LIVRE BLANC

CLOUDFLARE

Débuter avec le modèle SASE : Un guide pour sécuriser et rationaliser votre infrastructure de réseau

Le modèle SASE (Secure Access Service Edge) simplifie l'architecture de réseau traditionnelle en fusionnant les services de réseau et de sécurité sur un réseau mondial unique.
Ce livre blanc explore l'évolution de la sécurité des réseaux qui a abouti au modèle SASE, présente la portée des services inclus dans une solution SASE et propose des mesures concrètes pour l'adoption du modèle SASE.

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

INTRODUCTION

Inventé par Gartner en 2019, le terme SASE (Secure Access Service Edge) a été initialement proposé pour constituer une avancée majeure dans le processus de transformation numérique : des services de réseau et de sécurité fortement personnalisables, intrinsèquement intégrés à la structure même d'une plateforme de Cloud mondiale. Avec un taux d'adoption de 20 % attendu d'ici 2023, Gartner a affirmé que la demande de fonctionnalités SASE « redéfinirait l'architecture de sécurité des réseaux d'entreprises et de la sécurité des réseaux et transformerait radicalement le paysage concurrentiel. »[1]

Depuis, le terme s'est répandu comme une traînée de poudre dans le secteur de la sécurité informatique et des entreprises. Tandis que les fournisseurs de sécurité des réseaux et de réseaux SD-WAN se bousculent pour se positionner comme autant de leaders de l'approche SASE, les entreprises se trouvent confrontées à un ensemble hétéroclite de services de réseau et de sécurité qui évoque, sans toutefois vraiment l'incarner, une infrastructure SASE.

L'adoption d'un véritable modèle SASE nécessite plus que l'accumulation de solutions ponctuelles existantes : elle exige de repenser intégralement l'infrastructure du réseau d'entreprise. Le maintien d'un périmètre de réseau strict sur site ne suffit plus à protéger une main-d'œuvre toujours plus mobile et distribuée, et le recours à plusieurs services de sécurité pour protéger une infrastructure hybride peut s'avérer coûteux, faire du déploiement et de la gestion un véritable casse-tête pour les équipes informatiques et laisser d'immenses failles en matière de sécurité.

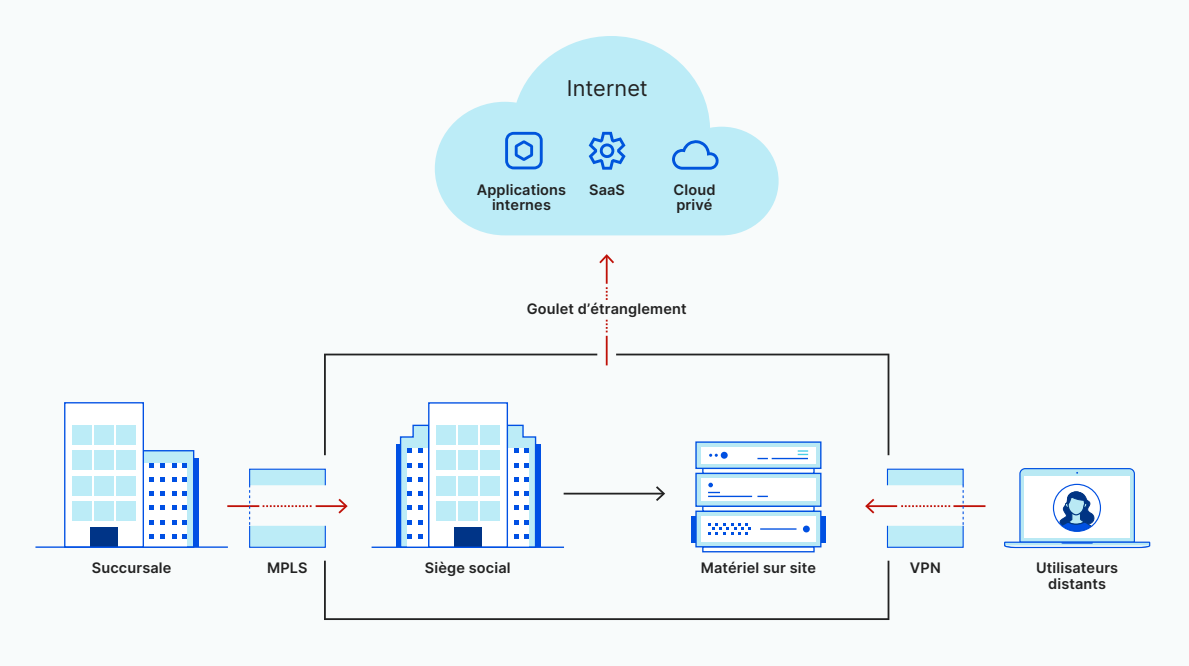
Le modèle SASE relève ces défis en déplaçant le périmètre du réseau des datacenters centralisés vers l'utilisateur. En consolidant la connectivité réseau et les services de sécurité du réseau et en les déployant depuis une plateforme unique dans le Cloud, le modèle SASE élimine les failles de sécurité entre les services, offre une meilleure visibilité de l'activité du réseau aux équipes informatiques et simplifie le processus de migration vers le Cloud.

1. LES ORIGINES DU MODÈLE SASE

Pour comprendre le tournant décisif que représente le modèle SASE, il est important d'examiner l'évolution progressive des infrastructures et de la sécurité des réseaux.

Avant l'adoption généralisée du Cloud, les ressources, les données et les applications des entreprises résidaient dans des locaux sur site, protégés par des pare-feu matériels et des équipements anti-DDoS. Les employés présents dans une agence accédaient aux ressources internes au moyen de connexions privées, filtrées par des pare-feux réseau. Les utilisateurs qui se connectaient depuis des sites distants le faisaient généralement via un VPN, qui était sujet à des problèmes de latence et d'encombrement.

À l'origine de cette configuration était la crainte de l'internet ouvert – un outil initialement conçu dans l'optique de la résilience, toutefois sans tenir compte des besoins de performances et de sécurité des entreprises. Internet s'étant révélé intrinsèquement vulnérable aux attaques, les organisations ont choisi d'établir leurs propres réseaux privés et de sécuriser (souvent, avec une efficacité limitée) les données, les applications et les ressources des entreprises au moyen de boîtiers de pare-feu et d'équipements anti-DDoS physiques. Le trafic entrant était acheminé dans des datacenters centralisés, où il était inspecté et filtré, créant un goulet d'étranglement.



Infrastructure réseau pré-SASE

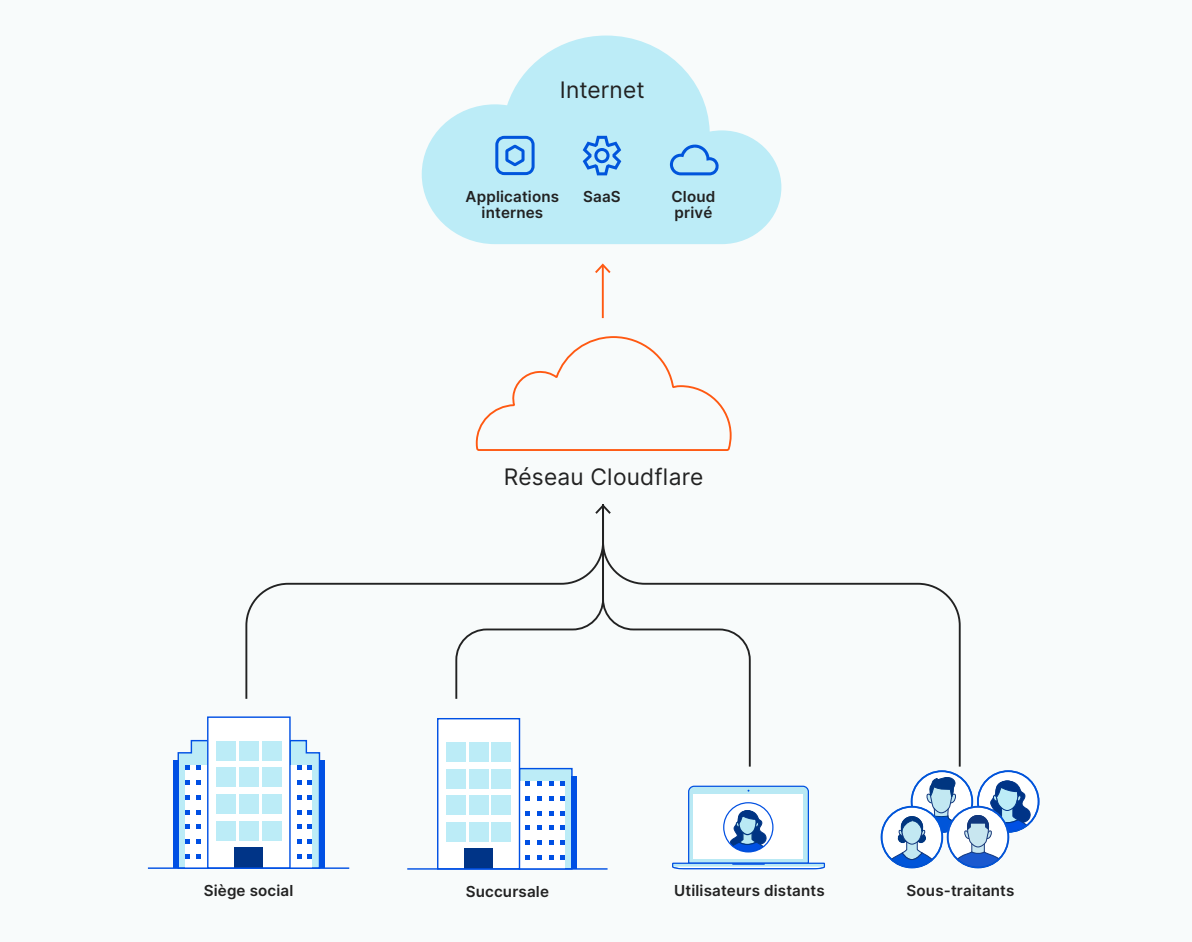
Ce modèle de sécurité des réseaux était à la fois coûteux et complexe, et les entreprises restaient vulnérables aux violations de données et aux menaces internes. Lorsqu'un attaquant avait franchi le périmètre du réseau, il pouvait causer des dommages considérables au sein d'une entreprise en diffusant des logiciels malveillants, en prenant le contrôle de comptes d'utilisateurs[2] et en dérobant de précieuses données de clients.[3]

Avec l'avènement du Cloud et des services SaaS, les organisations ont désormais plus de liberté et de flexibilité pour réimaginer l'infrastructure de leur réseau, car il n'est plus nécessaire que les applications, les données et les collaborateurs résident exclusivement dans des locaux sur site.

1. LES ORIGINES DU MODÈLE SASE

Toutefois, cette liberté comporte de nouveaux défis en matière de sécurité. Les équipes informatiques ont la charge de protéger un ensemble hétérogène de services sur site et dans le Cloud, ainsi que de sécuriser une main-d'œuvre toujours plus mobile et distante.[4] Pour y parvenir, elles doivent souvent gérer du matériel coûteux et superposer les services de sécurité ponctuels de différents fournisseurs, dont la mise en œuvre et la gestion peuvent s'avérer fastidieuses et difficiles.

La prochaine évolution en matière de sécurité des réseaux ne ressemblera probablement pas au matériel qui protégeait les infrastructures en étoile traditionnelles, ni aux complexes solutions alternatives que nécessite une architecture de Cloud hybride.
Au lieu de cela, elle prendra plutôt la forme d'une infrastructure SASE, qui consolide les services réseau et de sécurité et les déploie sous la forme d'un service intégré.



L'infrastructure du réseau SASE

Plutôt que de dépendre d'équipements matériels inefficaces ou d'assembler des services de sécurité en silo, le modèle SASE propose une approche rationalisée de la sécurité des réseaux. Il remplace le réacheminement complexe par la périphérie d'Internet, permettant ainsi aux entreprises d'acheminer, d'inspecter et de sécuriser le trafic en une seule opération. Associé aux politiques d'accès Zero Trust et à une protection contre les menaces au niveau du réseau, le modèle SASE élimine la nécessité de déployer des VPN patrimoniaux, des pare-feux matériels et des équipements de protection anti-DDoS, offrant ainsi aux entreprises une meilleure visibilité et un meilleur contrôle des configurations de sécurité de leur réseau.

2. DÉFINIR LA PORTÉE DU MODÈLE SASE

Le modèle SASE est un modèle de sécurité basé sur le Cloud, qui associe un réseau étendu défini par logiciel à des services essentiels de sécurité des réseaux, qu'il déploie à la périphérie du Cloud. La plupart des offres SASE sont caractérisées par cinq fonctionnalités principales :

Construction et gestion de réseaux

Un réseau étendu défini par logiciel (SD-WAN) permet aux organisations d'établir des réseaux d'entreprise privés sans l'aide de routeurs matériels ou de circuit MPLS (Multiprotocol Label Switching). Cette architecture logicielle virtuelle offre aux entreprises davantage de flexibilité dans la création et la maintenance de leur infrastructure réseau, bien qu'elle comporte également certaines vulnérabilités de sécurité intégrées.

Filtrage du trafic

Les passerelles web sécurisées (SWG) permettent de lutter contre les cybermenaces et les fuites de données en filtrant les contenus indésirables du trafic web, en bloquant les comportements indésirables d'utilisateurs et en appliquant les politiques de sécurité d'entreprises. Elles incluent généralement le filtrage des URL, la détection et le blocage des logiciels malveillants et le contrôle des applications, entre autres fonctionnalités.

Sécurisation des données

Un Cloud Access Security Broker (CASB) exécute plusieurs tâches de sécurité pour les services hébergés dans le Cloud (par exemple, applications SaaS, IaaS et PaaS). Les CASB standard sécurisent les données confidentielles en appliquant le contrôle des accès et la prévention des pertes de données. Ils permettent de révéler les phénomènes de Shadow IT et de garantir le respect des réglementations en matière de confidentialité des données.

Connexion des utilisateurs aux applications

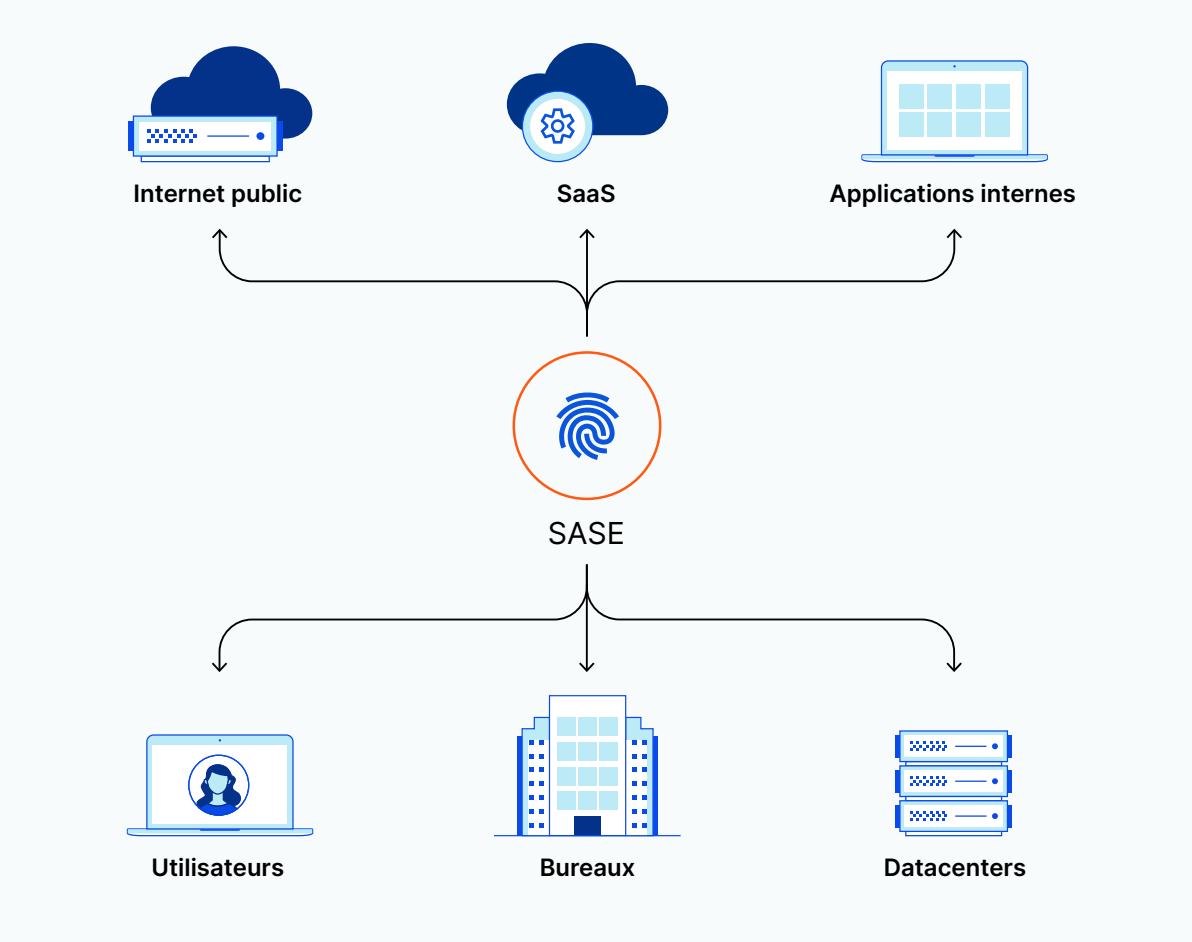
L'accès réseau Zero Trust (ZTNA) nécessite une vérification en temps réel de chaque utilisateur pour chaque application protégée, afin de protéger les ressources internes et d'offrir une défense contre les violations de données potentielles. Avec une approche Zero Trust, aucune entité n'est automatiquement approuvée tant que son identité n’a pas été vérifiée, même si elle se trouve déjà dans le périmètre d’un réseau privé.

Protection des applications et de l'infrastructure

Les pare-feux Cloud (FWaaS) protègent l'infrastructure et les applications dans le Cloud contre les cyberattaques grâce à un ensemble de fonctionnalités de sécurité telles que le filtrage d'URL, la prévention des intrusions et la gestion uniforme des politiques.

2. DÉFINIR LA PORTÉE DU MODÈLE SASE

Bien qu'une solution SASE classique inclue les cinq services décrits ci-dessus, cette liste constitue davantage un point de départ qu'un ensemble d'exigences strictes. Fondamentalement, le modèle SASE repose sur la convergence de deux fonctionnalités fondamentales et distinctes, l'architecture réseau basée sur des logiciels et les services de sécurité dans le Cloud. Les fournisseurs peuvent ensuite ajouter ou soustraire des services supplémentaires, selon le besoin.



3. LES AVANTAGES D'UNE APPROCHE SASE

Tandis que le modèle SASE continue à évoluer, sa mise en œuvre peut varier considérablement d'un fournisseur à l'autre et d'une organisation à l'autre. Cependant, la plupart des solutions SASE possèdent plusieurs avantages essentiels communs par rapport aux configurations de sécurité des réseaux sur site et hybrides :

Mise en œuvre simplifiée

En consolidant les services réseau et de sécurité, le modèle SASE élimine la nécessité d'incorporer des services dans le Cloud, de déployer des équipements sur site et d'investir du temps, de l'argent et des ressources internes dans l'actualisation de ces composants pour faire face aux nouvelles menaces.

Réduction de la latence

L'approche SASE permet de réduire la latence et d'amélorer les performances en acheminant le trafic réseau sur un réseau périphérique mondial, sur lequel le trafic est traité au plus près de l'utilisateur. Les optimisations du routage peuvent contribuer à déterminer le chemin réseau le plus rapide en fonction de l'encombrement du réseau et d'autres facteurs.

Gestion simplifiée des politiques

Le modèle SASE permet aux entreprises de définir, surveiller, ajuster et appliquer des politiques d'accès sur l'ensemble des emplacements, utilisateurs, équipements et applications. Les attaques et les menaces entrantes peuvent être identifiées et atténuées depuis un portail unique, plutôt qu'être surveillées et gérées individuellement avec différents outils de sécurité dédiés.

Un réseau mondial

Une infrastructure SASE est bâtie sur un réseau mondial unique, permettant aux organisations d'étendre le périmètre de leur réseau à tout utilisateur, succursale, appareil ou application distant et de bénéficier d'une meilleure visibilité et d'un contrôle renforcé sur l'ensemble de leur infrastructure de réseau.

Accès réseau basé sur l'identité

L'approche SASE repose lourdement sur un modèle de sécurité Zero Trust, dans lequel l'identité et l'accès des utilisateurs sont définis en fonction de différents facteurs tels que la localisation de l'utilisateur, l'heure de la journée, les règles de sécurité de l'entreprise, les politiques de conformité et une évaluation continue des risques et de la confidentialité. Ce niveau de sécurité (qui constitue une avancée significative par rapport aux VPN, trop permissifs et intrinsèquement vulnérables) offre une protection contre les violations de données, tant externes qu'internes, ainsi que d'autres attaques.

4. DÉBUTER AVEC LE MODÈLE SASE

Pour les entreprises qui ont investi beaucoup de temps, de ressources et d'argent dans des configurations sur site élaborées, qui gèrent des ensembles complexes de services de sécurité dans le Cloud ou qui s'adaptent encore à l'avenir du télétravail, l'adoption du modèle SASE peut paraître décourageante – mais cela n'est pas une fatalité.

Voici cinq mesures pratiques que vous pouvez prendre pour vous familiariser avec l'approche SASE :

1. Protégez votre personnel à distance.

Déployez une solution ZTNA qui vous permet de supprimer votre VPN, de protéger les données et les ressources de l'entreprise contre les menaces internes et externes et d'améliorer l'expérience des utilisateurs. En déplaçant votre passerelle Web sécurisée et votre pare-feu Cloud vers la périphérie, vous pouvez inspecter et filtrer le trafic sans le réacheminer par un datacenter.

2. Placez les succursales derrière un périmètre de Cloud.

Dans les succursales, appliquez une architecture Zero Trust qui élimine la nécessité de déployer des équipements de sécurité sur site (pare-feu matériel, protection anti-DDoS, etc.), qui peuvent s'avérer coûteux à l'usage, mais aussi inefficaces dans un environnement de menaces rapidement changeant.

3. Déplacez la protection anti-DDoS vers la périphérie.

Débarrassez-vous des équipements anti-DDoS physiques et défendez les réseaux d'entreprise contre les attaques avec une protection anti-DDoS de couche réseau, dans le Cloud, capable de détecter et d'atténuer les menaces en temps réel.

4. Migrez les applications vers le Cloud.

À mesure que votre entreprise se développe, déplacez les applications des datacenters sur site vers le Cloud et assurez-vous d'appliquer des politiques de sécurité du Cloud cohérentes à l'ensemble du trafic.

5. Remplacez les équipements de sécurité sur site par l'application unifiée des politiques dans le Cloud.

Réduisez le coût et la complexité de la maintenance des équipements réseau en déplaçant l'application des politiques vers la périphérie, où vous pouvez surveiller et gérer l'ensemble du trafic, des modèles d'attaque et des politiques de sécurité depuis une interface unique.

5. DÉPLOIEMENT DE L'ARCHITECTURE SASE PAR CLOUDFLARE

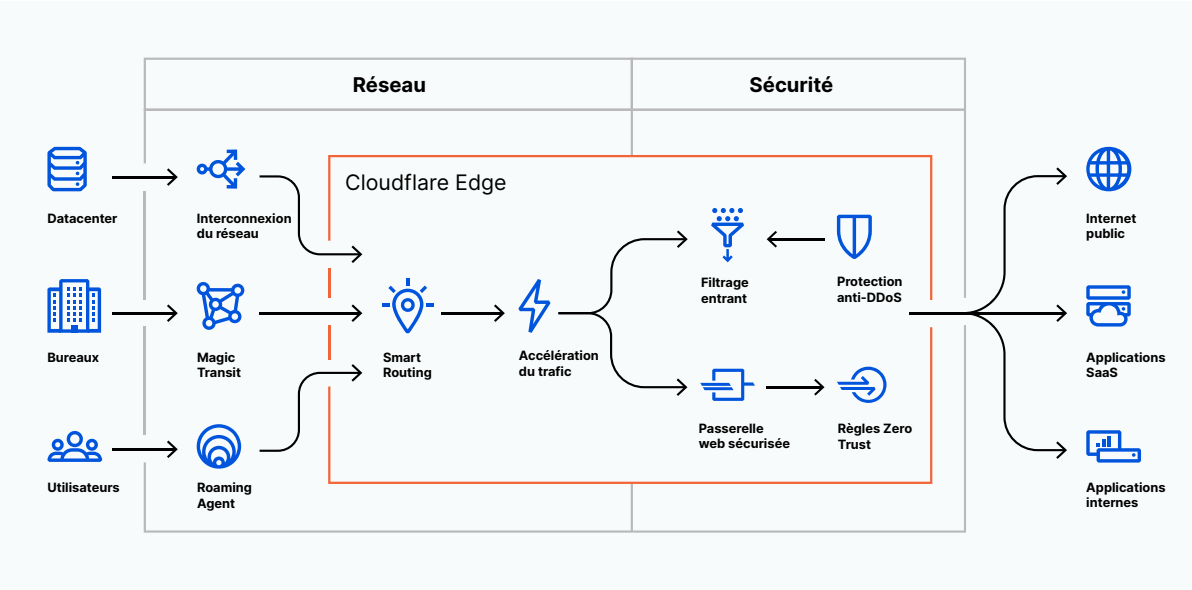
Que vous l'appeliez « SASE » ou simplement « nouvelle réalité », les entreprises ont besoin de flexibilité à chaque couche du réseau et de la pile d'applications. Les utilisateurs doivent disposer d'un accès sécurisé et authentifié, où qu'ils se trouvent : au bureau, sur un appareil mobile ou à leur domicile.

Cloudflare One™ est une solution réseau en tant que service (NaaS) complète qui simplifie et sécurise la gestion de réseau des entreprises pour les équipes de toutes tailles.

Avec Cloudflare One, vous pouvez :

- **Déployer un accès Zero Trust.** Remplacez les vastes périmètres de sécurité par une vérification individuelle de chaque requête transmise à chaque ressource. Appliquez les règles Zero Trust à chaque connexion à vos applications d'entreprise, indépendamment de la localisation ou de l'identité des utilisateurs.
- **Sécuriser le trafic Internet.** Les menaces sur Internet se propagent rapidement, aussi, les moyens de défense que vous utilisez pour les arrêter doivent être plus rapides. Cloudflare One protège le personnel distant contre les menaces sur Internet et applique des politiques qui empêchent les fuites de données précieuses depuis votre entreprise.
- **Protéger et connecter les bureaux et les datacenters.** Les réseaux d'entreprise sont devenus excessivement complexes, et le trafic des utilisateurs doit souvent accomplir plusieurs sauts avant d'atteindre sa destination. Avec Cloudflare One, protégez vos agences et vos datacenters avec une plate-forme Cloud unique et cohérente.

L'architecture unique de Cloudflare est conçue pour déployer un réseau intégré et des services de sécurité sur nos plus de 200 sites dans le monde, et ainsi, éviter aux entreprises d'acheminer le trafic par un datacenter centralisé ou de gérer des solutions multipoints dans le Cloud.



Comment Cloudflare One protège l'infrastructure de réseau

5. DÉPLOIEMENT DE L'ARCHITECTURE SASE PAR CLOUDFLARE

Cloudflare One	Fonctionnalité essentielle	Service SASE
Cloudflare Gateway inspecte le trafic des utilisateurs et empêche les contenus malveillants d'atteindre leurs appareils et de se propager au sein d'une organisation.	Filtrage du trafic	SWG, CASB
Cloudflare Access renforce les exigences d'accès en appliquant à chaque requête entrante et sortante des filtres d'identité et de contexte.	Connexion des utilisateurs aux applications	ZTNA, CASB
Cloudflare Magic WAN fournit un plan de contrôle permettant d'accélérer et d'acheminer le trafic sur le réseau Cloudflare en utilisant WARP, Magic Transit et Cloudflare Network Interconnect (CNI).	Construction et gestion de réseaux	SD-WAN
Cloudflare Magic Firewall remplace les pare-feux sur site par une protection, au niveau du réseau, des utilisateurs distants, des succursales, des datacenters et de l'infrastructure de Cloud.	Protection des applications et de l'infrastructure	FWaaS
Cloudflare Browser protège les appareils des utilisateurs contre les menaces zero-day en isolant le navigateur du code potentiellement dangereux.	Sécurisation des appareils et des données	Isolation de navigateur à distance

Pour en savoir plus sur Cloudflare One, consultez le site www.cloudflare.com/cloudflare-one/.

RÉFÉRENCES

1. Gartner, « The Future of Network Security Is in the Cloud ». Analyste(s) : Neil MacDonald, Lawrence Orans, Joe Skorupa. 30 août 2019. Gartner.
2. Twitter Inc. « An update on our security incident ». Twitter. Accès le 27 octobre 2020.
3. Marriott International News Center. « Marriott International Notifies Guests of Property System Incident ». Marriott. Accès le 27 octobre 2020.
4. Bursztynsky, Jessica. « Dropbox is the latest San Francisco tech company to make remote work permanent ». CNBC. CNBC. Accès le 27 octobre 2020.