CLOUDFLARE

Infographie

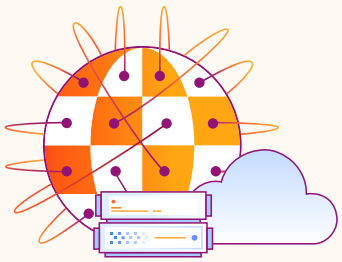
5 questions à poser à votre fournisseur de services d'atténuation des attaques DDoS

Face à l'augmentation de la fréquence et de la complexité des attaques DDoS, le choix du bon service d'atténuation des attaques DDoS pour protéger vos réseaux et vos utilisateurs se révèle essentiel. Tous les services ne se valent cependant pas et un mauvais choix à cette étape peut conduire à des désagréments, des problèmes de performances et des interruptions de service.

Vous trouverez ci-dessous cinq questions à vous poser au moment de choisir un fournisseur de services d'atténuation des attaques DDoS :

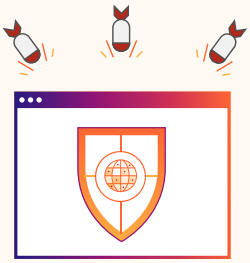
1. Le service a-t-il été développé nativement dans le cloud ?

Pour être efficace, un service d'atténuation des attaques DDoS doit être cloud-native et pas reposer sur une technologie sur site virtualisée et hébergée dans des datacenters situés dans le cloud. Quelle est la différence ? Les services d'atténuation cloud-native peuvent s'adapter parfaitement aux besoins de votre entreprise, sans imposer de goulets d'étranglement artificiels en termes de performances, alors que les équipements virtuels hébergés dans le cloud s'accompagnent des difficultés de gestion propres aux équipements physiques sur site.



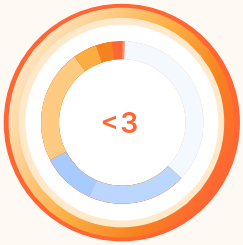
2. Quelle est la capacité réseau du fournisseur ?

Les attaques DDoS à grande échelle, comme l'attaque de 2,3 Tb/s dont un client d'AWS a fait les frais en 2020, peuvent submerger les fournisseurs de services dont le réseau n'est pas suffisamment performant pour absorber le trafic DDoS. L'attaque DDoS la plus volumineuse détectée et atténuée par Cloudflare s'est produite en 2023 et culminait à 2,6 Tb/s.[1] Choisissez un fournisseur proposant une capacité réseau suffisante pour résister aux attaques de cette ampleur sans interruption de service ni dégradation des performances.



3. Le service peut-il détecter les attaques DDoS et y réagir rapidement ?

Lorsque vous faites face à une attaque, un délai d'atténuation faible (c'est-à-dire, le temps nécessaire pour détecter et atténuer les attaques) s'avère essentiel. Une interruption de service supérieure à quelques secondes peut engendrer des conséquences irréversibles pour l'expérience client, la réputation de la marque et le chiffre d'affaires de l'entreprise.



1. Source : https://wiki.cfdata.org/display/COM/Public-Facing+Stats

4. Le service est-il disponible dans tous les datacenters ?

En cas d'indisponibilité des fonctions de nettoyage DDoS dans un datacenter, le trafic fait l'objet d'une redirection forcée vers des « centres de nettoyage » spécialisés qui ajoutent souvent de la latence et nuisent aux performances des applications. Choisissez un fournisseur capable de proposer des services d'atténuation dans chaque datacenter, mais aussi de faire en sorte que votre trafic emprunte toujours le meilleur itinéraire possible.

5. Le service est-il automatisé ?

Un service d'atténuation des attaques DDoS efficace doit proposer des fonctionnalités d'automatisation et de libre-service accessibles depuis un tableau de bord ou une API afin de vous permettre d'activer et de gérer rapidement votre solution de protection contre les menaces. Sélectionnez un fournisseur facile à contacter, réactif et capable d'adopter une attitude proactive en matière de détection des menaces, mais aussi d'atténuer ces dernières sans entraîner d'interruption de vos services.

Cloudflare Magic Transit protège des sous-réseaux IP entiers contre les attaques DDoS, tout en accélérant le trafic. Constitué de datacenters implantés dans plus de 320 villes, le réseau mondial de Cloudflare bloque en moyenne 209 milliards de menaces par jour, dont certaines des attaques DDoS les plus volumineuses de l'histoire.

Pour bien débuter avec Magic Transit, demandez votre démonstration gratuite dès aujourd'hui.

© 2024 Cloudflare, Inc. Tous droits réservés. 01 73 01 52 44 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-6051.2024AUG20