CLOUDFLARE

DOSSIER DE SOLUTION

Secure Access Service Edge (SASE)

Accélérer la transformation du réseau et la modernisation de la sécurité

Qu'est-ce que le modèle SASE ?

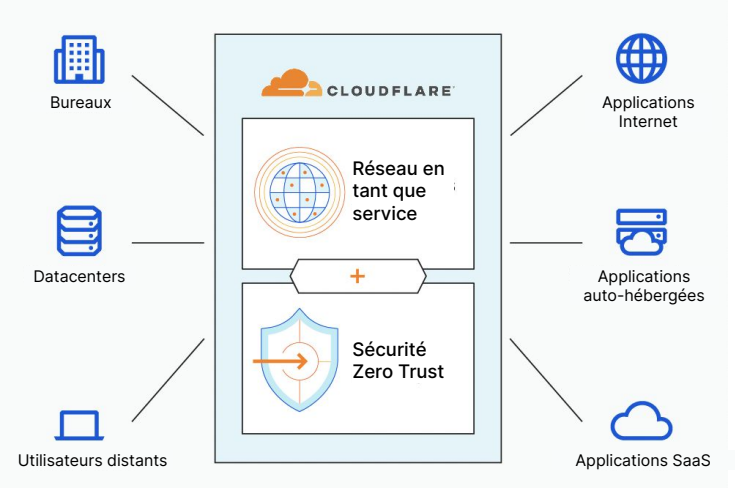
L'émergence d'initiatives numériques et de cloud a déplacé les applications des datacenters centralisés vers des sites distribués tels que le cloud public, le cloud privé et les infrastructures SaaS. Parallèlement à cela, les utilisateurs travaillent désormais depuis leur domicile, leur bureau ou tout autre endroit distant, ou ils adoptent un mode de travail hybride. Ce nouveau modèle de trafic (de point à point) a étendu la surface d'attaque de l'architecture réseau existante, entraînant une augmentation du risque de cyberattaques.

L'adoption d'une architecture SASE permet de répondre à l'évolution de l'accès aux applications. L'approche SASE incarne la convergence du réseau et des fonctions de sécurité du réseau pour le trafic de point à point, avec de meilleurs contrôles de sécurité fondés sur les principes Zero Trust. Gartner prévoit que « d'ici 2025, au moins 60 % des entreprises disposeront de stratégies et de calendriers explicites d'adoption de l'architecture SASE, englobant l'accès des utilisateurs, des succursales et des périphéries, contre 10 % en 2020. » [1]

Comment Cloudflare soutient le déploiement de l'architecture SASE

La plateforme SASE de Cloudflare, Cloudflare One, constitue une solution de réseau en tant que service Zero Trust bâtie sur une plateforme réseau unique et unifiée, native d'Internet. Elle place des mesures de sécurité basées sur l'identité, les pare-feu, l'approche WAN-as-a-Service et bien d'autres services à proximité des utilisateurs, partout dans le monde, afin de les aider à se connecter rapidement et de manière sécurisée à n'importe quelle ressource de l'entreprise.

Au lieu d'accorder une confiance et un accès totaux aux applications lorsqu'elles se trouvent sur le réseau de l'entreprise, l'approche Zero Trust utilise une architecture d'interdiction par défaut, basée sur un proxy, qui impose la vérification et l'autorisation de chaque requête entrante, sortante et transmise entre les entités présentes sur votre réseau – garantissant ainsi que les utilisateurs peuvent atteindre uniquement les applications auxquelles ils sont explicitement autorisés à accéder.



Obstacles au déploiement de solutions SASE

Selon Gartner, un des obstacles au déploiement de solutions SASE est l'étendue mondiale. En moyenne, les entreprises du classement Fortune 500 sont présentes dans 32 pays. Pourtant, de nombreux fournisseurs de solutions SASE proposent des services dans plusieurs régions et pays. L'absence d'étendue mondiale entraîne une application incohérente des politiques de sécurité et des problèmes de performance.

Pour les entreprises qui aspirent à unifier pleinement la sécurité et les services à la périphérie du réseau auprès d'un fournisseur unique, Cloudflare One propose des services développés sur notre réseau mondial couvrant plus de 275 villes dans plus de 100 pays, situé à ~50 ms de 95 % de la population connectée à Internet.

> « L'architecture SASE est tributaire d'une mise en œuvre depuis le cloud, et l'étendue du cloud d'un fournisseur peut empêcher les déploiements dans certaines zones géographiques telles que la Chine, la Russie et le Moyen-Orient, où la présence des fournisseurs dans le cloud peut être limitée. »[2]
>
> Gartner

La composabilité accélère les déploiements SASE

Selon les investissements existants, les clients qui optent pour le déploiement d'une solution SASE ont souvent recours à plusieurs fournisseurs, afin de couvrir l'intégralité de la solution. Le recours à plus d'un ou deux fournisseurs entraîne une augmentation du coût total de possession, des complexités opérationnelles, des problèmes de performance et, surtout, une diminution de la flexibilité opérationnelle. Il existe des dizaines de fournisseurs de solutions SASE, dont certains sont spécialisés dans la sécurité, d'autres dans les réseaux ; cependant, très peu sont experts dans ces deux domaines.

La consolidation du matériel et des produits dédiés peut demander des années, car le matériel est renouvelé suivant des cycles de 5 à 7 ans. Actualiser le matériel du réseau en premier lieu peut provoquer des problèmes d'interopérabilité avec le service de sécurité existant, et inversement. Pour accélérer l'adoption d'une solution SASE à leur rythme, les clients doivent disposer d'une plateforme SASE composable. Les services privilégiant la composabilité sont disponibles à la demande, prêts à l'emploi et compatibles, et interopérables avec l'infrastructure existante.

Cloudflare One est une plateforme SASE composable. Avec notre plateforme, les services de sécurité et de connectivité réseau résident tous sur la même infrastructure et sont architecturalement unifiés à tous les niveaux – pas seulement sur une interface unique. Un plan de contrôle pour un plan de données, avec une inspection en une seule passe aussi près que possible de l'utilisateur, afin d'éliminer toute latence supplémentaire. Avec un plan de contrôle unique, tous les accès directs peuvent se connecter et sécuriser le trafic vers n'importe quelle ressource avec des intégrations uniques. Une interface de gestion : interface utilisateur, API et interface de ligne de commande.

> « Évitez, autant que possible, de faire appel à plus de deux fournisseurs pour tous les services essentiels, afin de minimiser la complexité et d'améliorer les performances… »[2]
>
> Gartner

Notre périphérie de services mondiale et exhaustive

Cloudflare

✓ Accès réseau Zero Trust	✓ Identité/Contexte	✓ Prévention des menaces
✓ CASB	✓ Règles du profil d'appareil	✓ Protection contre la perte de données
✓ Passerelle web sécurisée	✓ Contrôle des accès en fonction du rôle	✓ Découverte de l'application cloud
✓ Firewall-as-a-Service	✓ Chiffrement/déchiffrement	✓ Accélération SaaS
✓ WAN-as-a-Service	✓ Isolation du navigateur	✓ Restrictions géographiques
✓ Mise en cache/CDN	✓ Protection DNS	✓ Dissimulation/Confidentialité
✓ Coût opt. réseau interm.	✓ WAF/WAAPaaS	✓ Protection Wi-Fi

Pourquoi les clients utilisent Cloudflare pour adopter l'architecture SASE

Simplicité de déploiement

Cloudflare propose une plateforme uniforme et composable, pour une configuration et des opérations plus simples. Avec leurs connecteurs exclusivement logiciels et leurs intégrations en une seule passe, les accès directs et les services périphériques de Cloudflare fonctionnent tous ensemble. Cette approche permet de proposer une meilleure expérience à vos collaborateurs et vos utilisateurs finaux.

Résilience du réseau

Nos mesures d'automatisation du trafic de bout en bout assurent une connectivité réseau fiable et évolutive, offrant une protection constante depuis n'importe quel emplacement. Avec Cloudflare, chaque service périphérique est conçu pour s'exécuter dans n'importe quel emplacement réseau, afin d'être disponible pour chaque client – contrairement aux solutions proposées par d'autres fournisseurs de solutions de sécurité.

Rapidité de l'innovation

Notre architecture pérenne nous aide à développer et déployer très rapidement de nouvelles capacités de connectivité réseau et de sécurité. Qu'il s'agisse de notre adoption rapide des nouvelles normes applicables à Internet et à la sécurité ou du développement de scénarios d'utilisation à l'initiative de nos clients, notre historique de prouesses techniques parle pour lui. En outre, la fondation même de notre solution offre une liberté de choix absolue.

Commencez votre parcours vers un réseau plus rapide, plus fiable et plus sécurisé

Essayer maintenant

Pas encore prêt à l'essayer ? Apprenez-en davantage sur Cloudflare One

1. 2021 Gartner Strategic Roadmap for SASE Convergence 2. Gartner Hype Cycle™ for Network Security, 2021

GARTNER et HYPE CYCLE sont des marques déposées et des marques de service de Gartner, Inc. ou de ses filiales aux États-Unis et dans le monde entier, et sont utilisées ici avec son accord. Tous droits réservés.