LIVRE BLANC

Optimiser les performances et la sécurité des sites web en Chine

Stratégies pour s'engager sur le marché Internet en Chine et prendre part à une économie colossale, complexe et dynamique

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

Résumé

La Chine abrite la plus vaste population d'utilisateurs d'Internet du monde. Cependant, la complexité de son réseau et la menace permanente des cyberattaques peuvent rendre difficile l'exploitation de ce marché. Pour aider les entreprises à surmonter ces obstacles et à optimiser au mieux l'expérience que proposent leurs sites web aux utilisateurs en Chine, Cloudflare a étendu à la Chine ses services mondiaux de performance et de sécurité des réseaux.

Les entraves à l'expansion d'une activité en ligne en Chine

La vaste et dynamique économie en ligne de la Chine fait de cette nation un marché attrayant pour de nombreuses entreprises différentes. Plus d'un milliard de citoyens chinois sont connectés à Internet, formant la plus vaste population d'internautes du monde, et plus de 812 millions de ces utilisateurs ont effectué un achat en ligne au cours du premier semestre de 2021. Les dépenses en ligne globales ont quelque peu reculé pendant cette période par rapport aux années précédentes, notamment en raison de l'instabilité économique générale due à la pandémie de Covid-19. Néanmoins, l'économie chinoise a connu une croissance à deux chiffres pendant l'après-Covid, tandis que le marché de l'e-commerce a progressé de 12,5 % en 2020.

À l'instar de tout marché régional, les entreprises mondiales présentes en Chine doivent adapter leurs services et leurs expériences en ligne pour satisfaire aux attentes locales. Malheureusement, les réglementations chinoises en matière d'Internet, l'infrastructure sous-jacente et le contexte des menaces se traduisent par un certain nombre de difficultés uniques pouvant compliquer la tâche des entreprises mondiales désireuses de proposer des expériences d'une qualité conforme aux attentes des consommateurs locaux. Ces difficultés concernent notamment :

- La latence due à la fragmentation des réseaux et à l'insuffisance des interconnexions locales
- Les compromis en matière de performances des sites web mobiles
- Les cyberattaques nationales persistantes

Ce document présente ces difficultés dans le détail, décrit les stratégies à mettre en place pour les surmonter et explique comment Cloudflare peut vous y aider.

La latence due à la fragmentation des réseaux et à l'insuffisance d'interconnexions locales

Comme de nombreux consommateurs, les Chinois ont des attentes élevées concernant les expériences en ligne. Selon le rapport de HSBC, la Chine mène et domine le marché de l'e-commerce dans le monde entier et, selon l'analyse de business.com, elle est identifiée comme le plus grand marché d'e-commerce dans le monde par pays.

Malheureusement, il est souvent difficile pour les entreprises de garantir aux utilisateurs en Chine un fonctionnement fiable et rapide de leurs sites.

Les goulets d'étranglement du réseau figurent parmi les causes de ces difficultés. Tout le trafic Internet circulant en provenance et à destination de la Chine transite par l'un des trois points d'interconnexion Internet (IXP) situés à Pékin, Shanghai et Guangzhou. Pendant les périodes d'utilisation intensive, ces IXP peuvent être saturés et allonger considérablement les temps de chargement des sites web hébergés hors de Chine. Une série de tests a révélé que lors d'un premier accès, le chargement du site web TED pendant une période de pointe de navigation demandait entre 8 et 38 secondes à Shanghai, contre 5 à 8 secondes à New York pendant une période comparable.

Pour éviter ces goulets d'étranglement, certaines entreprises mondiales choisissent d'héberger leurs sites web dans des datacenters proches de l'un des trois IXP de Chine (par exemple, Hong Kong, proche de l'IXP de Guangzhou) ou sur des serveurs situés sur le territoire chinois. Toutefois, ces solutions les laissent encore exposées à un autre obstacle majeur du réseau : le faible nombre de fournisseurs d'accès Internet (FAI) locaux, avec des interconnexions insatisfaisantes.

Les entreprises déjà familières avec l'environnement de l'Internet chinois savent peut-être déjà que trois FAI appartenant à l'État dominent le marché : China Telecom, China Mobile et China Unicom. Ces FAI prévalent chacun dans une région du pays ; par ailleurs, le nombre d'interconnexions (c'est-à-dire les connexions entre réseaux séparés au sein des IXP) qu'ils ont établies est très limité. Une étude réalisée en 2017 par Mlytics a révélé que le réseau le plus interconnecté de Chine était connecté à deux FAI seulement ; ce nombre atteint 66 en Amérique du Nord et 71 en Europe.

Cela signifie que même le trafic Internet national doit souvent transiter sur une grande distance sur le réseau pour, en fin de compte, parcourir une distance géographique relativement courte, entraînant ainsi une latence supplémentaire pour les utilisateurs finaux.

Comment remédier aux goulets d'étranglement et à l'insuffisance des interconnexions locales

Confrontées à ces obstacles qui grèvent les performances d'Internet, de nombreuses organisations mondiales présentes en Chine optent pour un réseau de diffusion de contenus (CDN) qui leur permet de mettre en cache les contenus statiques (ou non spécifiques à l'utilisateur) de leur site web dans des datacenters proches des utilisateurs finaux, et ainsi, d'éviter qu'une grande partie de leurs requêtes ne soient réacheminées jusqu'au serveur d'origine. Les entreprises doivent opter pour des réseaux CDN qui :

- **Disposent d'un réseau étendu et riche en interconnexions**. Plus un réseau CDN comporte de datacenters, plus il sera proche des utilisateurs finaux ; et plus la couverture assurée par les trois principaux FAI de Chine est performante, moins les requêtes des utilisateurs finaux devront effectuer de sauts sur le réseau.
- **Peuvent résoudre les requêtes DNS en Chine.** Le processus de résolution DNS (c'est-à-dire le processus par lequel les noms de domaine sont convertis en adresses IP) peut générer de la latence si le trafic doit entrer et sortir de Chine, même si les autres contenus des sites web sont mis en cache localement.
- **Minimalisent le code HTML, CSS et Javascript des sites web.** Ces types de code, qui sont les composantes fondamentales de la plupart des sites web, indiquent aux navigateurs des utilisateurs finaux l'apparence que doit adopter le site. La minimalisation consiste à supprimer les caractères inutiles du code, ce qui en réduit la taille globale, et ainsi, réduit la consommation de bande passante lors de son transit sur un réseau. La réduction de la bande passante permet d'accélérer le chargement du site.
- **Utilisent du code serverless à la périphérie du réseau pour créer des règles personnalisées afin de répondre aux requêtes.** Le code serverless est un code qui n'est pas limité à un serveur particulier, contrôlé par un développeur. Lorsqu'il est exécuté à la périphérie du réseau, le code serverless est présent sur un vaste réseau de datacenters. Cela signifie que le code peut facilement et rapidement appliquer des règles spéciales à du trafic utilisateur spécifique. Par exemple, une entreprise peut créer du code serverless sur un réseau basé en Chine afin d'appliquer des règles spéciales pour les utilisateurs mobiles, les connexions Internet lentes ou de nombreux autres scénarios d'utilisation.

Le partenariat de réseau de Cloudflare avec JD Cloud et ses services de performance à l'échelle mondiale peuvent remédier aux goulets d'étranglement du trafic et à l'insuffisance des interconnexions. Consultez la section suivante de ce document pour découvrir comment.

Les cyberattaques nationales persistantes

Comme dans toutes les régions, les sites web déployés en Chine sont en proie à différentes menaces de sécurité.

Les attaques par déni de service distribué (DDoS), durant lesquelles les serveurs ou l'infrastructure réseau sont bombardés avec un volume de trafic indésirable tellement élevé qu'ils ne parviennent plus à répondre aux requêtes légitimes, constituent l'une de ces menaces. Un rapport publié par Talos Intelligence en 2017 a révélé que les services DDoS à la demande, permettant à des utilisateurs non experts de lancer facilement des attaques en utilisant un botnet existant d'appareils infectés, connaissaient un développement rapide en Chine.

Depuis, les forces de l'ordre chinoises ont démantelé plusieurs grands botnets utilisés pour lancer des attaques DDoS, dont un, en 2019, avait infecté plus de 200 000 appareils et permis de lancer des attaques atteignant 200 Gb/s. Toutefois, d'autres botnets restent actifs, tels que DoubleGuns, dont les opérateurs sont toujours recherchés à la date de publication de ce document.

Les sites web en Chine doivent également bloquer les tentatives d'accès aux données confidentielles et aux environnements de développement. En 2018, des acteurs malveillants ont exploité une vulnérabilité d'une infrastructure PHP populaire dans le but d'accéder aux serveurs de plus de 45 000 sites web chinois. Les attaques contre l'infrastructure ont commencé moins de 24 heures après la divulgation de sa vulnérabilité. Par ailleurs, en 2020, deux pirates situés en Chine ont été condamnés pour avoir illégalement accédé aux réseaux privés de centaines d'entreprises au cours des dix dernières années, en tirant là aussi parti de différentes vulnérabilités des applications web.

Par ailleurs, les organisations qui souhaitent protéger des données confidentielles en Chine peuvent se trouver dans l'incapacité d'utiliser leurs outils habituels. L'absence de normes de chiffrement modernes, telles que TLS 1.3 et ESNI (Encrypted Server Name Identification), sur les réseaux chinois multiplie les opportunités d'espionnage du trafic par des observateurs non autorisés.

Comment se défendre contre les cyberattaques nationales persistantes en Chine

Compte tenu de l'augmentation du nombre d'attaques DDoS dans le monde, les services d'atténuation des attaques DDoS (et d'autres outils de sécurité des applications, tels que les pare-feu d'applications web [WAF]) sont devenus un enjeu déterminant pour la sécurité fondamentale de tout site web actif. La Chine ne déroge pas à la règle, et les entreprises qui aspirent à se protéger sur ce marché doivent envisager les solutions suivantes :

- **Atténuation des attaques DDoS depuis la périphérie du réseau, plutôt que dans un nombre restreint de « centres de nettoyage de données ».** Bien que la quasi-totalité des services d'atténuation des attaques DDoS modernes soit déployée dans le Cloud, beaucoup comptent sur un nombre restreint de datacenters pour filtrer (ou « nettoyer ») le trafic malveillant. Le réacheminement du trafic vers ces « centres de nettoyage » aux fins de son inspection peut nécessiter des sauts de réseau supplémentaires et, par conséquent, générer de la latence et des désagréments pour les utilisateurs – tout particulièrement en Chine, en raison des limitations des réseaux. Pour garantir une atténuation des attaques DDoS sans incidence sur les performances Internet en Chine, les entreprises doivent envisager d'utiliser des services de Cloud qui proposent une atténuation des attaques DDoS dans tous les datacenters en périphérie, sans ajouter de sauts de réseau supplémentaires.
- **Limitation du taux pour bloquer les utilisations abusives.** Il est essentiel de disposer de contrôles granulaires permettant d'atténuer les attaques DDoS très précises de la couche 7, de mettre un terme à l'utilisation abusive des API afin de garantir leur disponibilité, de protéger les informations sensibles des clients contre les tentatives de connexion par force brute et de protéger les serveurs d'origine contre l'épuisement des ressources, tout en évitant les coûts imprévisibles dus aux pics de trafic.

- **Des pare-feu d'applications web proposant des mises à jour automatiques et rapides.** Les pirates chinois ont démontré leur capacité à tirer très rapidement parti des nouvelles vulnérabilités des applications web. Certaines entreprises préfèreront être en mesure de créer leurs propres règles de pare-feu WAF, mais elles ne doivent pas se fier uniquement aux informations dont elles disposent sur les menaces, quand bien même elles seraient capables de les actualiser. Elles doivent envisager le déploiement de pare-feu d'applications web proposant des mises à jour automatiques, en fonction d'une large sélection de menaces observées. Et si une organisation veut mettre elle-même ses règles à jour, elle doit avoir la certitude que ces modifications seront propagées le plus rapidement possible.
- **Options de chiffrement personnalisables.** En l'absence de TLS 1.3 et d'ESNI, pour protéger les données en transit, les organisations doivent réfléchir à des services de sécurité proposant une sélection plus vaste de méthodes de chiffrement personnalisables.

Les services de sécurité de Cloudflare, disponibles dans le cadre de notre offre China Network, proposent l'atténuation sans latence des attaques DDoS et un pare-feu WAF qui s'appuie sur un réseau mondial de collecte d'informations sur les menaces pour garantir des mises à jour rapides. Consultez la section suivante de ce document pour en apprendre davantage.

Comment Cloudflare vient en aide aux sites web mondiaux présents en Chine

Cloudflare exploite un réseau de datacenters présents dans 200 villes, dans plus de 100 pays. En Chine, en mars 2022, 45 datacenters sont répartis dans 38 villes. Chacun de ces datacenters peut exécuter de nombreux services de sécurité, de performance et de fiabilité, notamment la diffusion de contenus, la résolution DNS, l'atténuation des attaques DDoS, la mise en œuvre de pare-feu WAF, l'exécution de code sans serveur et bien davantage. Ces services étant exécutés dans chaque datacenter, ils peuvent opérer à proximité immédiate des utilisateurs finaux, et ainsi, contribuer à réduire la latence et à fournir à notre réseau une vue détaillée et actualisée des nouvelles menaces et de l'état du réseau. Par ailleurs, les organisations peuvent gérer tous ces services depuis un tableau de bord unique.

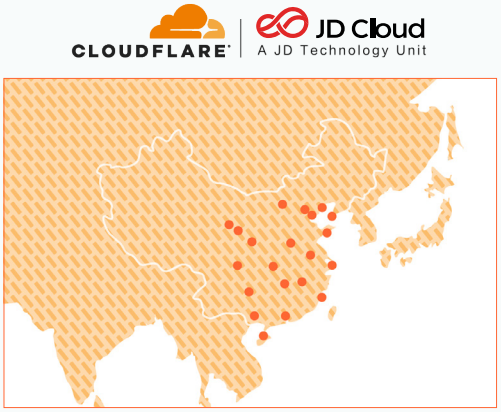
Cloudflare aide depuis 2015 les entreprises à proposer une expérience Internet sécurisée, rapide et fiable aux visiteurs basés en Chine. Pour améliorer encore ces services, nous nous sommes récemment engagés dans un partenariat avec JD Cloud, la division dédiée au Cloud et aux technologies intelligentes du géant chinois de l'Internet JD.com.

Voici comment ce réseau aidera les organisations à surmonter les obstacles décrits dans la section précédente.

Comment Cloudflare contribue à neutraliser l'effet de latence

Le réseau de Cloudflare et de JD Cloud en Chine propose les fonctionnalités suivantes :

- **Routage intelligent Argo :** la transmission des données du client au serveur d'origine, et inversement, peut introduire une latence. Avec la mise en cache, le contenu statique peut éviter la congestion du réseau, tandis que le contenu dynamique dépend de la disponibilité, de la fiabilité et des performances d'Internet. Cela peut entraîner des temps de chargement longs, des dépassements du délai de connexion, des déconnexions et une dégradation de l'expérience de l'utilisateur final. Le **routage intelligent Argo** a la capacité unique de **détecter la congestion en temps réel** et d'**acheminer le trafic web** sur **les liaisons réseau les plus rapides et fiables**. Les requêtes adressées au réseau de Cloudflare par les clients de Cloudflare et leurs utilisateurs nous aident à comprendre comment les différentes parties d'Internet fonctionnent à un moment donné. Le routage intelligent Argo utilise les données temporelles collectées par Cloudflare pour **acheminer dynamiquement le trafic vers les liaisons les plus rapides jusqu'au serveur d'origine**, et ainsi, améliorer les performances. En moyenne, Argo améliore d'environ 30 % les performances des ressources web. Et cela se traduit ultérieurement par une augmentation de vos ventes et de la fidélité de vos clients.
- **Mise en cache et diffusion de contenus statiques depuis de nombreux datacenters en Chine**, ce qui permet de réduire la latence et d'accélérer le chargement des pages, quel que soit l'endroit où se trouvent les utilisateurs finaux. Notre réseau est étroitement interconnecté avec tous les FAI chinois, le nombre de sauts de réseau que doit effectuer le trafic est ainsi réduit.



Datacenters en Chine continentale

- **Résolution DNS optionnelle sur le territoire chinois**, permettant une fois encore d'accélérer les temps de réponse.
- Possibilité d'**utiliser Internet Protocol version 6** (IPv6) pour améliorer l'efficacité du routage et du traitement des paquets.
- Possibilité de **minimaliser le code des sites web** grâce à la fonctionnalité Auto Minify, qui peut être activée facilement, en cochant simplement une case sur le tableau de bord Cloudflare.
- **Code serverless** via le service Cloudflare Workers, déployé dans tous les datacenters de notre réseau China Network. Cette fonctionnalité vous permet de répondre à certaines requêtes de manière personnalisable, d'améliorer les applications existantes et même d'en créer de nouvelles, sans avoir à configurer ni entretenir l'infrastructure.

Comment Cloudflare aide à contenir les cyberattaques nationales persistantes en Chine

Les services de sécurité intégrés au réseau China Network de Cloudflare permettent aux organisations :

- **D'atténuer les attaques DDoS.** Chacun de nos datacenters en Chine peut atténuer les attaques ; le réseau dispose ainsi d'une capacité phénoménale d'absorption des attaques de la plus grande ampleur, sans perte de requêtes légitimes, sans qu'il soit nécessaire d'avoir recours aux datacenters Cloudflare situés ailleurs dans le monde. L'inspection du trafic se déroulant à proximité des utilisateurs finaux, leurs requêtes ne sont pas réacheminées vers un « centre de nettoyage de données » potentiellement lointain. Et compte tenu des écueils que comporte la connectivité réseau en Chine, Cloudflare offre des capacités exclusives de configuration automatisée du trafic permettant de rediriger automatiquement le trafic des attaques. Toutes ces fonctionnalités évitent toute forme d'incidence négative sur les performances du trafic légitime à l'intérieur et à l'extérieur de la Chine.
- **De protéger les vulnérabilités des applications web** avec le pare-feu WAF de Cloudflare. En plus d'arrêter les vecteurs d'attaque connus grâce à des ensembles de règles gérées (par exemple, un déploiement des règles de l'OWASP et de règles propriétaires de Cloudflare), le pare-feu WAF s'appuie sur un flux continu d'informations sur les menaces provenant de l'ensemble de notre réseau pour arrêter automatiquement les menaces les plus récentes. En outre, les organisations peuvent facilement créer leurs propres règles et les propager sur l'ensemble du réseau en quelques minutes seulement. Les améliorations apportées en 2021 permettent de déployer plus rapidement le pare-feu WAF, et facilitent son extension afin de couvrir encore plus de trafic. Le pare-feu WAF dispose également d'ensembles de règles mis à jour qui offrent un meilleur contrôle en séparant l'état des règles de l'action. Les utilisateurs peuvent désormais parcourir les règles plus facilement grâce au filtrage avancé, à l'édition en bloc, aux identifiants de règles, etc.
- **De tirer parti de la limitation du taux**, intégrée à nos règles personnalisées de pare-feu WAF, qui offre une protection contre les attaques DDoS, les tentatives de connexion par force brute, la surcharge du serveur d'origine et d'autres types d'abus visant les API et les applications. Les utilisateurs peuvent configurer des seuils, définir le trafic, personnaliser les réponses et obtenir de précieuses informations sur des URL spécifiques de sites web, d'applications ou de points de terminaison d'API.
- **Chiffrer les données avec TLS 1.2** et gérer facilement leurs propres certifications depuis le tableau de bord Cloudflare.

EN SAVOIR PLUS

Le service China Network de Cloudflare est à la disposition de tous les clients Cloudflare Enterprise. Il est pleinement conforme aux lois et réglementations chinoises, conformément auxquelles une licence valide de fournisseur de contenu Internet (ICP) est une condition obligatoire pour intégrer le réseau China Network.

Alors que l'économie chinoise de l'Internet continue de se développer, de nouveaux défis en matière de sécurité et de performances vont inévitablement apparaître. Les plans de croissance continue de Cloudflare en Chine offrent aux entreprises présentes sur notre réseau la capacité de réagir rapidement à ces écueils et de continuer à proposer des expériences utilisateur fluides.

Appelez Cloudflare dès aujourd'hui pour commencer à optimiser votre présence en ligne en Chine !

Pour en savoir plus sur le réseau China Network de Cloudflare, consultez la page cloudflare.com/network/china/ ou contactez votre représentant Cloudflare.