CLOUDFLARE

PRÉSENTATION DE SOLUTION

Sécuriser les lieux de travail décentralisés

Une protection cohérente pour toutes les requêtes, pilotée depuis une interface unifiée, quel que soit l'emplacement du bureau

Faites migrer votre sécurité vers le cloud

Réduisez la complexité et les risques dans les bureaux grâce à Cloudflare

Avec des collaborateurs au bureau et en télétravail, de nombreuses entreprises réévaluent la manière dont elles sécurisent leur bureaux à l'heure actuelle, qu'elles s'appuient sur des équipements installés dans les datacenters ou qu'elles autorisent un accès direct et non sécurisé à Internet.

Leur nouvelle préoccupation consiste à proposer une protection et une expérience cohérentes à tous les utilisateurs, qu'ils se situent sur ou en dehors du réseau. La plupart du temps, cette approche implique une migration des mesures de contrôle loin des outils disparates, comme les VPN, les proxys web et les pare-feu, vers une plateforme de sécurité unique proposée via le cloud.

Deux scénarios d'utilisation courants se dégagent de la manière dont Cloudflare voit les entreprises moderniser la sécurité de leurs bureaux.

Scénario d'utilisation recommandé

Sécuriser l'accès aux applications à l'aide du Zero Trust afin de remplacer les VPN

Appliquez des politiques précises et sensibles à l'identité en fonction de l'application, plutôt que d'autoriser les mouvements latéraux sur l'ensemble du réseau d'entreprise.

- **Étape 1 :** intégrez votre ou vos fournisseurs d'identité.
- **Étape 2** : protégez toutes vos applications web à l'aide d'un navigateur.
- **Étape 3** : sécurisez les environnements SSH, VNC et RDP à l'aide d'un navigateur.

> **Combinez l'accès des bureaux régionaux et l'accès à distance sous un déploiement unique afin de garantir la cohérence des politiques et de minimiser le nombre de fournisseurs nécessaires. Déployez le ZTNA pour renforcer ou remplacer vos anciens VPN afin de limiter les investissements dans des technologies obsolètes.[1]**
>
> Gartner

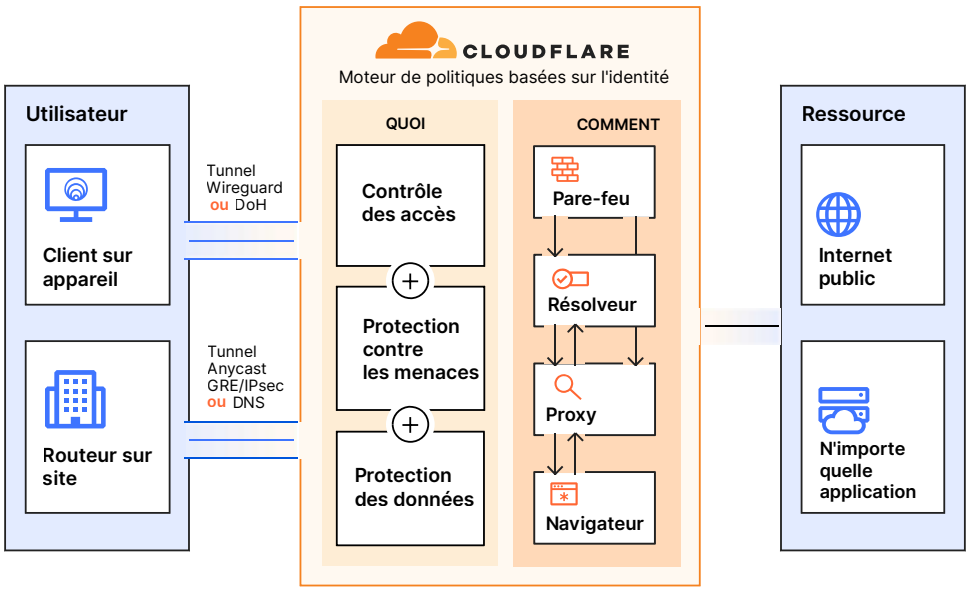
Scénario d'utilisation recommandé

Filtrer l'accès Internet afin d'assurer une sécurité cohérente, assortie d'un délai de rentabilité réduit

Protégez tout d'abord les utilisateurs sur site grâce au filtrage DNS, puis à l'aide d'inspections plus complètes partout dans le monde. Plus besoin de rediriger le trafic via des équipements de sécurité installés dans des datacenters sur site.

- **Étape 1 :** faites pointer le trafic DNS vers le réseau mondial de Cloudflare.
- **Étape 2** : définissez un filtrage DNS en fonction de l'emplacement afin de vous protéger contre les rançongiciels, le phishing et les autres menaces Internet.
- **Étape 3** : contrôlez les flux de données en appliquant des règles HTTP, réseau et d'isolement de navigateur, en plus d'une inspection TLS 1.3 illimitée.

Fonctionnement



Un déploiement sans client pour vérifier les accès et filtrer les requêtes DNS provenant de vos bureaux.

Assurez le déploiement à l'aide du client sur appareil Cloudflare afin de renforcer la visibilité et les mesures de contrôle en fonction de l'utilisateur et de l'appareil.

Figure 1 : vérifiez, filtrez, isolez et inspectez le trafic de vos bureaux en une seule passe grâce à la plateforme Cloudflare Zero Trust.

Des accès directs (on-ramp) flexibles depuis n'importe quelle source

Vous pouvez commencer à utiliser Cloudflare à des fins de résolution DNS via des routeurs réseau. Au fil du temps, vous pourrez envoyer le trafic de couche 3 vers notre réseau mondial par l'intermédiaire de tunnels GRE ou IPsec, ou utiliser votre méthode de routage SD-WAN existante.

Vous pouvez également déployer le client Cloudflare à des fins de filtrage et d'inspection DNS et HTTP sur les appareils gérés.

Une mise en œuvre rapide des politiques, pensée pour évoluer à l'échelle mondiale

Toutes les fonctions d'amélioration de la sécurité, des performances et de la fiabilité sont conçues pour s'exécuter sur chaque serveur de chaque datacenter, sur l'ensemble de notre réseau, implanté dans plus de 275 sites répartis dans plus de 100 pays.

L'échelle de notre réseau implique que les protections sont toujours appliquées à proximité des bureaux et des utilisateurs finaux, peu importe leur position géographique, et ce à grande vitesse, grâce à l'inspection en une seule passe.

D'autres scénarios d'utilisation à explorer au cours des six à douze mois à venir

Reprenez le contrôle des applications SaaS

Identifiez et atténuez le risque d'informatique fantôme (Shadow IT) que vos collaborateurs utilisent au bureau et chez eux.

Prévenez les fuites de données et les violations de la conformité à l'aide de politiques de CASB mises en œuvre depuis le tableau de bord Cloudflare. Découvrez comment.

Déchargez le trafic MPLS

Remplacez les connexions MPLS privées coûteuses, vieillissantes et lentes.

Simplifiez votre architecture WAN existante en utilisant le réseau mondial de Cloudflare pour gérer le trafic sur l'ensemble de vos bureaux régionaux, datacenters et services cloud publics. Découvrez comment.

1. 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.

RÉV. : BDES-6043.2024AUG06