Cloudflare Magic Transit protège les réseaux tout en améliorant les performances

Cloudflare Magic Transit offre une protection anti-DDoS et permet une accélération du trafic pour les réseaux sur site, dans le cloud et hybrides. Avec des datacenters présents dans plus de 200 villes et une capacité d'atténuation des attaques DDoS dépassant 42 Tbit/s, Magic Transit peut détecter et atténuer les attaques à proximité de l'origine dans un délai de 10 secondes (moins de 3 secondes en moyenne), tout en profitant d'avantages intégrés en matière de performances.

Ce document présente les résultats des tests Catchpoint que nous avons effectués sur notre réseau afin de quantifier l'incidence de la solution Magic Transit sur la latence. Les résultats de ces tests font état d'une amélioration des performances réseau (en termes de latence et de perte de paquets) pour le client test lors de l'acheminement du trafic par Cloudflare Magic Transit. Plus concrètement, nos observations ont révélé une diminution de la latence de l'ordre de 3 ms et une quantité de paquets perdus quasiment nulle dans ce cas de figure.

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

Comment la solution Magic Transit protège-t-elle l'infrastructure réseau sans nuire aux performances ?

Avant l'apparition de Magic Transit, la protection de l'infrastructure réseau contre les attaques DDoS reposait sur deux stratégies principales : les équipements physiques anti-DDoS sur site et les solutions de nettoyage dans le cloud, ou « scrubbing ».

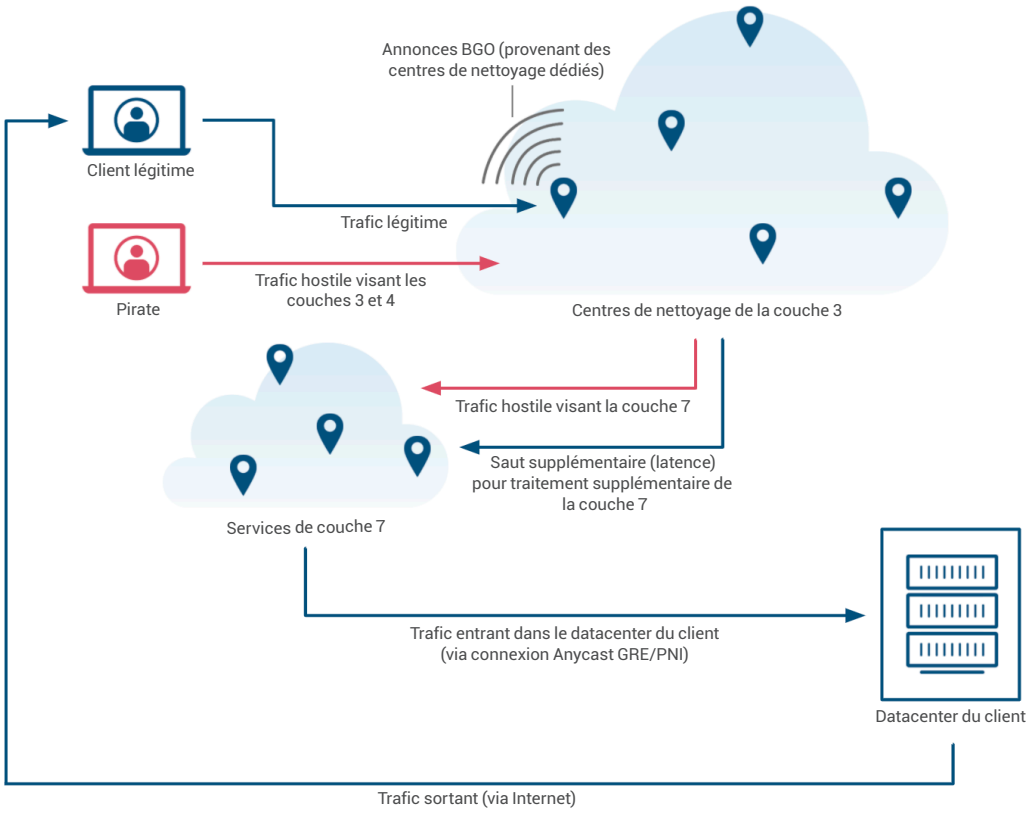
Dans une certaine mesure, les équipements physiques protègent efficacement votre infrastructure. Ces appareils disposent toutefois d'une bande passante limitée et peuvent se voir submergés en cas d'attaques de grande ampleur ou simultanées. Ils nécessitent également un investissement initial considérable, ainsi que la mobilisation de nombreuses ressources pour leur gestion et leur maintenance.

L'apparition des centres de nettoyage dans le cloud (ou « scrubbing centers ») a apporté une solution plus simple : le routage du trafic vers ces centres, qui filtrent et éliminent le trafic hostile. Cette approche a ainsi permis d'alléger le fardeau financier et de résoudre les problèmes de maintenance associés aux appareils sur site.

Toutefois, elle a également engendré un nouveau problème : un temps de latence non négligeable.

L'arsenal de centres de nettoyage des fournisseurs cloud étant limité et géographiquement dispersé, le trafic peut être amené à effectuer de grands détours pour se faire nettoyer avant d'atteindre sa destination finale. Les fournisseurs cloud ne disposent généralement que d'une poignée de centres de nettoyage. Aussi, si vous ou vos utilisateurs finaux en êtes éloignés, votre trafic devra circuler sur de longues distances, quand bien même sa destination finale serait très proche. C'est ce qu'on appelle l'effet trombone, source de retards perceptibles et préjudiciables (le nom « effet trombone » vient d'ailleurs de la ressemblance entre le tracé de l'itinéraire sur une carte et la forme d'un trombone).

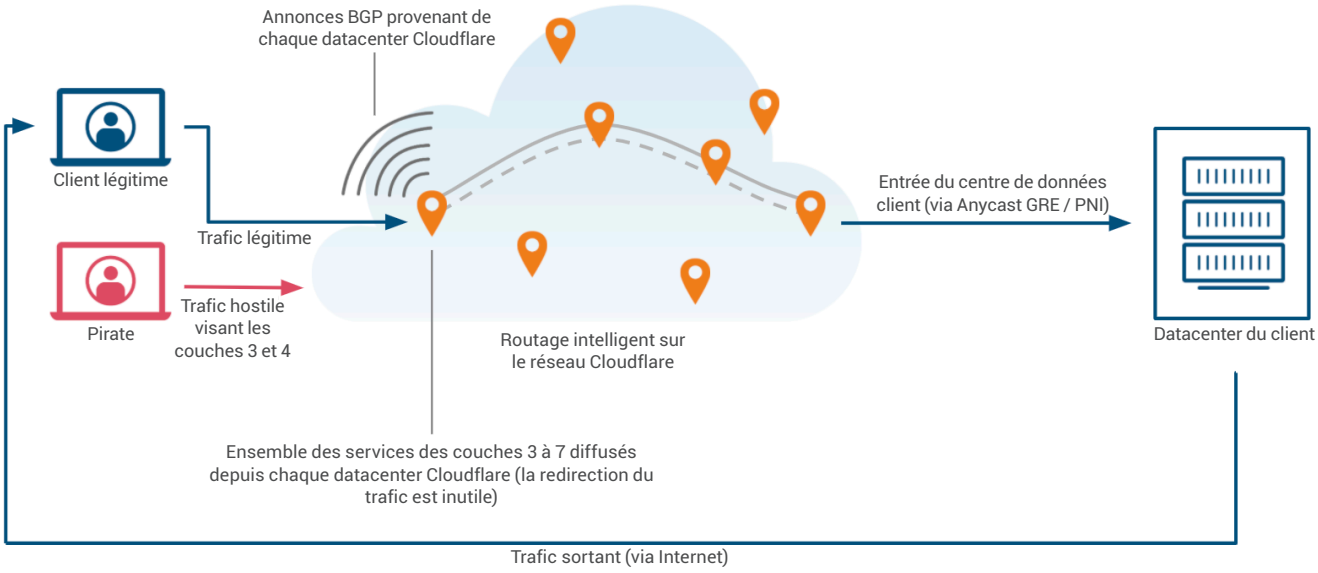
Les « scrubbing centers » (ou centres de nettoyage) sont peu nombreux, éloignés et dédiés à l'atténuation des attaques DDoS. Le trafic réseau doit être dirigé vers un autre datacenter afin de subir un traitement complémentaire des couches 4 à 7, entraînant ainsi un délai supplémentaire.



Dans le scénario ci-dessus, imaginons que vous avez besoin de faire nettoyer le trafic des couches 3 et 4, ainsi que celui des services de la couche 7 (par ex. un pare-feu WAF, une solution de gestion de bots, etc.). Dans ce cas, votre trafic atteint tout d'abord un centre de nettoyage éloigné dédié à l'atténuation des attaques DDoS sur la couche 3, avant d'être ensuite envoyé vers un datacenter secondaire pour subir un traitement supplémentaire de la couche 7. Ce cheminement ajoute un saut réseau au trafic de bout en bout et génère une latence inutile. La latence est particulièrement prononcée si le fournisseur cloud dispose d'un nombre limité de centres de nettoyage et si la source de votre trafic réseau en est éloignée.

Magic Transit offre une meilleure solution. Au lieu de prévoir des centres de nettoyage dédiés, nous permettons à tous les datacenters du réseau mondial de Cloudflare de se charger du nettoyage. En fait, chaque datacenter Cloudflare exécute l'ensemble des services Cloudflare. Votre trafic n'a ainsi besoin que de rejoindre le datacenter Cloudflare le plus proche. Comme notre réseau se compose de datacenters présents dans plus de 200 villes et répartis dans plus de 100 pays, il est fort probable que la distance sera courte.

Chaque datacenter Cloudflare exécute l'ensemble des services des couches 3 à 7, de sorte que le trafic réseau est traité au même endroit

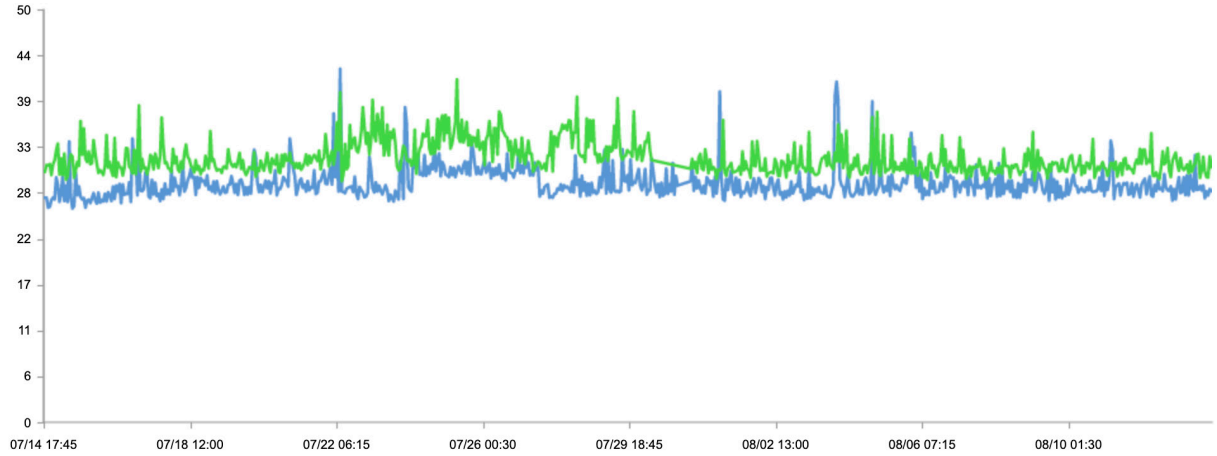


L'effet trombone est ainsi éliminé et la latence générée, minime. Les performances du réseau constituaient l'une de nos principales préoccupations lors du développement de Magic Transit, car nous souhaitions nous assurer que nos utilisateurs n'aient pas à sacrifier ces dernières au nom de la sécurité.

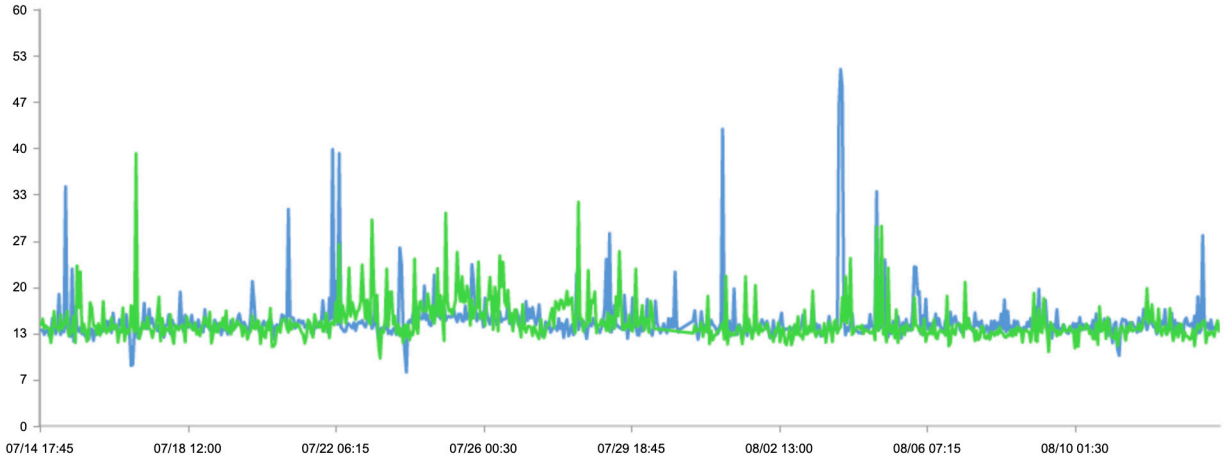
Tests Catchpoint

Pour contrôler ce résultat, nous avons eu recours à Catchpoint afin de conduire des tests visant à déterminer les effets de l'utilisation de Magic Transit sur les performances générales du réseau. Avec des sondes réparties dans le monde entier, nous avons effectué des tests ping ICMP vers deux adresses IP hébergées au sein de la même infrastructure réseau : l'une protégée par Magic Transit, l'autre non. Nous avons ainsi pu mesurer simultanément la latence, la quantité de paquets perdus et la gigue pour chaque adresse, afin de révéler les différences en termes de performances.

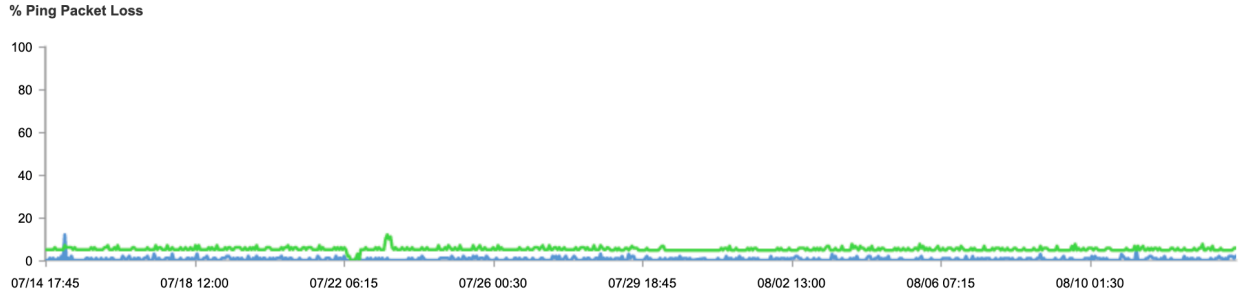
Performances en matière de latence (délai de réponse à la commande ping, exprimé en ms) avec Magic Transit (bleu) et sans Magic Transit (vert)



Performances en matière de gigue (exprimée en ms) avec Magic Transit (bleu) et sans Magic Transit (vert)



Performances en matière de quantité de paquets perdus (exprimée en pourcentage) avec Magic Transit (bleu) et sans Magic Transit (vert)



Dans le test illustré ci-dessus, la ligne bleue représente les performances constatées lors de l'utilisation de Magic Transit et la ligne verte les performances observées sans Magic Transit.

Résultats du test :

Performances étudiées	Avec Magic Transit (bleu)	Sans Magic Transit (vert)
Latence	28,96 ms	31,98 ms
Gigue	15,61 ms	15,24 ms
Quantité de paquets perdus	0,52 %	5,26 %

Principales conclusions de ces tests :

- La latence a diminué de 3 ms avec Magic Transit
- La gigue a augmenté de 0,36 ms avec Magic Transit
- La quantité de paquets perdus était quasiment nulle (0,52 %) avec Magic Transit, alors qu'elle était de 5,26 % sans Magic Transit

Que faut-il retenir de ces résultats ?

Latence : la latence correspond au temps nécessaire pour que les paquets de données se déplacent d'un point à un autre du réseau. Au cours de nos tests, nous avons observé une latence inférieure sur le réseau de Cloudflare.

Cloudflare optimise en permanence les itinéraires du trafic en fonction de l'état des différents chemins réseau, de sorte que les chemins empruntés par les paquets du réseau de Cloudflare vers le réseau du client sont souvent plus efficaces que ceux qu'ils suivraient sans l'optimisation de Cloudflare.

Ce processus permet de s'assurer que la latence du réseau n'augmente pas. D'ailleurs, comme l'indiquent les résultats de nos tests, elle s'en trouve même réduite dans de nombreux cas. Il s'agit d'une garantie particulièrement importante pour les applications sensibles à la latence (en temps réel), comme les jeux vidéo en ligne et les applications de voix sur IP (VoIP).

Gigue : la gigue du réseau correspond à l'intervalle entre les livraisons de paquets sur un réseau. Il est essentiel de maintenir le niveau de la gigue faible pour les applications telles que la VoIP. Avec Magic Transit, la gigue a augmenté de 0,36 ms, soit un niveau considéré comme négligeable, même pour les applications qui y sont sensibles.

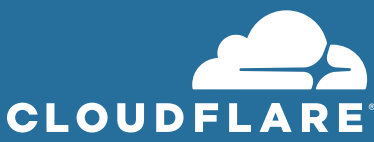
Perte de paquets : il y a perte de paquets lorsqu'un ou plusieurs des paquets d'une transmission réseau n'atteignent pas leur destination. En fonction du protocole, la perte de paquets entraîne un allongement de la retransmission ou une dégradation de la qualité. Pour les transmissions particulièrement sensibles aux délais, comme la vidéoconférence, une quantité de paquets perdus inférieure à 1 % est considérée comme acceptable*. Lors de nos tests, nous avons constaté que la quantité de paquets perdus était descendue à presque zéro sur le réseau de Cloudflare (alors qu'elle était de plus de 5 % sans Magic Transit).

En résumé, les effets de Magic Transit sur la latence, la gigue et la quantité de paquets perdus n'altéreront en rien l'expérience de l'utilisateur, qui devrait d'ailleurs constater une amélioration dans de nombreux cas. En d'autres termes, les clients de Cloudflare n'ont pas à s'inquiéter de devoir « faire des concessions » sur les performances du réseau s'ils ont recours à Magic Transit.

En outre, la solution Magic Transit s'intègre à l'ensemble des produits Cloudflare consacrés à l'amélioration de la sécurité, des performances et de la fiabilité, dont la finalité est d'optimiser toujours plus les propriétés Internet.

Pour plus d'informations sur Cloudflare Magic Transit, rendez-vous sur www.cloudflare.com/fr-fr/magic-transit/ ou contactez-nous à l'adresse suivante : sales@cloudflare.com

* https://web.archive.org/web/20131010010244/http://sdu.ictp.it/pinger/pinger.html



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

RÉV. : 27 AOÛ 2020