Comment Cloudflare Access remplace un VPN

L'avènement du télétravail a pris de nombreuses entreprises au dépourvu. De nombreuses organisations n'ont acheté des licences de VPN et des équipements qu'en nombre suffisant pour couvrir les besoins d'une partie de leurs équipes. L'essor du télétravail exerce une pression considérable sur ces deux ressources.

Cloudflare Access vous aide à réduire la pression exercée sur votre VPN avec une solution d'authentification moderne pour vos applications gérées en interne. Access protège les applications web, les connexions SSH, les ordinateurs distants et d'autres protocoles grâce au réseau mondial de Cloudflare, qui évalue l'identité de chaque requête transmise à une ressource. Lorsque des applications pour entreprises sont protégées par Access, elles se comportent comme des applications SaaS et offrent aux employés une procédure de connexion simple et cohérente.

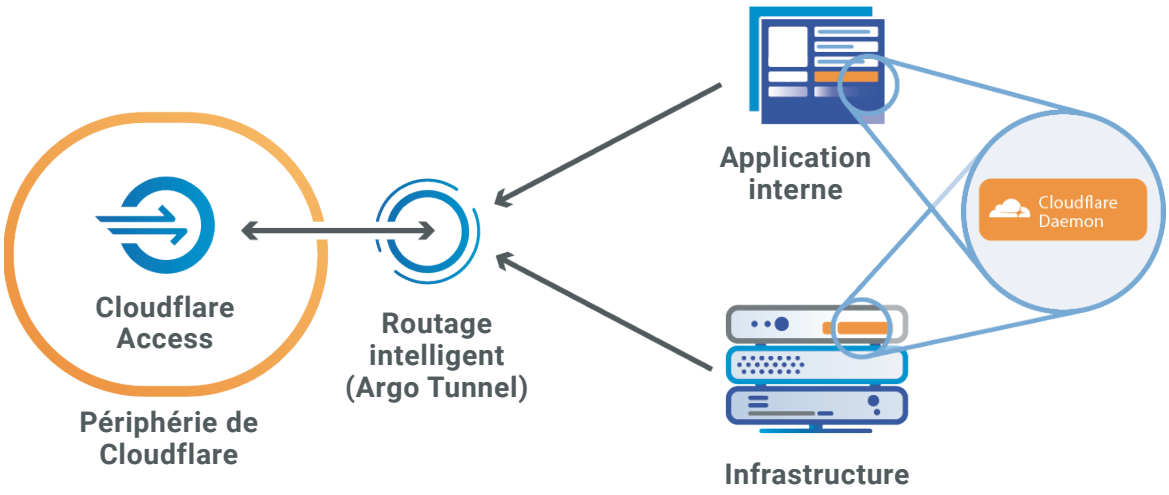
Voici comment Cloudflare Access permet de remplacer un VPN par le réseau de Cloudflare.

1. Cloudflare Access connecte les outils internes à Internet, en toute sécurité

Les équipes connectent leurs ressources à Access via Argo Tunnel, une connexion sortante sécurisée. Celle-ci s'exécute sur votre infrastructure pour connecter vos applications et vos équipements à Cloudflare. Argo Tunnel permet de sécuriser l'exposition des serveurs web à Internet, sans ouvrir de ports de pare-feu ni configurer de listes de contrôle d'accès.

Ce tunnel effectue uniquement des appels sortants vers le réseau Cloudflare.

Peu importe que vos applications soient exécutées sur site ou hébergées chez un fournisseur de services de Cloud : Argo Tunnel peut connecter votre infrastructure à Cloudflare.

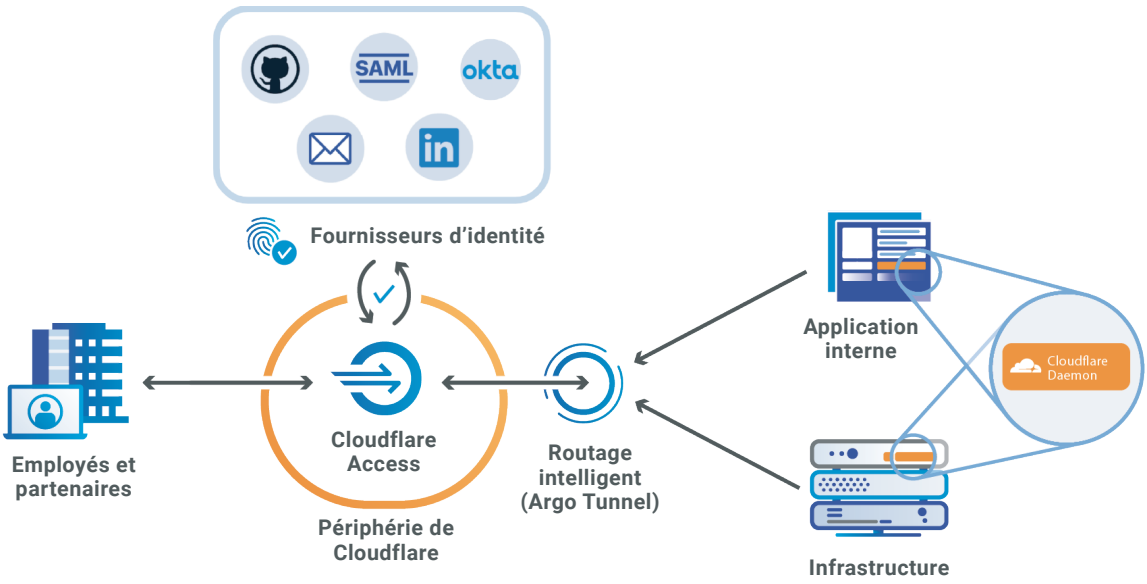


2. Les requêtes adressées à des ressources protégées sont acheminées via la périphérie de Cloudflare

Argo Tunnel utilise Argo Smart Routing pour acheminer, sur le chemin le plus rapide du réseau Cloudflare, le trafic entre l'utilisateur et les data centers les plus proches du serveur d'origine.

Les data centers de Cloudflare offrent un temps de réponse inférieur à 100 millisecondes à 99 % de la population connectée à Internet dans les pays industrialisés.

Lorsqu'une requête adressée à vos ressources atteint la périphérie de Cloudflare, Access se comporte comme un videur placé devant la ressource, qui détermine quelles requêtes sont autorisées à passer.

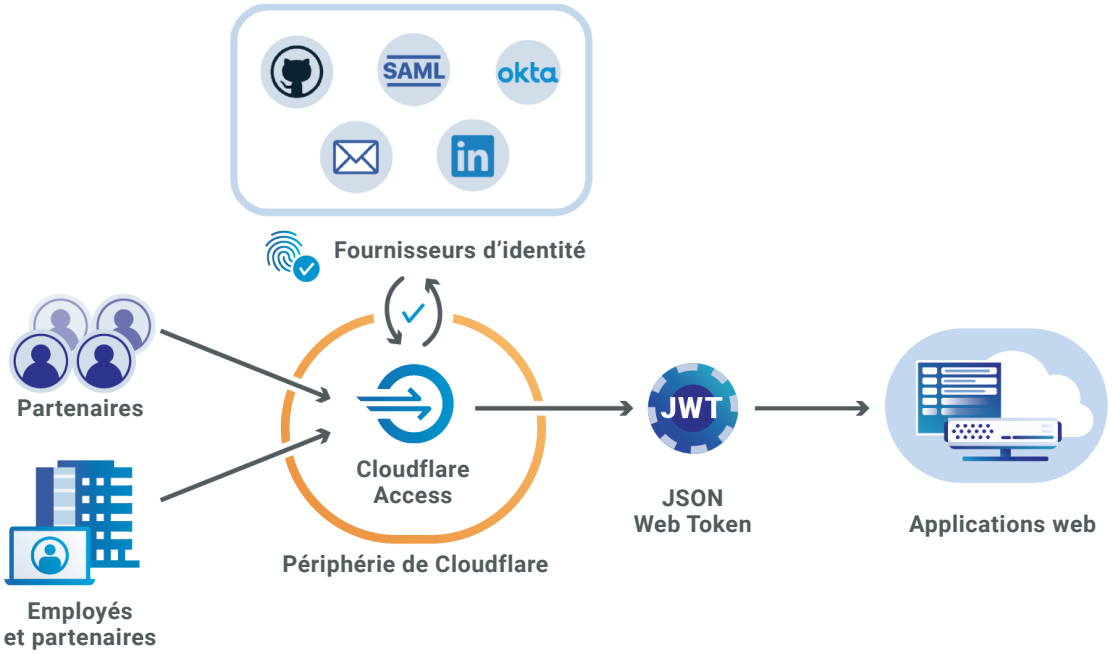


3. À la périphérie de Cloudflare, Access applique les stratégies définies par votre fournisseur d'identité (IdP) pour autoriser ou bloquer les requêtes

L'intégration de Cloudflare Access au fournisseur d'identité de votre entreprise permet de déterminer l'identité des utilisateurs. Lorsque les utilisateurs se connectent à une application protégée par Access, ils sont invités à se connecter avec le fournisseur d'identité configuré.

Access prend en charge les fournisseurs gérés par votre équipe tels qu'Okta©, G Suite© et AzureAD©, ainsi que les fournisseurs publics tels que LinkedIn© et GitHub©.

Access vous permet d'utiliser plusieurs fournisseurs d'identité simultanément, notamment les instances de même type.



Ce que vous pouvez protéger avec Access

Les connexions SSH

Le protocole Secure Shell (SSH) permet aux utilisateurs de se connecter à votre infrastructure pour effectuer des activités telles que l'exécution de commandes à distance. Cloudflare Access permet de sécuriser les connexions via le protocole Secure Shell (SSH). Lorsque les utilisateurs tentent d'accéder à des ressources au moyen de lignes de commande, Access ouvre une fenêtre de navigateur les invitant à se connecter avec leur fournisseur d'identité

Applications web

Utilisez Access pour protéger les applications gérées en interne telles que Jira, WordPress, GitLab et SAP, afin que les utilisateurs puissent se connecter et accéder à celles-ci sans VPN. Cloudflare Access évalue les requêtes transmises à votre application et détermine si le trafic des visiteurs est autorisé conformément aux stratégies que vous avez définies.

Ordinateurs distants

Le protocole RDP (Remote Desktop Protocol) permet aux utilisateurs de se connecter à un ordinateur depuis une autre machine. Cloudflare Access permet aux utilisateurs finaux de s'authentifier auprès de leur fournisseur d'authentification unique (SSO) et de se connecter à des fichiers partagés via RDP, sans devoir se connecter à un VPN.

Autres protocoles

Access vous permet d'ajouter un mécanisme d'authentification aux partages de fichiers SMB (Secure Messaging Block) ou aux applications qui utilisent des ports TCP arbitraires.

Fournisseurs d'identité pris en charge

L'intégration de Cloudflare Access au fournisseur d'identité de votre entreprise permet de déterminer l'identité des utilisateurs. Lorsque les utilisateurs se connectent à une application protégée par Access, ils sont invités à se connecter avec le fournisseur d'identité configuré. Les entreprises peuvent utiliser plusieurs fournisseurs d'identité à la fois, sans restriction.

- GSuite©
- Okta©
- Microsoft Azure AD©
- Centrify©
- Yandex©
- Citrix ADC©
- Facebook©
- Generic OIDC©
- GitHub©
- Google©
- JumpCloud SAML©
- KeyCloak SAML©
- LinkedIn©
- PingIdentity©
- OneLogin (OIDC et SAML)©
- One Time Pin (OTP) Login©
- Atlassian© Jira et Confluence SSO
- Redash©

Souscrivez dès aujourd'hui un abonnement Access sur teams.cloudflare.com