CLOUDFLARE®

Restez à la pointe

Amélioration des performances et de la sécurité de votre site de commerce en ligne pour les consommateurs mobiles

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/fr

Résumé

La technologie mobile est arrivée à un moment charnière : elle est en passe de devenir la pierre angulaire des stratégies de commerce en ligne. Aux États-Unis, 25 % des principaux détaillants en ligne ont déjà compris comment augmenter les taux de conversion mobiles pour s'approprier d'énormes parts de marché, dans une course où règne la loi du tout ou rien. Pour fidéliser les consommateurs et augmenter la visibilité des produits, ils utilisent des sites et applications mobiles rapides et toujours disponibles. Cloudflare peut vous aider à atteindre ces exigences stratégiques en vous offrant :

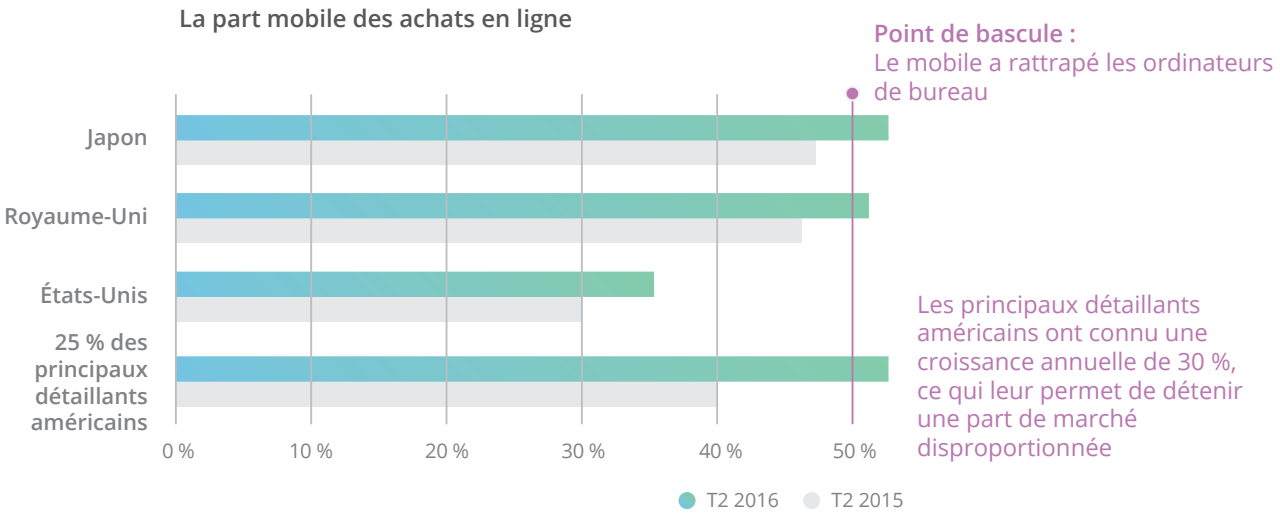
- L'un des réseaux de distribution du contenu (CDN) les plus rapides, fondé sur le routage Anycast et la possibilité de mettre du contenu en cache à proximité des consommateurs pour réduire la latence
- Une tarification fixe et sans surprise
- Optimisation mobile des images et du code, et prise en charge de IPv6 pour réduire la latence sur les appareils mobiles
- Protection contre les attaques DDoS visant les couches 3, 4 et 7, et contre les vulnérabilités d'application de la couche 7 pour augmenter le temps d'activité
- Chiffrement efficace et hautes performances

Pour les détaillants en ligne, installer Cloudflare pour accéder à ces fonctionnalités représente une progression de taille en vue de rendre leurs sites rapides et sûrs à tout moment.

Le commerce mobile est à un moment charnière

Le commerce en ligne est très prometteur : avec une croissance annuelle de 14,6 % en 2015 (et un bond de 36,2 % des ventes au détail aux États-Unis la même année), il a largement dépassé les magasins physiques en termes de croissance. Plus prometteur encore : le commerce mobile connaît une croissance encore plus rapide et se trouve véritablement à un moment charnière. Pour la première fois, au deuxième trimestre de 2016, la part mobile de l'e-commerce a dépassé les 50 % au Japon et au Royaume-Uni, devançant les ordinateurs de bureau. Aux États-Unis, cette part augmente aussi à grande vitesse, avec une croissance annuelle de 17 %. À ce rythme, même si le commerce mobile ne représente que 35 % des ventes au détail du pays, les États-Unis devraient combler leur retard et rattraper les pays en tête.

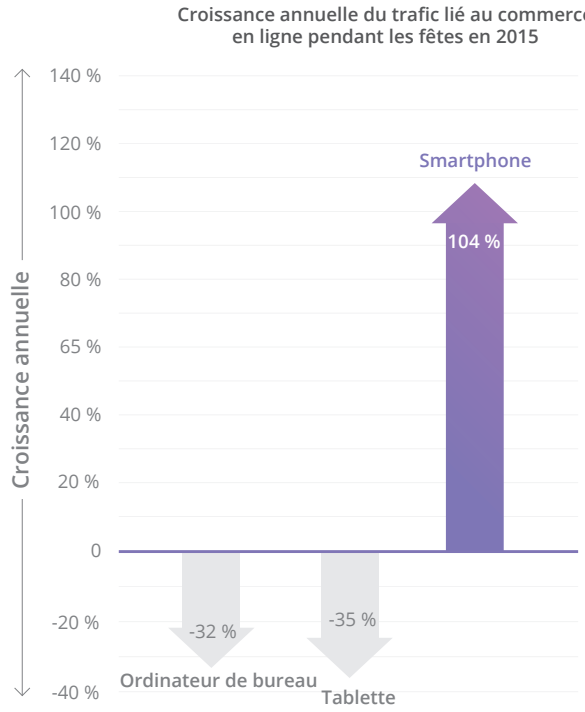
Le quartile des détaillants américains affichant les meilleurs résultats profite déjà de cette tendance en proposant des sites et applications de qualité. Ils parviennent à fidéliser les consommateurs et à augmenter la visibilité de leurs produits, sans compter que leurs taux de conversion sont jusqu'à 90 % supérieurs aux chiffres de la plupart des nouvelles entreprises. Ils s'approprient par conséquent le marché mobile, qui représente 52 % de leurs ventes en ligne et continuent de se développer avec une croissance époustouflante de 30 % par an.

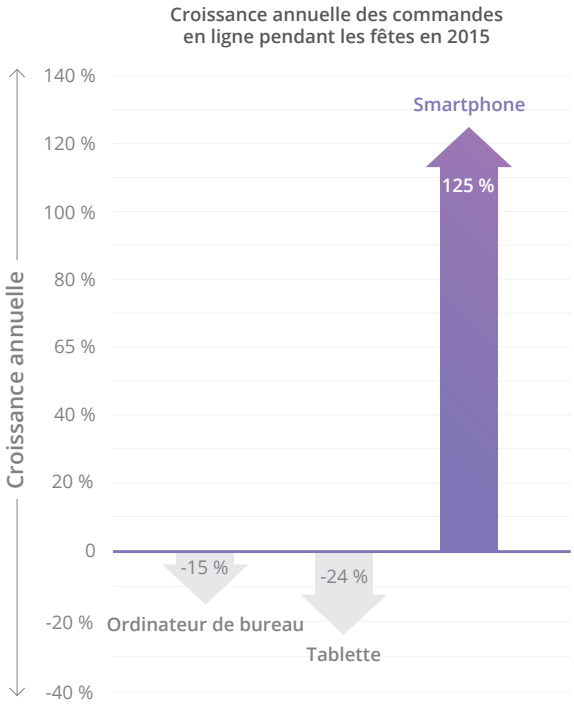


Le commerce en ligne est sans conteste devenu un enjeu stratégique de taille pour la vente et le marketing. Les détaillants qui offrent la meilleure expérience mobile l'emportent et peuvent compter sur une part de marché toujours plus importante.

La technologie mobile est d'une importance critique pendant les fêtes

Les soldes de fin d'année en ligne (Cyber 5) ont battu tous les records en 2015 : le Cyber Monday a remporté la palme, car c'est lors de cette journée qu'ont été enregistrées la majorité des dépenses en ligne de toute l'histoire américaine. Les smartphones ont joué un rôle extrêmement important, car c'est de ces appareils que provenaient 49 % du trafic et 27 % des commandes. Le trafic et les commandes issus de smartphones ont connu une croissance exceptionnelle, au détriment du trafic/des commandes depuis des ordinateurs de bureau ou tablettes, qui ont diminué proportionnellement.

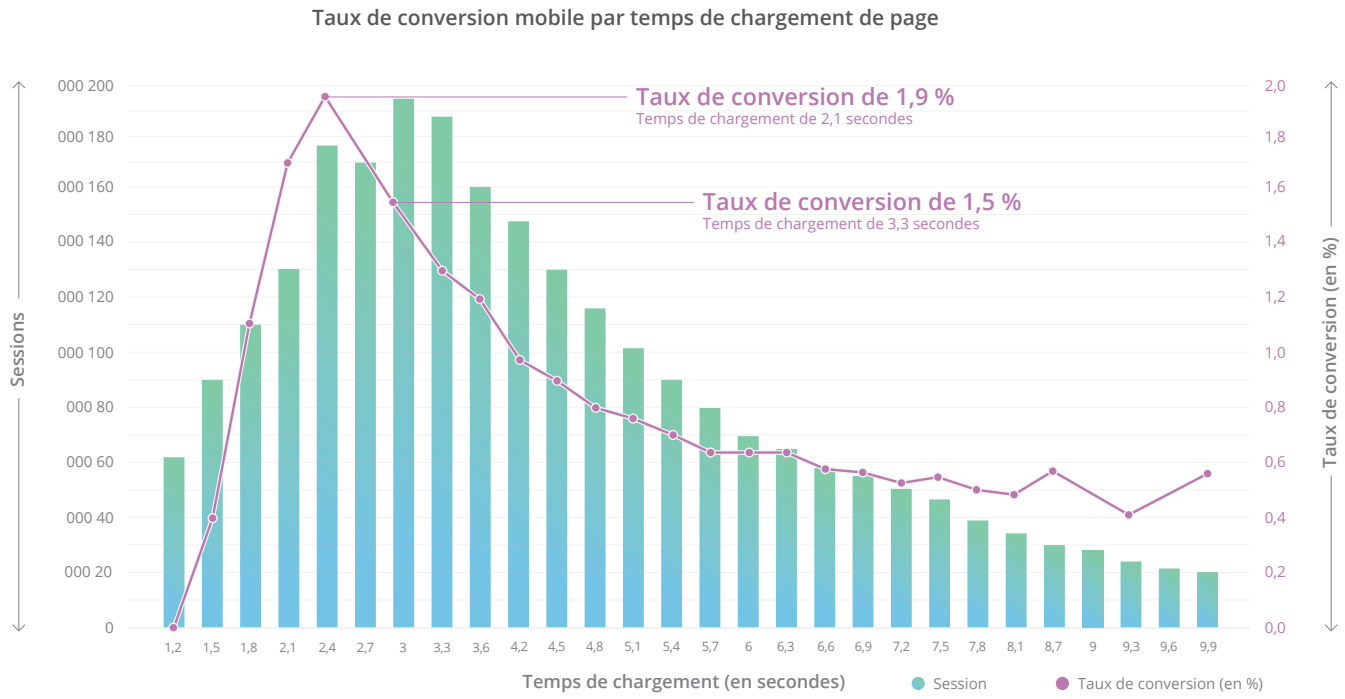




La période Cyber 5 de 2015 est une nouvelle preuve que les détaillants qui offrent les meilleures expériences mobiles s'approprient la plus grande part du gâteau. À titre d'exemple, Amazon a connu une croissance de 24,1 % pendant le Cyber 5 2014-2015. Cette année, à la saison des fêtes, les entreprises « Brick and Click » auront certainement plus d'afflux en ligne qu'en magasin. L'expérience d'achat mobile représente donc un enjeu majeur pour la croissance.

L'influence de la latence et de la disponibilité sur les taux de conversion

Comment se démarquer du lot ? Les principaux détaillants en ligne offrent les meilleurs sites et applications mobiles pour augmenter leurs taux de conversion. Les taux de conversion sur mobile sont encore bas et ils sont étroitement liés aux performances et à la disponibilité des sites et applications mobiles. À titre d'exemple, le taux de conversion de l'un des leaders du commerce en ligne a atteint 1,9 % avec un temps de chargement moyen de 2,4 secondes par page. À 3,3 secondes, soit à peine une seconde de plus, le taux de conversion chutait de 27 %.

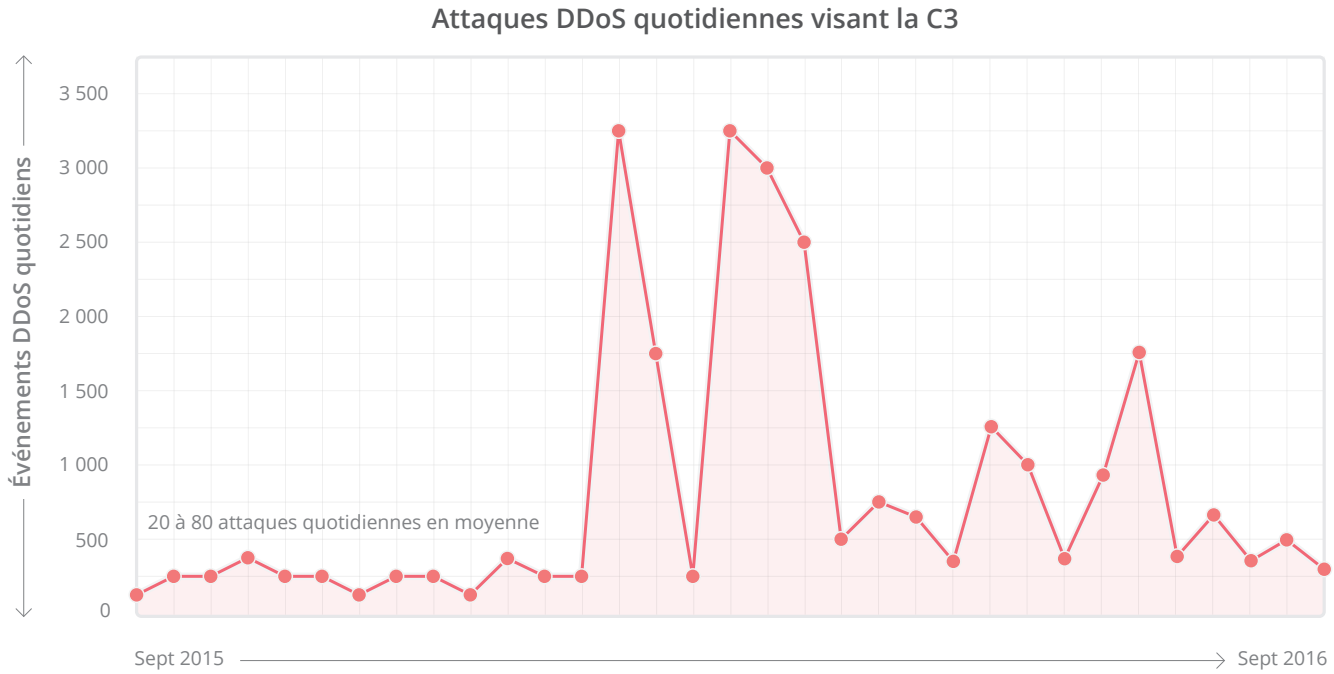


De nombreux exemples concrets illustrent le lien entre les performances et le taux de conversion d'un site

- Les revenus d'Amazon augmentent de 1 % pour chaque réduction de 100 ms de la latence du site
- Les revenus de Yahoo augmentent de 9 % pour chaque réduction de 400 ms de la latence du site
- Walmart a subi une chute de ses taux de conversion quand le temps de chargement de son site est passé de 1 à 4 secondes

De manière générale, Google constate qu'une latence de 100 à 400 ms influence grandement le comportement des consommateurs en ligne, et qu'un site 250 ms plus lent que le site d'un concurrent sera moins souvent visité.

En plus de la latence causée par les sites/les applications, les attaques par déni de service (DDoS) peuvent rendre un site complètement indisponible. Avec près de 10 % du trafic Internet mondial circulant par ses réseaux, Cloudflare peut filtrer et évaluer avec précision les attaques. L'année dernière, Cloudflare a vu les attaques augmenter en nombre et en intensité, avec jusqu'à 1 400 attaques DDoS par jour, des pics de trafic entrant à 400 Gbit/s et des attaques à 200 millions de paquets par seconde.



Ces attaques sont rarement des événements isolés, et les victimes sont généralement ciblées plusieurs fois sur une année. L'expérience de Cloudflare montre qu'elles peuvent viser n'importe qui, tant les petites organisations que les grandes. Malgré l'illégalité des attaques DDoS dans de nombreuses législations, il existe des fournisseurs de services DDoS, proposant des abonnements à partir de 5 à 10 $ par mois pour certains.

Même le site d'Amazon (99 milliards de dollars de revenus en 2015) a subi plusieurs dysfonctionnements inexplicables par le passé. En 2013, par exemple, Amazon.com est resté indisponible pendant environ 15 à 45 minutes, coûtant entre 1,8 et 5,3 millions de dollars de ventes perdues, d'après des estimations basées sur le revenu moyen du groupe (117 882 $ par minute). Pendant la période des fêtes, le coût relatif au temps d'inactivité peut être bien plus élevé en raison du caractère saisonnier du commerce. Par exemple, Amazon a réalisé 33 % de ses bénéfices annuels sur le dernier trimestre de 2015. Les autres effets négatifs des temps d'inactivité comportent notamment l'impact sur la satisfaction client, la visibilité sur les moteurs de recherche et les relations avec les investisseurs.

En bref, pour les détaillants en ligne qui veulent augmenter leurs taux de conversion, en particulier pendant les fêtes, il est impératif de proposer des sites/applications rapides et protégés contre les attaques DDoS afin d'améliorer le temps d'activité.

Des technologies essentielles pour des sites mobiles rapides et sûrs

Cloudflare peut vous aider à accélérer et protéger vos sites et applications de commerce mobile sans que vous ne deviez ajouter de matériel, installer de logiciels ni modifier la moindre ligne de votre code.

La première étape consiste à utiliser le réseau de distribution du contenu (CDN) de Cloudflare. Il s'agit de l'un des plus grands réseaux existants, qui traite plus de 10 billions de requêtes par mois. Cela représente environ 10 % de l'ensemble des requêtes sur Internet, pour plus de 2,5 milliards de personnes partout dans le monde. Selon Cedexis, le CDN de Cloudflare conserve une place confortable parmi les CDN les plus rapides, avec un temps de réponse médian de 34 ms (aux États-Unis). Ses fonctionnalités principales incluent :

Routage basé sur Anycast

Le CDN de Cloudflare utilise un routage de type Anycast, tandis que la majorité d'Internet fonctionne encore avec un mécanisme appelé Unicast. Sous Unicast, chaque nœud du réseau dispose d'une adresse IP unique. Les routeurs possèdent une carte des adresses IP du monde entier et calculent le chemin le plus court à travers les nombreux sauts à effectuer pour arriver à destination. Cependant, la destination finale peut se trouver à l'autre bout du continent ou du monde, nécessitant des sauts supplémentaires qui augmentent un peu plus la latence. Sous Anycast, le schéma de routage utilisé par Cloudflare, plusieurs machines du réseau CDN partagent la même adresse IP, ce qui permet aux routeurs d'envoyer le contenu au serveur le plus proche et de réduire la latence.

Mise en cache du contenu

Le réseau Anycast de Cloudflare fonctionne en association avec la mise en cache du contenu. Une fois qu'Anycast a acheminé une requête vers le serveur le plus proche, une copie du contenu en cache est disponible sur celui-ci. La mise en cache a l'avantage de permettre de déplacer les objets au plus près des visiteurs qui en demandent l'accès et d'en accélérer la distribution, mais aussi de diminuer la charge sur le serveur Web d'origine. Cloudflare offre des fonctionnalités de mise en cache automatique du contenu statique ; et avec Railgun, Cloudflare permet également de mettre en cache le contenu dynamique.

Cloudflare analyse le trafic acheminé par les serveurs du CDN pour identifier les portions statiques du site d'origine. Le contenu statique est alors mis en cache dans le CDN pour une courte période. Environ 66 % du contenu Web peut être mis en cache (via la « mise en cache automatique du contenu statique »), les 34 % restant ne le sont pas et doivent être obtenus à partir du serveur d'origine. Railgun est conçu pour accélérer l'acheminement du contenu qui ne peut pas être mis en cache ; pour permettre à tout Internet de pouvoir être mis en cache, en quelque sorte. Les pages qui ne peuvent pas être mises en cache ne changent pas très rapidement, et les petits changements entre différentes versions de pages Web peuvent être identifiés par les serveurs du CDN de Cloudflare. Cloudflare compresse alors ces changements, à un taux de compression atteignant 99,6 %, et les envoie à travers le lien, pour une amélioration jusqu'à 700 % des performances. Railgun nécessite l'installation d'une composante logicielle sur le serveur d'origine.

> « Avec l'augmentation des coûts de bande passante, bénéficier d'un CDN comme Cloudflare, qui dessert les images en périphérie à ses utilisateurs, c'est très rentable et ça permet de réduire lalatence pour nos clients mobiles »
>
> Chris Smith, Directeur du commerce en ligne, Big 5 Sporting Goods

Tarification stable

Pour faire partie d'Internet, Cloudflare achète de la bande passante, également appelée transit, à un certain nombre de fournisseurs différents. Cloudflare achète le transit en gros en fonction du volume utilisé en un mois donné, en payant pour une utilisation maximale sur une période définie. Les sommes que Cloudflare débourse peuvent varier considérablement de région en région, mais dans une volonté de simplifier sa tarification, Cloudflare propose ses services à un prix fixe, peu importe où le trafic doit être distribué sur la planète. À la différence de certains services cloud qui facturent leurs clients pour chaque bit acheminé à travers un réseau, avec Cloudflare, il n'y a pas de surprise à la fin du mois. Cloudflare poursuit ses efforts pour diminuer le prix du transit au profit du peering afin d'offrir les meilleurs services au prix le plus bas.

Optimisation des images et du code

Avec Polish, Mirage et Auto-Minify, Cloudflare porte un triple coup à la latence. Ces fonctionnalités sont particulièrement importantes pour les appareils mobiles, qui ont une bande passante limitée.

Polish supprime les métadonnées et compresse les images pour réduire leur taille. Il peut être exécuté en mode Lossless (sans pertes), supprimant les informations inutiles sans toucher aux données de l'image elle-même. La taille des images est réduite de 21 % en moyenne. Polish peut également être exécuté en mode Lossy (avec pertes), similaire au mode Lossless, mais qui applique en plus un algorithme de compression aux images compatibles. Visuellement, les images sont identiques avant et après, mais leur taille est diminuée de 48 % en moyenne. En général, les images représentent plus de 50 % des données d'un site.

Mirage gère le chargement des images sur les appareils mobiles. Il génère rapidement l'apparence d'une page utilisable avec laquelle l'utilisateur peut interagir, tout en complétant le reste de la page sans perturber l'expérience utilisateur.

- Mirage utilise le lazy loading pour charger en priorité les images qui seront affichées à l'ouverture de la page. Il charge ensuite les autres images de la page, qui se trouvent en dehors de l'affichage du navigateur, selon leur nécessité ou en fonction des ressources réseau disponibles.
- Étant donné leur taille réduite, les appareils mobiles nécessitent de plus petites images. Mirage réduit les images sur le serveur jusqu'à 1 % de leur résolution totale et envoie l'image en taille réduite en premier lieu. Une fois la page affichée avec les images réduites, celles-ci sont remplacées par leur version en pleine résolution. Les images apparaissent donc d'abord en faible résolution, puis retrouvent leur qualité d'origine.
- Au lieu d'envoyer une nouvelle requête pour chaque image, Mirage achemine les images depuis le réseau Cloudflare en une seule requête. Par conséquent, même une page avec des centaines d'images commencera à s'afficher après seulement deux requêtes. Les utilisateurs qui ne bénéficient pas de connexions mobiles rapides peuvent eux aussi commencer à interagir immédiatement avec la page sans devoir attendre le chargement des images en pleine résolution.

Auto-Minify élimine au vol tous les caractères inutiles (p. ex. les « whitespaces ») des fichiers HTML, JavaScript et CSS, économisant ainsi 20 % de la taille du fichier sans rien changer à ses fonctionnalités. La mise en œuvre d'Auto-Minify par Cloudflare est aisément 100x plus rapide que n'importe quelle approche équivalente.

Prise en charge de IPv6

Les analyses Real User Monitoring menées par Facebook et LinkedIn montrent que les temps de chargement des pages pour mobiles sont 10 % plus rapides avec IPv6 qu'avec IPv4 sur les quatre réseaux mobiles les plus importants des États-Unis. Et même si le IPv6 existe déjà depuis plusieurs dizaines d'années et est réputé lent, environ 60 % des requêtes Android et plus de 20 % des requêtes iPhone envoyées depuis les quatre réseaux mobiles les plus importants des États-Unis utilisaient IPv6 sur les sites en Dual-Stack (à la date du 04/05/2016). En plus de la prise en charge totale de IPv6 et d'une passerelle IPv6-to-IPv4 depuis 2012, Cloudflare a également rendu ces services accessibles en un clic. Si le serveur d'origine prend en charge IPv6, les visiteurs entrant avec une connexion IPv6 seront entièrement acheminés via le protocole. Si le serveur d'origine ne prend que IPv4 en charge, Cloudflare acceptera le visiteur en IPv6, puis enverra une requête au serveur en IPv4. Par ailleurs, si, sur le serveur d'origine, une application nécessite obligatoirement IPv4 pour s'exécuter, Cloudflare fournit un Pseudo IPv4. Une fois activée, chaque fois qu'une connexion est établie en IPv6, cette option ajoute un en-tête HTTP à la requête avec une « pseudo » adresse IPv4.

Protection contre les attaques DDoS visant les couches 3 et 4 : résilience du réseau Anycast avec plate-forme à auto-apprentissage

L'étape suivant l'utilisation du réseau de distribution du contenu (CDN) de Cloudflare est la protection des sites/applications contre les attaques malicieuses afin de garantir le temps d'activité. La protection avancée de Cloudflare contre les attaques DDoS prend la forme d'un service à la périphérie du réseau. Il égale les menaces en complexité et en ampleur, et peut être utilisé pour atténuer les attaques DDoS de toutes formes et de toutes tailles. Cloudflare a empêché plusieurs des attaques par déni de service les plus importantes, dont certaines atteignaient plus de 400 Gbit/s.

Les attaques DDoS contre les couches 3 et 4 sont généralement des attaques volumétriques de type amplification, flood et flood SYN. Redoutables pour un réseau basé sur Unicast, ces attaques sont atténuées par le réseau Anycast de Cloudflare. Il augmente en effet naturellement leur surface en dispersant le trafic hostile vers la centaine de datacenters Cloudflare et à travers plusieurs connexions à large bande passante avec d'autres réseaux, pour absorber l'attaque. En outre, Cloudflare fournit une plate-forme à auto-apprentissage, sur laquelle le trafic est analysé en temps réel afin d'identifier les anomalies ou les requêtes malicieuses. Dès qu'une nouvelle attaque est identifiée, Cloudflare bloque automatiquement ce type d'attaque pour le site Web concerné, mais aussi pour toute la communauté.

Même d'un point de vue financier, les attaques n'affectent habituellement pas Cloudflare : Cloudflare achète de grandes quantités de bande passante en gros et paie pour la moyenne la plus élevée du trafic entrant ou sortant sur un mois. Étant donné que Cloudflare fait office de proxy pour la mise en cache, le trafic sortant est toujours plus important que le trafic entrant, de 4 à 5 fois en général. Lors d'une attaque, les deux valeurs sont plus proches, mais il est rare qu'une attaque soit suffisamment importante pour occasionner des frais supplémentaires de bande passante pour Cloudflare. Les clients de Cloudflare profitent de cet avantage, et leur facture ne s'alourdit pas en cas d'augmentation du trafic causée par une attaque DDoS.

Étant donné que Cloudflare continue de développer son réseau et sa communauté, il devient de plus en plus difficile de lancer une attaque DDoS efficace contre les utilisateurs de Cloudflare.

Protection de la couche 7 : limitation du débit avec base de données de réputation IP

Tout comme les attaques volumétriques contre les couches 3 et 4, les attaques par déni de service contre la couche 7 emploient de gros volumes de requêtes pour empêcher les utilisateurs d'accéder à un site Web. Lors des attaques DDoS contre la couche 7, une adresse IP unique envoie de grandes quantités de requêtes semblables au trafic normal non malicieux. C'est pourquoi il est difficile de s'en protéger.

Le Traffic Protector de Cloudflare (actuellement disponible via le programme d'accès anticipé) surveille le nombre de requêtes envoyées par chaque adresse IP vers un site et identifie les sites qui ont trop de requêtes par minute. Une fois l'adresse IP suspecte identifiée, le trafic de cette adresse passe par une page interstitielle pendant environ 5 secondes, le temps d'effectuer une série de vérifications mathématiques. Si les requêtes échouent à la vérification, Traffic Protector fait baisser la réputation de l'IP et le trafic de cette adresse sera redirigé vers une page CAPTCHA à chaque nouvelle tentative d'accès.

Quand Cloudflare identifie une adresse IP qui semble faire des requêtes malicieuses, celle-ci est enregistrée dans la base de données de réputation IP de Cloudflare. En fonction du niveau de menace évalué, une requête est soit acceptée, soit testée par CAPTCHA. Si le CAPTCHA échoue et que l'adresse IP est identifiée comme malicieuse, la requête est bloquée à la périphérie de la totalité du réseau Cloudflare, protégeant l'ensemble de la communauté Cloudflare.

Attaque non-DDoS contre les vulnérabilités d'application de la couche 7 : pare-feu applicatif Web (WAF)

Les attaques contre la couche 7 sont les types d'attaques les plus sophistiquées et les plus complexes. En imitant l'utilisation normale d'une application, elles sont capables d'échapper à la plupart des mesures d'atténuation DDoS et des services de protection des vulnérabilités. Parmi ces attaques, on retrouve communément les injections SQL et les attaques de type Cross-Site Scripting (XSS), qui permettent aux pirates d'accéder aux données des clients ou de n'importe quel type d'application, et de les modifier.

Cloudflare répond à ces menaces grâce à son pare-feu applicatif Web (WAF). Le pare-feu applicatif met en application l'ensemble de règles OWASP Core Rule Set, des règles à action immédiate fournies par Cloudflare, ainsi que des règles personnalisées créées par la communauté ou les clients. Chaque nouvelle règle publiée par Cloudflare se propage à tous les nœuds des serveurs Cloudflare en moins de 30 ms, et le pare-feu applicatif n'ajoute pas plus de 1 ms de latence, ce qui garantit un niveau de sécurité sans compromis sur les performances. De cette manière, Cloudflare est à même de protéger ses clients contre les principales vulnérabilités Zero-Day, dont les failles Shellshock et Heartbleed Bug.

> « Nous prenons les attaques DDoS très au sérieux. Mais même lorsque nous en avons été victimes, Cloudflare a rapidement été en mesure de protéger notre domaine, garantissant une expérience ininterrompue pour nos utilisateurs. Pour nous, le principal avantage de Cloudflare, c'est cette tranquillité d'esprit : quelqu'un surveille le réseau et vous donne les moyens d'atténuer n'importe quelle attaque. »
>
> Chris Smith, Directeur du commerce en ligne, Big 5 Sporting Goods

TLS 1.3 et HTTP/2 avec Server Push

Le chiffrement est essentiel pour proposer une expérience d'achat digne de confiance. Les dernières améliorations du protocole SSL permettent justement d'effectuer un chiffrement de qualité et d'améliorer les performances. Transport Layer Security 1.3 (TLS) élimine non seulement les fonctionnalités moins stables présentes dans les versions précédentes, mais cette version réduit aussi la latence en divisant la distance parcourue du protocole par deux. Cloudflare a déployé TLS 1.3 en premier et a largement contribué à sa qualité. Cloudflare a également déployé en premier HTTP/2, qui fonctionne uniquement avec TLS. HTTP/2 améliore les performances, notamment la latence, et le résultat est perceptible pour un utilisateur final lorsqu'il utilise un navigateur. HTTP/2 fonctionne parallèlement avec Server Push, qui permet à un serveur d'envoyer au client des ressources qu'il n'a pas encore demandées afin d'accélérer encore les performances perçues. TLS 1.3 et HTTP/2 avec Server Push sont deux exemples parmi d'autres des efforts constamment déployés par Cloudflare pour intégrer les nouvelles technologies à son réseau.

Conclusions

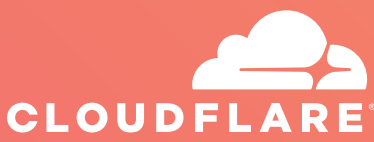
Inscrivez-vous à Cloudflare pour améliorer les performances de vos sites et applications mobiles tout en les protégeant des attaques DDoS et des vulnérabilités d'applications. L'installation est simple et ne prend que 5 minutes. Consultez nos offres, de l'offre Gratuite à l'offre Entreprise, sur www.cloudflare.com/fr.

Contactez-nous pour en savoir plus sur Cloudflare.

www.cloudflare.com/fr

enterprise@cloudflare.com

1 888 99 FLARE



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/fr