Accès réseau Zero Trust avec routage privé

Empêcher les mouvements latéraux et réduire la dépendance aux VPN

En matière d'accès aux applications, toute confiance accordée aux mesures de contrôle basées sur le réseau (les VPN et la restriction d'adresses IP, par exemple) peut augmenter votre surface d'attaque, limiter votre visibilité et frustrer vos utilisateurs finaux. L'accès réseau Zero Trust de Cloudflare agit en collaboration avec vos fournisseurs d'identité et vos plateformes de protection des points de terminaison pour appliquer des règles Zero Trust. En refusant l'accès par défaut, ces dernières permettent de limiter l'accès aux applications, aux espaces IP privés et aux noms d'hôte de l'entreprise. Soutenue par le vaste et performant réseau Anycast de Cloudflare, cette solution rend les connexions des utilisateurs plus rapides qu'un VPN.

Depuis le déploiement de l'accès réseau Zero Trust en interne, Cloudflare a constaté les avantages suivants :

- Réduction de 91 % de la surface d'attaque[1]
- Multiplication par deux des économies réalisées sur les coûts grâce à la réduction des efforts informatiques
- Réduction d'environ 80 % du temps consacré aux tickets concernant le VPN
- Réduction d'environ 70 % du volume de tickets reçus
- Plus de 300 heures de productivité dégagées sur une année lors de l'intégration d'un nouvel employé

Que pouvez-vous faire avec Access ?

Protéger n'importe quelle application

À la fois indépendantes de l'identité et de l'origine, les solutions Cloudflare vous permettent de protéger n'importe quelle application (SaaS, dans le Cloud ou sur site), tout en continuant à travailler avec votre fournisseur d'identité préféré.

Connecter vos utilisateurs de manière flexible, avec ou sans client

Favorisez les applications web et les connexions SSH, sans logiciel client ni configuration de la part de l'utilisateur final. Pour les applications non web, les connexions RDP et le routage privé, utilisez un client complet couvrant divers scénarios d'utilisation en matière d'Internet et d'accès aux applications.

Autoriser la fédération d'identité sur plusieurs fournisseurs d'identité

Intégrez l'ensemble de vos fournisseurs d'identité professionnels (Okta, Azure AD et bien d'autres) pour un processus de migration, d'acquisition et d'accès des utilisateurs tiers plus sûr. Déployez des codes confidentiels à usage unique pour les accès temporaires ou intégrez les sources d'identité sociales, comme LinkedIn et GitHub.

Limiter les mouvements latéraux entre les ressources de l'entreprise

Déployez des méthodes d'authentification robustes et cohérentes, comme le pare-feu IP et les règles Zero Trust, même sur les applications plus anciennes.

Appliquer des politiques d'accès tenant compte des appareils

Avant d'accorder un accès, évaluez la stratégie de sécurité, notamment la présence d'un client Gateway, d'un numéro de série et d'un certificat mTLS, afin de vous assurer que seuls les appareils connus et sécurisés peuvent se connecter à vos ressources. Intégrez le niveau de sécurité des appareils issu de vos fournisseurs EPP (Endpoint Protection Platform, plate-forme de protection des points de terminaison), notamment Crowdstrike, Carbon Black, Sentinel One et Tanium.

Consigner l'activité des utilisateurs sur l'ensemble des applications

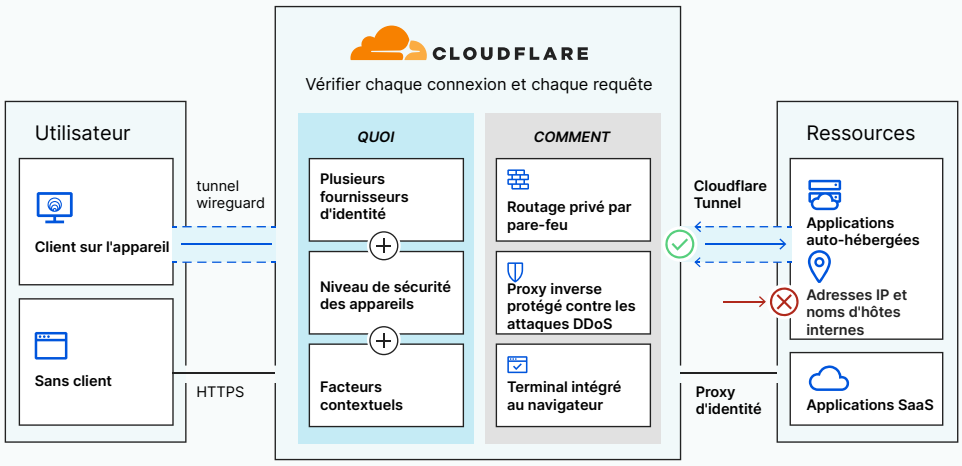
Consignez toutes les requêtes effectuées dans vos applications protégées, pas uniquement les connexions et les déconnexions. Regroupez vos journaux d'activité au sein de Cloudflare ou exportez-les vers votre fournisseur SIEM.

[1]Lorsque l'accès réseau Zero Trust est associé à la navigation sur Internet

La différence Cloudflare

- **Notre solution aux performances imbattables** achemine les requêtes plus rapidement sur le réseau Anycast de Cloudflare grâce à un routage optimisé et intelligent. L'accès aux applications web se révèle en moyenne 30 % plus rapide et le temps aller-retour des connexions TCP diminue de 17 %. Notre corpus d'informations repose sur l'analyse des données réseau issues d'un ensemble couvrant 25 millions de requêtes HTTP par seconde et 39 000 nouvelles connexions par seconde.
- **Notre gestion simplifiée** allie, parmi bien d'autres, nos solutions d'accès réseau Zero Trust, de passerelle web sécurisée (Secure Web Gateway) et d'isolation du navigateur (Remote Browser Isolation) au sein d'un plan de contrôle unique. Intégralement conçue par nos soins, l'expérience d'administration qui en résulte s'avère cohérente, car elle ne provient pas d'une démarche d'acquisition et d'assemblage (« acquire-and-stitch ») de plusieurs fournisseurs.
- **L'inspection en une seule passe** permet de vérifier, de filtrer, d'isoler et d'inspecter le trafic de manière rapide et cohérente dans le monde entier. En effet, chaque service Cloudflare est déployé dans chacun des datacenters qui composent notre réseau, couvrant plus de 200 sites à travers le monde.

Fonctionnement



Au lieu de passer par un VPN, les utilisateurs se connectent aux ressources de l'entreprise par l'intermédiaire d'un client ou de leur navigateur web. Les requêtes acheminées et accélérées en périphérie du réseau Cloudflare sont évaluées en fonction de règles Zero Trust intégrant des signaux issus de vos fournisseurs d'identité, de vos appareils et d'autres contextes. Là où les logiciels RDP, les applications de visionnage de fichiers SMB et les autres programmes client lourds nécessitaient l'usage d'un VPN pour bénéficier d'une connectivité réseau privée, les équipes peuvent désormais acheminer tout le trafic TCP ou UDP de manière privée via le réseau Cloudflare. Le trafic y est accéléré, vérifié et filtré en une seule passe, favorisant ainsi l'accroissement des performances et de la sécurité.

« Cloudflare Access nous a épargné la peine de devoir développer notre propre système de gestion de l'identité et des accès (IAM). Nous n'avons pas à intégrer de fonctions d'authentification des utilisateurs dans les applications protégées par Access. Nous avons opté pour la formule intégrale, au sein de laquelle chaque employé de l'entreprise dispose d'une place sur Access. »

Jim Tyrell
Directeur de l'infrastructure, Canva

« Chez Delivery Hero, nous nous efforçons de toujours offrir une expérience extraordinaire à nos clients. Cloudflare Access nous aide à faire de même pour nos équipes internes. En leur offrant un environnement de travail sécurisé, elles n'ont plus besoin d'un VPN pour accéder à l'ensemble de nos applications à travers le monde. »

William Carminato
Directeur principal de l'ingénierie, Delivery Hero

Intégrations de plates-formes de gestion des identités et des accès (IAM, Identity and Access Management)

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML OIDC

Intégrations de plates-formes de protection des points de terminaison (EPP, Endpoint Protection Platforms)

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

Caractéristiques principales

Politique cohérente	
Politiques personnalisées en matière d'accès aux applications, au réseau privé et à Internet	**Illimitées**
Authentification par fournisseurs d'identité sociaux et professionnels	✓
Définition du niveau de sécurité des appareils à l'aide d'intégrations d'outils tiers et de Cloudflare	✓
Importation groupée de listes (au format CSV) des numéros de série des appareils de l'entreprise	✓

Amélioration de la visibilité	
Conservation des logs d'activité	**6 mois**
Affichage des détails relatifs au pays, à l'État et à l'appareil en fonction de l'identité	✓
Transfert des logs vers un espace de stockage dans le cloud ou des SIEM	✓

Connectivité sécurisée	
Connexions vers Internet chiffrées à l'aide d'un client (client WARP)	**Windows, Mac, iOS, Android**
Accès sécurisé sans client aux applications auto-hébergées et SaaS	✓
Connexions privées pour les applications autohébergées, les adresses IP et les noms d'hôtes internes (Cloudflare Tunnel)	✓

Interopérabilité simple	
Intégrations de solutions de gestion de la mobilité et des points de terminaison	✓
Split-Tunneling, pour une connectivité locale ou par VPN	✓
Auto-inscription au client pour les appareils non gérés	✓
Lanceur d'applications personnalisable	✓
Prise en charge de plusieurs fournisseurs d'identité en simultané pour l'authentification	✓
Connecteurs génériques et personnalisés pour prise en charge des normes SAML et OIDC	✓
Authentification par jeton pour les services automatisés	✓
Authentification reposant sur des certificats pour l'IdO et les autres scénarios d'utilisation mTLS	✓

Aucun compromis sur les performances	
Garantie de disponibilité dans le cadre du SLA	**100 %**
L'un des réseaux les plus rapides (moins de 50 ms de plus de 250 points de présence)	✓
Résolveur DNS ultrarapide, privilégiant la confidentialité (7-31 ms via plus de 250 points de présence)	✓
Mise à jour ultrarapide des politiques (moins de 500 ms sur plus de 250 points de présence)	✓
Navigateur à distance ultra-rapide (pas de Pixel Pushing – exécution sur notre réseau, pas dans un Cloud tiers)	**Service supplémentaire**

Vous souhaitez en savoir plus ?

Rendez-vous sur www.cloudflare.com/fr-fr/products/zero-trust/access/ pour créer un compte, gratuit jusqu'à 50 utilisateurs.