveur, d'un service ou d'un réseau ciblé en l'inondant de trafic Internet. Pour être efficaces, ces attaques exigent que leurs auteurs prennent le contrôle d'ordinateurs, de routeurs, de dispositifs IoT ou d'autres terminaux connectés et qu'ils les utilisent comme sources de trafic lors de l'attaque. Ces machines sont infectées par des logiciels malveillants, puis transformées en armes sous la forme d'un « botnet » activé à distance.

Lorsque l'adresse IP d'un serveur ou d'un réseau ciblé est établie, tous les bots transmettent simultanément des requêtes à cette cible, avec l'objectif de provoquer un dépassement de capacité et ainsi, d'entraîner un déni de service pour le trafic normal. Chaque bot étant en soi un appareil légitime, il peut être extrêmement difficile de séparer le trafic de l'attaque du trafic normal.

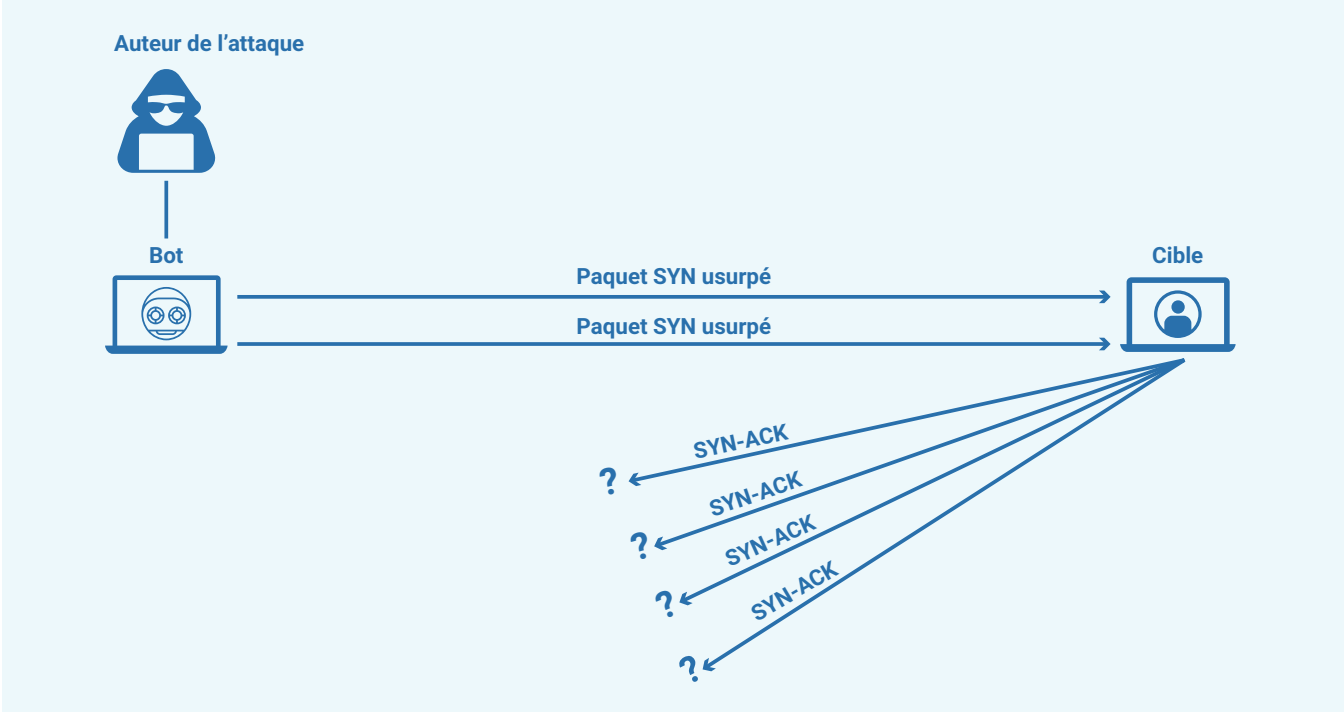
Types d'attaques DDoS

Les attaques DDoS peuvent cibler n'importe laquelle des 7 « couches » distinctes utilisées par le modèle OSI pour les connexions réseau. Si ces attaques, dans leur ensemble, consistent à « noyer » les cibles en les inondant de trafic malveillant, elles peuvent être divisées en trois catégories distinctes.

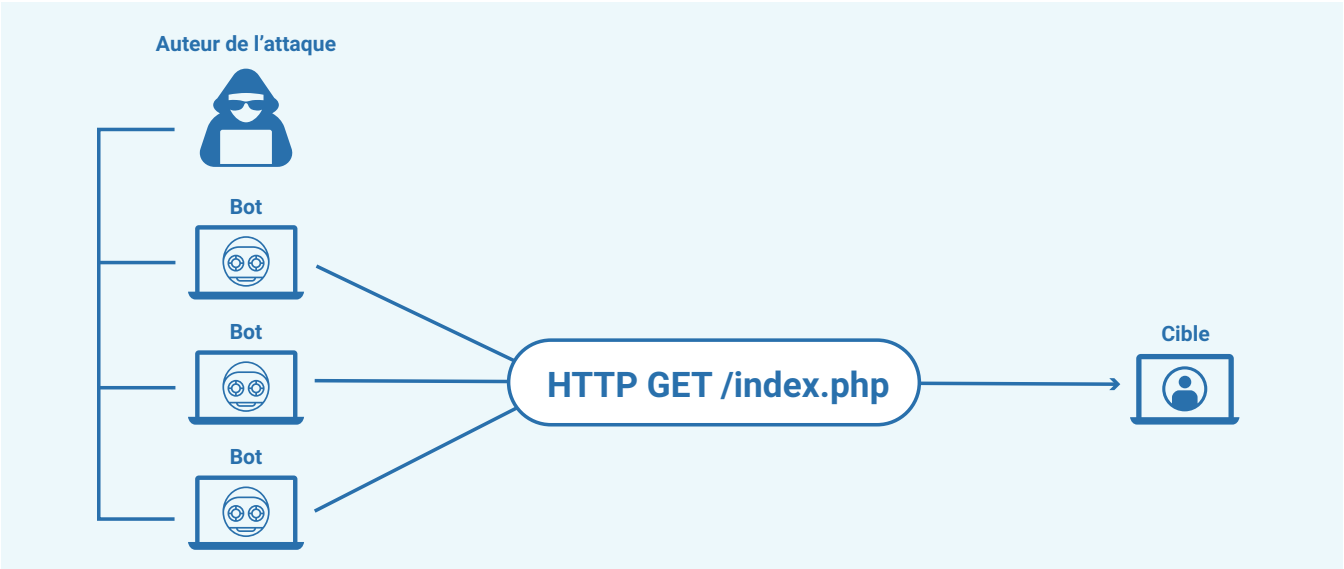
ATTAQUES VOLUMÉTRIQUES : ces attaques sont conçues pour entraîner une congestion entre le site et Internet en ciblant le réseau, en grevant les performances du web et en dégradant l'accès pour les utilisateurs légitimes. Ces attaques recourent souvent à l'amplification DNS et à d'autres techniques pour générer des surcharges massives de trafic, mesurées en bits par seconde (bit/s).



ATTAQUES DE PROTOCOLE : l'objectif des attaques de protocole est de cibler les vulnérabilités des couches 3 (réseau) et 4 (transport) du modèle OSI et de consommer toute la capacité disponible des serveurs web ou de leurs ressources intermédiaires, notamment des pare-feu et des équipements de répartition de charge. Ces attaques peuvent recourir aux techniques SYN flood et Ping of Death, aux attaques DDoS par rebond (« Smurf DDoS ») et aux attaques par fragmentation de paquets, toutes mesurées en paquets par seconde (p/s).



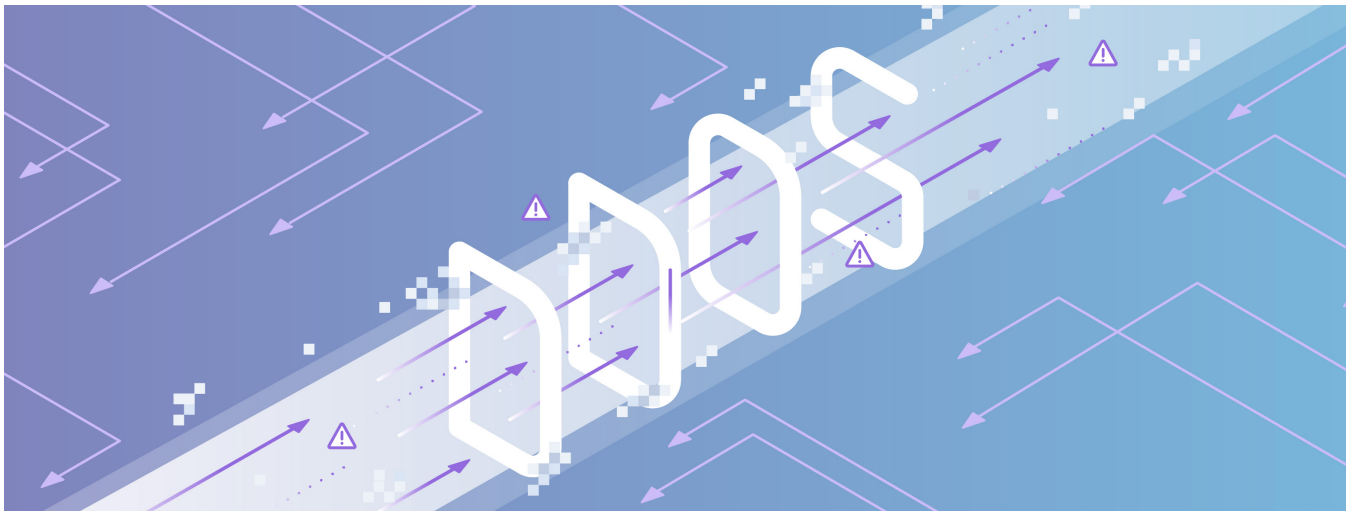
ATTAQUES CONTRE LA COUCHE D'APPLICATION : parfois appelées attaques DDoS de couche 7, ces attaques visent la couche dans laquelle les pages web sont générées sur le serveur, avant d'être diffusées en réponse aux requêtes HTTP ou HTTPS. Ces attaques peuvent être comparées à l'utilisation répétée de la fonction « Actualiser » d'un navigateur web sur plusieurs ordinateurs à la fois. Le flux HTTP/S résultant est mesuré en requêtes par seconde (r/s).



Ces différents types d'attaques se recoupent à certains niveaux. Certaines attaques de protocole peuvent être volumétriques, par exemple. Il y a ensuite les attaques multi-vecteurs, dans lesquelles les auteurs de l'attaque ciblent plusieurs couches de la pile de protocoles en même temps ou changent de vecteur d'attaque en fonction des contre-mesures mises en œuvre par la cible. Par ailleurs, de nombreuses attaques multi-vecteurs sont de simples écrans de fumée et sont destinées à couvrir une tentative de violation de données ou un autre crime.

Comment les attaques DDoS portent atteinte à la réputation de votre entreprise

La mise hors ligne d'une infrastructure informatique suite à une attaque DDoS peut avoir un impact négatif sur les revenus, la qualité du service à la clientèle et les activités opérationnelles fondamentales. Que l'objectif de l'attaque soit de paralyser votre site ou votre réseau, de rediriger le trafic vers des rivaux, de masquer le vol de données de l'entreprise ou simplement de gravement porter atteinte à votre réputation, les utilisateurs n'hésiteront pas à tenir votre entreprise responsable de l'incident. En moyenne, une attaque DDoS peut coûter 123 000 dollars à une petite entreprise et plus de 2 millions de dollars à une grande entreprise[1]. Et les attaques sont incessantes. Le nombre total d'attaques DDoS dans le monde devrait passer de 11,9 millions en 2020 à plus de 14,5 millions d'ici 2022[2].



2E PARTIE

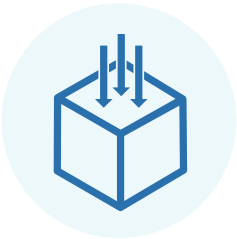
Les défis changeants des attaques DDoS et comment les relever

D'une manière générale, pour vous protéger contre les attaques DDoS, vous devez pouvoir :

- Différencier les pics de trafic résultant d'une attaque ou d'une forte demande de la part d'utilisateurs légitimes
- Bloquer le trafic provenant des botnets sans interrompre le trafic légitime
- Acheminer intelligemment le reste du trafic en le scindant en fragments gérables, afin d'éviter les dénis de service
- Analyser continuellement le trafic à la recherche de modèles malveillants pouvant contribuer au développement de défenses adaptées et renforcées

Aujourd'hui, deux tendances émergentes rendent tout cela plus difficile.

Les attaques volumétriques gagnent en ampleur



- Le nombre d'attaques DDoS volumétriques de plus de 100 Gb/s a progressé de 967 % entre 2018 et 2019[3]
- Les attaques DDoS atteignant 1,3 Tb/s, telles que l'attaque qui a fait tomber GitHub en 2018, sont également devenues monnaie courante
- Début 2020, une attaque DDoS volumétrique de la couche réseau aurait atteint 92 Gb/s et 10,38 millions de paquets par seconde (mp/s)[4]
- Si la plupart des attaques DDoS volumétriques durent quelques minutes seulement, certaines peuvent durer des heures, et jusqu'à 73 % des organisations frappées par des attaques volumétriques sont ciblées une nouvelle fois dans un délai de 24 heures[5]

Les attaques deviennent plus complexes

- Trois quarts[6] des attaques DDoS ciblent plusieurs vecteurs
- L'attaque par amplification DNS des couches 3 et 4, associée à une attaque HTTP/S flood de la couche 7, est un exemple d'attaque DDoS multi-vecteurs
- Plus l'attaque est complexe, plus il est difficile de la mitiger. L'objectif de l'auteur de l'attaque est de se fondre dans la masse autant que possible, afin de rendre d'autant plus difficile la différenciation du trafic légitime et du trafic malveillant
- Les tentatives de mitigation visant à refuser ou limiter le trafic s'avéreront inutiles si l'attaque s'adapte pour contourner cette contre-mesure

Voici cinq bonnes pratiques que les organisations spécialistes de la mitigation d'attaques DDoS doivent privilégier, inspirées de ces exigences et de l'évolution des tendances.

3E PARTIE

Bonnes pratiques pour la mitigation des attaques DDoS

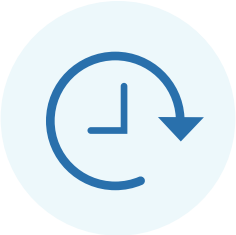
1 ADAPTEZ VOS TACTIQUES AUX RESSOURCES QUE VOUS PROTÉGEZ

Si votre objectif est de protéger vos serveurs web, un proxy inverse empêchera les attaquants d'identifier et de cibler les adresses IP de vos serveurs. Au lieu de cela, ils ne pourront cibler que le proxy inverse. Pour les attaques DDoS de couche 7, plus complexes, un pare-feu d'application web (WAF, « Web Application Firewall ») peut se comporter comme un proxy inverse, en protégeant les serveurs cibles contre certains types de trafic malveillant. Certaines entreprises créent ou déploient leurs propres proxy inverses. Cependant, ceci nécessite des ressources considérables d'ingénierie logicielle et matérielle, ainsi qu'un investissement important en matériel physique.

Un des moyens les plus simples et économiques de tirer parti des avantages d'un proxy inverse est d'utiliser un réseau de diffusion de contenu (CDN, « Content Delivery Network »). Privilégiez un réseau CDN offrant une fonctionnalité de répartition de charge des serveurs à l'échelle mondiale, permettant de répartir le trafic de votre site sur plusieurs serveurs à travers le monde. Ceci permettra de mitiger les attaques DDoS plus près de la source, sans altérer les performances.

Si l'objectif est de protéger l'infrastructure du réseau, la redirection avec le protocole Border Gateway Protocol (BGP) peut être mise en œuvre pour réacheminer le trafic vers des centres de nettoyage de données permettant de filtrer le trafic malveillant. Cela dit, la redirection de tout le trafic vers un nombre restreint de centres de nettoyage de données géographiquement distants peut ajouter une latence considérable.

Il est donc recommandé d'opter pour des solutions de mitigation des attaques DDoS dans le Cloud, dotées d'une capacité suffisante. Avec une solution de mitigation dans le Cloud, les numéros de système autonome (ASN) sont annoncés par le fournisseur de services de mitigation. Ainsi, le trafic est directement acheminé vers le centre de nettoyage de données, au lieu d'être adressé au serveur d'origine. Le trafic est filtré plus près de la source de l'attaque, réduisant ainsi encore la latence.

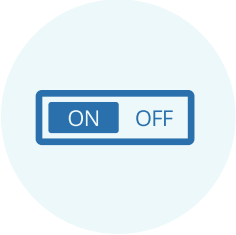


2 PRIVILÉGIEZ LES DEUX INDICATEURS LES PLUS IMPORTANTS : LA CAPACITÉ ET LE DÉLAI DE MITIGATION

Évaluez votre capacité actuelle à mitiger les attaques DDoS sans altérer le fonctionnement de votre site. Traditionnellement, l'approche mise en œuvre pour absorber les pics de trafic générés par les attaques DDoS consistait à installer de vastes batteries de serveurs sur site. Toutefois, cette approche s'avère rapidement coûteuse, et même la plus robuste des infrastructures d'entreprise risque d'être finalement dépassée face à des attaques volumétriques dont l'ampleur croît de jour en jour.

La limitation du débit peut se montrer utile. Toutefois, elle grève les performances et peut malgré tout engendrer une défaillance en cas de surcharge de votre infrastructure. À l'heure où la moindre diminution de la disponibilité peut entraîner une perte importante de revenus et de productivité, le délai de mitigation devient primordial. Pour réduire le délai de mitigation, vous devez vous assurer qu'en cas de défaillance, le trafic peut être transféré vers un autre site. Toutefois, cette approche n'est viable qu'un certain temps – jusqu'à ce que votre infrastructure ne soit submergée.

Ici encore, une approche plus efficace consiste à déployer une solution de mitigation dans le Cloud, qui offre une capacité illimitée de protection contre les attaques DDoS (quelle que soit leur ampleur ou leur complexité). Elle doit également permettre de provisionner des services à la périphérie du réseau, pour une agilité maximale lors de la mitigation d'attaques DDoS rapidement changeantes.



3 RÉFLÉCHISSEZ TOUJOURS AUX AVANTAGES DE LA PROTECTION TOUJOURS ACTIVE OU DE LA PROTECTION À LA DEMANDE

Avec les services de mitigation à la demande, le trafic circule comme il le fait habituellement, jusqu'à ce qu'une attaque DDoS soit détectée. À cet instant, le trafic est redirigé vers le service de mitigation dans le Cloud, filtré, puis renvoyé vers le serveur d'origine. Vous ne payez la mitigation des attaques DDoS que lorsqu'elle est nécessaire, et aucune gestion ou ressource supplémentaire n'est requise. Cependant, ce choix impose certains compromis, notamment au regard du délai de mitigation.

Arrêter l'attaque demande plus de temps, car les pics de trafic doivent atteindre certains seuils avant que l'analyse ne démarre et qu'un opérateur n'active manuellement le service de mitigation. À titre de comparaison, la mitigation toujours active achemine et filtre continuellement tout le trafic du site. Ainsi, à tout instant, seul le trafic légitime atteint les serveurs du client. Bien qu'elle soit plus coûteuse que les services à la demande, la mitigation toujours active offre une protection ininterrompue et des temps de réponse plus rapides, puisque le service n'a jamais besoin d'être activé manuellement. Par ailleurs, compte tenu du nombre croissant d'attaques DDoS, des services toujours actifs proposés à un prix forfaitaire pourraient s'avérer moins coûteux pour les organisations confrontées à un barrage d'attaques continu.

4 NE SACRIFIEZ JAMAIS LA PERFORMANCE AU PROFIT DE LA SÉCURITÉ

Les attaques DDoS provoquent des lenteurs et des défaillances qui dégradent les performances, mais nuisent également à la capacité des organisations à pérenniser leur croissance. Aujourd'hui, les consommateurs numériques s'attendent à ce que les sites web et les applications se chargent instantanément et ne soient jamais (mais alors, vraiment jamais) hors ligne. La latence devient perceptible par l'utilisateur moyen dès 30 millisecondes, et une seule seconde de temps de chargement supplémentaire peut faire chuter les conversions de 7 %[7].

La latence nuit également à la productivité. Même dans les meilleurs scénarios, un employé perd une semaine par an à attendre que le réseau de son entreprise réagisse.[8] Pour les entreprises du classement Fortune 1000, le coût total moyen des temps d'arrêt se situe actuellement entre 1,25 et 2,5 milliards de dollars par an[9]. Se protéger contre les attaques DDoS sans altérer les performances exige de trouver un juste équilibre.

Comme nous l'avons expliqué, de nombreuses entreprises tentent de mitiger ces menaces en redirigeant le trafic vers des centres de nettoyage de données, généralement très éloignés de la source de trafic ou du serveur d'origine. Ceci crée un goulet d'étranglement, qui se traduit par des niveaux de latence pouvant être tout aussi préjudiciables qu'une attaque. C'est pourquoi les services limités qu'offrent les centres de nettoyage de données ne sont pas un choix réaliste pour contrer les attaques DDoS. Par ailleurs, intéressez-vous aux services de mitigation dans le Cloud offrant la capacité de mettre en œuvre la détection et la mitigation sur des sites physiquement proches de la source d'une attaque, dans n'importe quelle région du monde, afin d'améliorer les temps de réponse.

5 OPTEZ POUR L'INTELLIGENCE POUR GARDER UNE LONGUEUR D'AVANCE SUR LES AUTEURS D'ATTAQUES

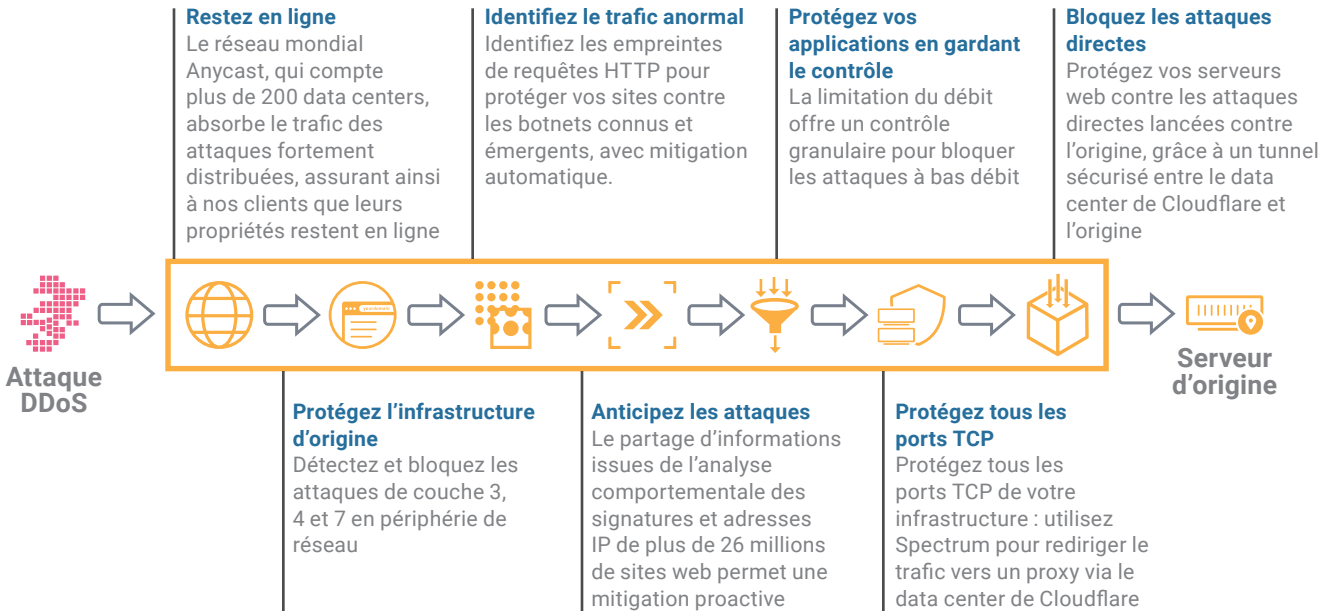
Repousser des attaques DDoS toujours plus complexes nécessite plus qu'une approche par couches. Cela nécessite d'analyser en permanence le trafic à la recherche de modèles malveillants pouvant contribuer au développement de défenses intelligentes et adaptatives, indispensables pour contrer de futures attaques. L'attaque DDoS qui se déroule en ce moment contient le secret pour triompher de la prochaine attaque.

Lorsque vous évaluez des solutions de mitigation dans le Cloud, il est important de regarder au-delà de la capacité ou des vitesses de transfert et de filtrage. Étudiez également le type d'informations que génère l'étendue des différentes solutions. Plus un réseau de mitigation est vaste et résilient, plus il peut fournir d'informations sur l'évolution des modèles d'attaque – et plus ces services peuvent être préventifs.

Comment Cloudflare peut vous aider

L'approche de sécurité par couches de Cloudflare réunit plusieurs fonctionnalités de mitigation des attaques DDoS dans un seul service. Elle empêche les interruptions provoquées par le trafic malveillant tout en autorisant le trafic légitime, préservant ainsi la disponibilité et le bon fonctionnement des sites web, des applications, des API et des réseaux dans leur ensemble.

Avec des data centers dans plus de 200 villes et plus de 90 pays et une capacité de réseau supérieure à 35 Tb/s, Cloudflare mitige les attaques DDoS près de la source, dans un délai de 100 millisecondes pour 99 % de la population connectée à Internet dans le monde développé.



MITIGATION RAPIDE ET AUTOMATISÉE

Contrairement aux solutions traditionnelles, dont la capacité dépend d'un nombre limité de centres de nettoyage de données, nos points de présence dans le monde entier hébergent des services de sécurité pour vous protéger contre les attaques DDoS, quelle que soit leur ampleur ou leur complexité. Ces services incluent notamment la capacité de disséminer le trafic sur des serveurs distribués, jusqu'à ce qu'il soit absorbé par le réseau.

INFORMATIONS SUR LES MENACES AVEC UNE PORTÉE MONDIALE

La protection anti-DDoS de Cloudflare est alimentée par les informations de son réseau mondial, qui protège plus de 25 millions de sites web et achemine chaque jour plus d'un milliard d'adresses IP uniques. Ces informations offrent un point de vue unique pour vous protéger contre les attaques les plus sophistiquées.

PROTECTION ÉCONOMIQUE

Tous les programmes de Cloudflare proposent une mitigation illimitée et non mesurée des attaques DDoS, quelle que soit leur ampleur, sans frais supplémentaires – et sans pénalité en cas de pics de trafic réseau résultant d'une attaque distribuée.

UTILISATION ET GESTION FACILES

La protection anti-DDoS toujours active dans le Cloud de Cloudflare repose sur une interface intuitive, permettant aux utilisateurs de protéger rapidement et facilement leurs propriétés Internet contre les attaques DDoS, quelle que soit leur ampleur ou leur sophistication, en quelques clics seulement.

SÉCURITÉ ET PERFORMANCES INTÉGRÉES

Notre protection est conçue pour s'intégrer, apprendre et s'exécuter de manière fluide avec d'autres solutions de sécurité et de performance telles que Web Application Firewall, Bot Management, Magic Transit, Load Balancer, CDN et d'autres.

ANALYSE DES DONNÉES À VOTRE CONVENANCE

Cloudflare Analytics vous permet d'analyser les événements DDoS depuis le tableau de bord intégré ou l'interface GraphQL de Cloudflare. Les journaux de Cloudflare peuvent également être intégrés aux principaux SIEM tiers pour offrir une intégration fluide aux processus de votre activité.

Conclusion

Relever les défis associés aux attaques DDoS exige d'adopter une approche globale, capable de répondre à toutes les menaces, à tous les niveaux. Les solutions sur site peuvent constituer une partie de la réponse, mais elles peuvent rapidement s'avérer coûteuses. Une solution plus fiable devra allier performances et mitigation évolutive dans le Cloud et provisionner les services en périphérie de réseau, afin d'offrir une agilité maximale et une capacité illimitée. Elle offrira ainsi une résilience garantie contre les attaques DDoS, quelle que soit leur ampleur ou leur complexité.

Notes de bas de page

1 Kaspersky Labs, « DDoS Breach Costs Rise to Over $2M for Enterprises Finds Kaspersky Lab Report », Kaspersky Labs, 22 février 2018

2 Crane, Casey, « The 15 Top DDoS Statistics You Should Know in 2020 », Cybercrime Magazine, 16 novembre 2019

3 DeNisco Rayome, Alison, « Major DDoS attacks increased 967% this year », TechRepublic, 24 avril 2019

4 Avital, Nadav, « 2019 Global DDoS Threat Landscape Report », Security Boulevard, 5 février 2020

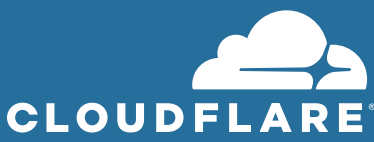
5 Cook, Sam, « DDoS attack statistics and facts for 2018-2019 », Comparitech, 20 août 2019

6 Ibid.

7 Stein, Jake, « Behind the Buzzword: The Reality of Real Time », InformationWeek, 5 septembre 2019

8 Tyson, Mark, « Users Lose a Full Working Week Every Year Due to Slow Computers », Hexus.net, octobre 2013

9 « IDC Study - The cost of downtime », Tech Republic, 30 septembre 2017



+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : 200330