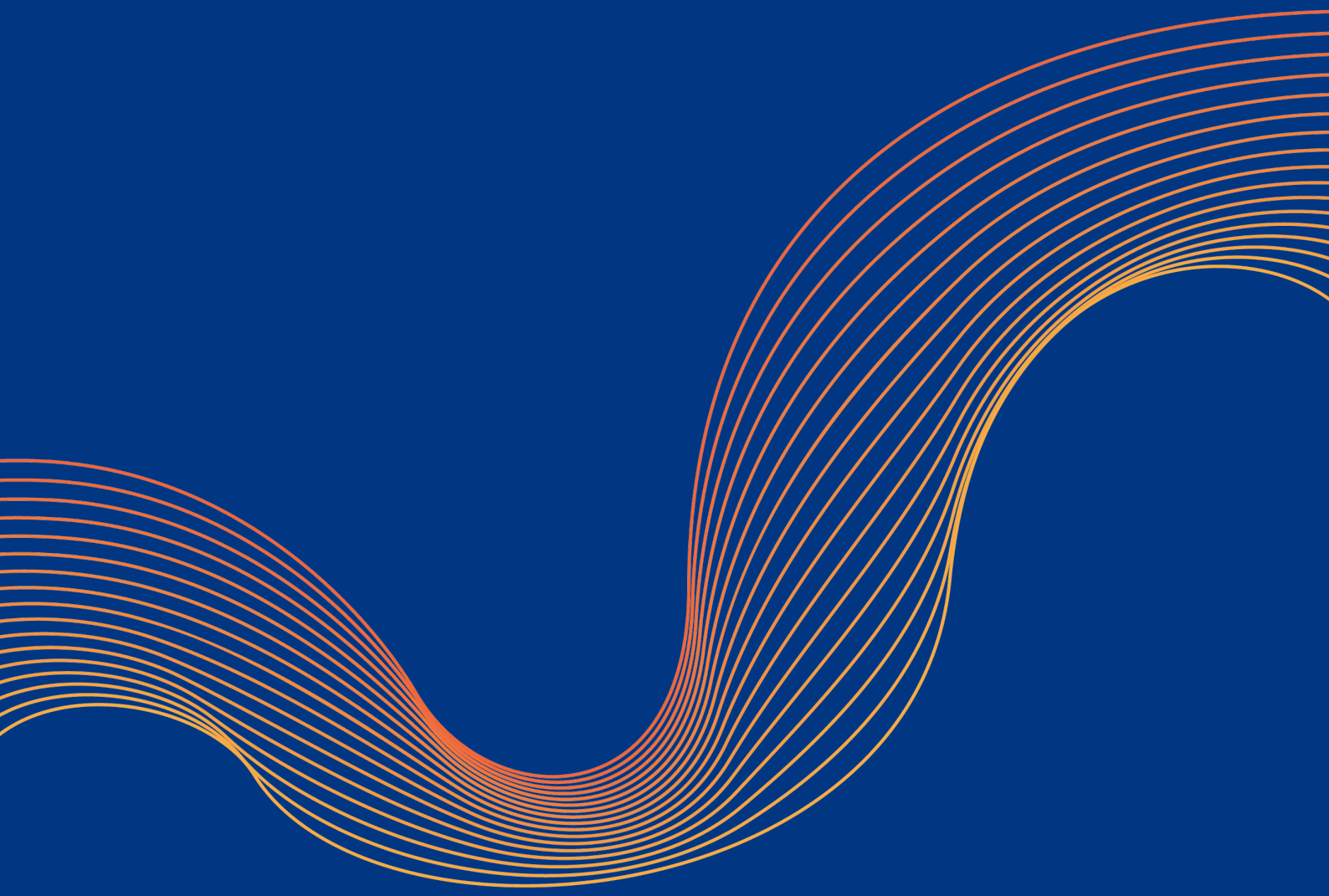
LIVRE BLANC

CLOUDFLARE

Le ZTNA peut-il remplacer votre VPN ? Comparez trois approches de l'accès à distance



+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

INDEX

INTRODUCTION

Un accès à distance sécurisé et fluide constitue un atout pour l'entreprise : il dynamise la productivité des utilisateurs distants et réduit le temps que consacrent les équipes informatiques à l'intégration et à la maintenance de la connectivité entre utilisateurs et applications, le tout avec agilité et résilience. L'accès à distance demeure néanmoins un défi pour de nombreuses entreprises.

Les VPN proposaient autrefois un moyen simple de connecter une poignée d'utilisateurs distants aux réseaux d'entreprise, pendant de courtes périodes. Toutefois, plus les effectifs se trouvaient dispersés (et plus les entreprises devaient maintenir la connexion des utilisateurs distants pendant des périodes prolongées), plus les défauts de cette approche devenaient évidents, de la baisse des performances générales à l'accroissement des risques envers la sécurité, en passant par les problèmes d'évolutivité.

À mesure que les besoins d'accès à distance augmentent, les entreprises délaissent de plus en plus le déploiement de VPN traditionnels au profit de solutions d'accès à distance plus sûres et plus performantes. L'accès réseau Zero Trust (ou ZTNA, Zero Trust Network Access) établit des frontières sécurisées autour d'éléments spécifiques (applications, adresses IP privées et noms d'hôtes). Il remplace ainsi les connexions VPN autorisant l'accès par défaut et leur substitue des politiques refusant l'accès par défaut, mais accordant ce dernier en fonction de l'identité et du contexte.

Près de 5 % de l'ensemble des accès à distance ont principalement été assurés par le ZTNA en 2020. Toutefois, en raison des limites d'accès imposées par les VPN traditionnels et de la nécessité de proposer des mesures plus précises de contrôle des accès et des sessions, ce chiffre devrait bondir à 40 % d'ici 2024.[1]

Si les solutions de ZTNA offrent plusieurs avantages évidents (et des fonctionnalités étendues) par rapport aux VPN, de nombreuses entreprises ont découvert qu'elles ne remplaçaient pas totalement l'infrastructure VPN. La situation évolue toutefois rapidement, à mesure que les déploiements ZTNA deviennent plus robustes et les VPN plus problématiques. Cet article compare les VPN et les solutions d'accès à distance ZTNA afin de mettre en lumière leurs avantages et leurs limites, tout en présentant les considérations les plus importantes pour les projets de migration. Il détaille la manière dont Cloudflare propose le ZTNA et préconise un ensemble d'étapes concrètes à suivre pour passer d'une infrastructure VPN existante à un modèle de connectivité Zero Trust, plus rapide et plus sûr pour les utilisateurs distants.

[1] *Riley, Steve, MacDonald, Neil, et Orans, Lawrence. « Market Guide for Zero Trust Network Access » (rapport sur le marché de l'accès réseau Zero Trust), Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. Dernier accès le 21 juin 2021. Consultez le tableau 1 pour plus de détails.*

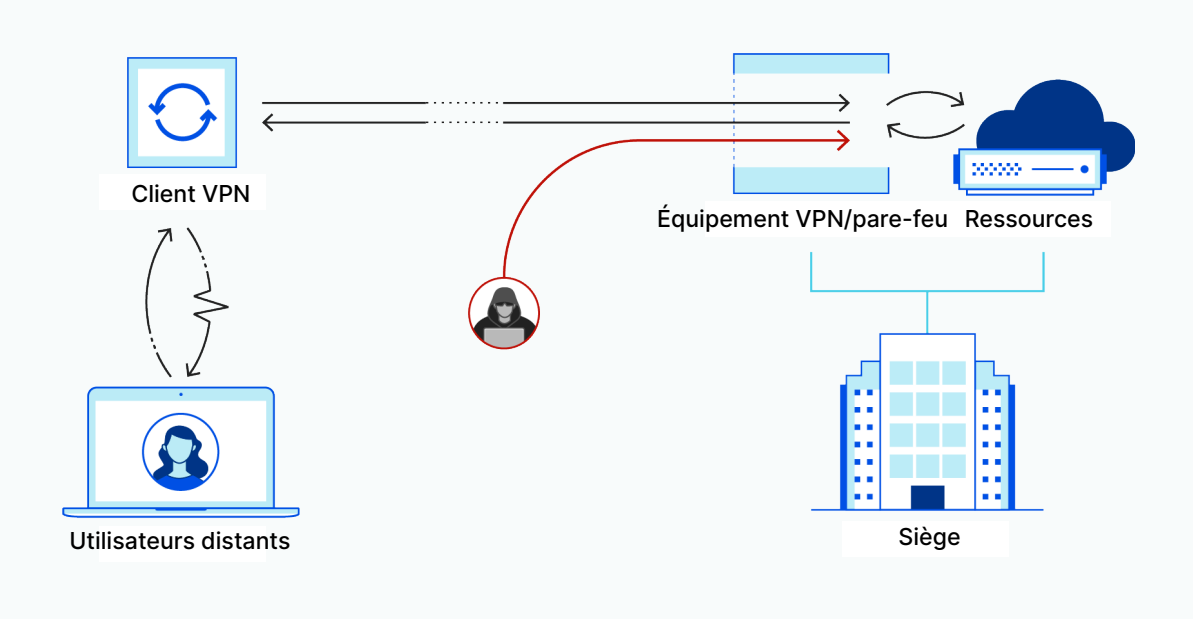
APPROCHE Nº 1 : VPN TRADITIONNEL

Depuis des décennies, les VPN permettent aux entreprises de connecter leurs utilisateurs distants aux réseaux d'entreprise avec un certain niveau de confidentialité et de sécurité. Les VPN permettent aux utilisateurs d'accéder en toute sécurité aux ressources internes par l'intermédiaire d'une connexion chiffrée, plutôt que de les laisser accéder aux informations sensibles via l'Internet public (sur lequel n'importe quel pirate informatique pourrait espionner ou dérober des données).

Les VPN avec client et les VPN sans client constituent les deux modes de déploiement VPN les plus courants. Chaque approche comporte ses propres avantages et ses propres défis :

Les VPN avec client connectent les utilisateurs distants à un réseau privé via un tunnel chiffré. Cette connexion est établie par l'intermédiaire d'une application logicielle (ou client), qui nécessite que les utilisateurs s'authentifient une fois à l'aide d'un nom d'utilisateur et d'un mot de passe afin d'obtenir un accès persistant à toute ressource située sur ce réseau.	**Avantage :** une fois la connexion établie, la liberté de mouvement latéral permet aux utilisateurs d'accéder rapidement à plusieurs ressources par l'intermédiaire des applications et en se connectant aux hôtes internes. **Défis :** • **Approche non conçue pour les utilisateurs nomades et les appareils mobiles**. Les ordinateurs portables et les appareils mobiles se reconnectent en toute fluidité aux divers réseaux sans fil, afin de suivre les déplacements des utilisateurs passant d'un endroit à un autre. Les clients VPN ne gèrent toutefois pas ces reconnexions de manière fluide. Les utilisateurs se voient donc contraints de forcer le redémarrage du client VPN à plusieurs reprises, avant de s'authentifier à nouveau. Ce processus entraîne ainsi une perte de productivité et la création de nouveaux tickets informatiques. • **Mauvaise visibilité.** Avec cette méthode, l'infrastructure VPN place le point de terminaison du tunnel chiffré créé par le client VPN derrière le pare-feu interne du datacenter. Si ces connexions sont journalisées, aucun log centralisé et spécifique à une application n'indique pas à quelle application les utilisateurs ont accédé ni les actions que ces derniers ont effectuées au sein de l'application.

Les portails VPN basés sur le SSL sans client permettent à un nombre restreint d'utilisateurs distants de se connecter à quelques applications pour navigateur exécutées au sein d'un réseau privé. Ce type de connexion est rendu possible grâce à un serveur web intégré à l'équipement réseau et exécutant le service VPN.	**Avantage :** au lieu de passer par un client sur appareil, un navigateur web peut utiliser le certificat SSL du portail afin d'établir une connexion HTTPS chiffrée et d'assurer la prise en charge des sous-traitants sur des appareils non gérés. **Défis :** • **Problématiques de sécurité.** La plupart des configurations VPN au sein du datacenter accordent un accès total aux utilisateurs. Cette démarche pose un problème aux entreprises qui ne souhaitent pas que le personnel non salarié (comme les sous-traitants) dispose d'un accès illimité aux ressources et aux applications sensibles. • **Approche non conçue pour prendre en charge un grand nombre d'utilisateurs simultanés.** Contrairement aux services cloud modernes, le serveur web du portail ne peut pas évoluer de manière élastique pour répondre à une demande plus importante. L'extension du portail nécessite à la place l'installation d'un plus grand nombre d'équipements réseau et l'équilibrage de leur charge. Cette solution s'avère souvent coûteuse complexe et inefficace, car les autres fonctionnalités de l'équipement peuvent être sous-utilisées. • **Les portails VPN basés sur le SSL sans client exposent les ports des pare-feu et des serveurs web aux attaques.** Pour permettre au serveur web hébergeant le portail d'accéder aux applications internes, les administrateurs doivent ouvrir les ports entrants du pare-feu, qui se retrouvent exposés aux attaques de l'extérieur. Les ports ouverts et le serveur web lui-même doivent être protégés contre les attaques DDoS et les attaques conduites par des applications web. La sécurisation de cette méthode de connexion entraîne donc une configuration plus complexe et se révèle plus coûteuse.



Si les VPN proposent un niveau de confidentialité basique aux utilisateurs distants, ils n'ont pas été conçus dans une optique de sécurité ou d'évolutivité. Traditionnellement, les entreprises utilisent les VPN pour connecter une poignée d'utilisateurs distants au réseau de l'entreprise pendant de courtes périodes. Toutefois, dans un contexte d'expansion du télétravail, les problèmes liés aux VPN commencent à se multiplier :

- **Les utilisateurs souffrent de performances médiocres.** Si l'infrastructure VPN ne dispose pas de la capacité de gérer le débit du trafic et les connexions simultanées provenant du propre personnel de l'entreprise, les utilisateurs constateront un ralentissement de leur connexion Internet. Par ailleurs, lorsqu'un VPN se situe à bonne distance de l'utilisateur et du serveur d'applications auquel l'utilisateur tente d'accéder, le temps de transfert en résultant génère une certaine latence.
- **Les réseaux d'entreprise restent vulnérables aux attaques.** Les VPN s'appuient généralement sur un modèle de type « château et douves », au sein duquel un utilisateur peut accéder librement à toutes les ressources de l'entreprise lorsqu'il se connecte à un réseau. En l'absence de méthode intégrée de restriction des accès aux infrastructures et aux données stratégiques, les entreprises sont contraintes de configurer des services de sécurité complexes et coûteux, comme des pare-feu de nouvelle génération et des mesures de contrôle des accès au réseau. Sans ces dispositifs, elles resteraient vulnérables aux mouvements latéraux malveillants, susceptibles d'entraîner des violations de données plus importantes.

Le défi posé par les services VPN hébergés

Certains fournisseurs ont déplacé l'équipement réseau exécutant le service VPN vers le cloud public, où il fonctionne comme une machine virtuelle dans un ou plusieurs datacenters. Le VPN peut ou non être regroupé (ou chaîné) à des services de sécurité supplémentaires.

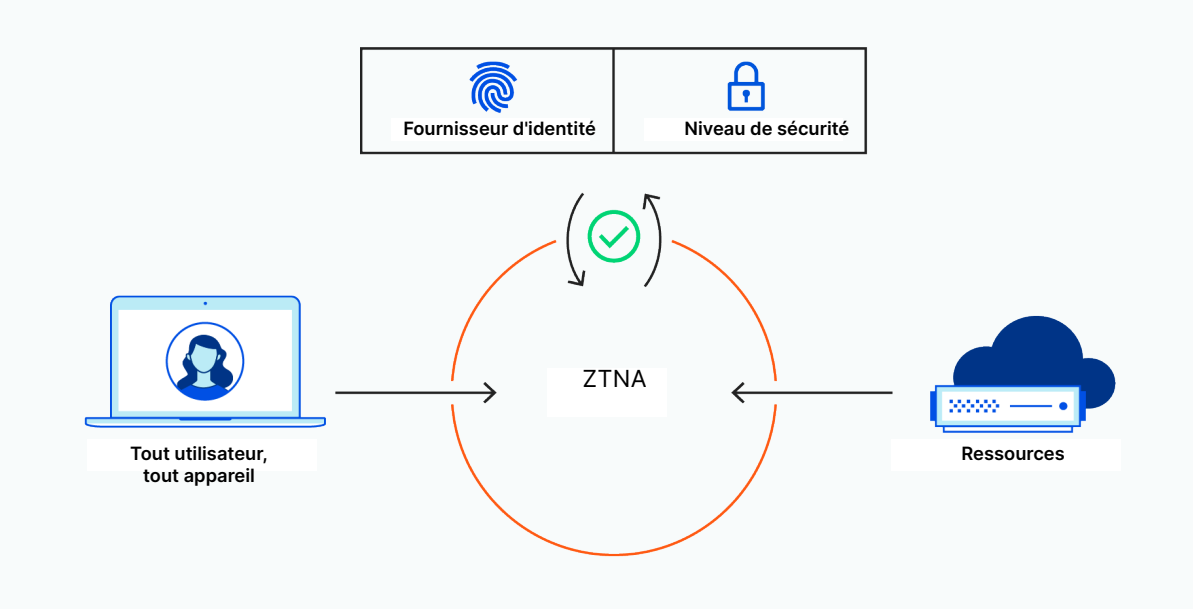
La migration d'un VPN vers le cloud peut donner l'impression de résoudre certains problèmes d'évolutivité inhérents aux équipements VPN physiques. Toutefois, cette approche présente également des défis importants en matière de sécurité et d'évolutivité.

Prenons l'exemple d'une entreprise qui héberge un pare-feu de nouvelle génération (NGFW, Next-Generation Firewall) complet, combinant une solution VPN à un pare-feu et des fonctionnalités de sécurité supplémentaires. Comme le pare-feu de nouvelle génération est proposé sous forme de service groupé, il s'avère impossible de faire évoluer une fonctionnalité spécifique à la demande, de manière indépendante. L'extension d'une fonction nécessite ainsi de faire évoluer l'ensemble du service. Pour ce faire, d'autres machines virtuelles doivent être déployées de manière à équilibrer la charge représentée par l'exécution d'une petite quantité de calcul sur chaque machine virtuelle. Cette solution se montre peu pratique et peu maniable, mais se révèle également susceptible d'entraîner des coûts élevés face à l'expansion constante des besoins de l'entreprise en matière d'accès à distance.

APPROCHE Nº 2 : ACCÈS RÉSEAU ZERO TRUST

La sécurité Zero Trust permet de contourner de nombreuses difficultés inhérentes aux VPN. Elle se fonde sur le principe qu'aucun utilisateur ou appareil présent sur un réseau ou extérieur à celui-ci n'est digne de confiance par défaut. Pour réduire le risque et l'impact des violations de données, des attaques internes et des autres menaces, une approche Zero Trust…

- authentifie et enregistre chaque connexion et chaque requête au sein d'un journal ;
- nécessite une vérification stricte de tous les utilisateurs et appareils ;
- limite les informations auxquelles peuvent accéder chaque utilisateur et chaque appareil, en fonction de l'identité et du contexte ;
- et ajoute une couche de chiffrement de bout en bout afin d'isoler les applications et les données surle réseau.



Comme pour les VPN, le ZTNA offre différentes possibilités de configuration :

1. **Le ZTNA sans client (ou initié par un service)** s'appuie sur le navigateur existant, plutôt qu'un client, pour établir une connexion sécurisée et authentifier les appareils des utilisateurs. Traditionnellement, le ZTNA sans client était limité aux applications basées sur le protocole HTTP/HTTPS, mais la compatibilité évolue rapidement.[2]
   - **Avantage :** le ZTNA sans client met en œuvre une connexion par proxy inverse pour prévenir l'accès direct aux applications, empêchant ainsi les utilisateurs d'accéder à des applications et des données qu'ils peuvent ne pas être autorisés à consulter. Cette solution confère également un plus grand degré de contrôle et de flexibilité aux administrateurs dans leurs tâches de gestion.
2. **Le ZTNA avec client (ou initié par un point de terminaison)** installe un logiciel sur l'appareil d'un utilisateur avant qu'une connexion chiffrée puisse être établie entre l'agent de contrôle et les applications autorisées.
   - **Avantage :** le ZTNA avec client permet aux administrateurs d'avoir un meilleur aperçu de la posture de l'appareil, de la position géographique et du contexte de risque des utilisateurs qui accèdent aux applications. Cette approche permet ainsi la création et l'application de politiques plus détaillées. En outre, comme cette méthode ne se limite pas au HTTP/HTTPS, elle peut servir à accéder à un plus grand nombre d'applications non HTTP, telles que celles qui s'appuient sur les protocoles SSH, RDP, VNC, SMB et d'autres connexions TCP.

[2] Depuis juin 2021, la solution ZTNA de Cloudflare prend en charge l'accès sans client aux applications SSH et VNC. La prise en charge du protocole RDP est prévue à l'avenir.

Les défis liés à la mise en œuvre du ZTNA

Si le ZTNA présente des avantages manifestes par rapport aux VPN traditionnels, il ne constitue pas une approche sans faille en matière de sécurisation de l'accès réseau des utilisateurs distants. À l'heure où les entreprises évaluent les avantages et les inconvénients de l'adoption du Zero Trust, elles peuvent se heurter à un ou plusieurs des défis suivants :

Les solutions ne sont pas vraiment cloud-native.

Si un fournisseur ne propose pas de ZTNA fondé sur le cloud (c'est-à-dire que ses clients doivent déployer le logiciel au sein de leurs propres datacenters), les utilisateurs ne bénéficient alors pas de certains avantages essentiels, comme l'évolutivité instantanée et le débit illimité.

Les fournisseurs peuvent ne pas proposer d'options d'accès ZTNA avec et sans client.

Cette absence de possibilités limite la valeur pour les entreprises qui ont besoin de connecter leurs utilisateurs à des applications non HTTP, comme les bureaux à distance, les applications SSH ou les applications de partage de fichiers.

La configuration peut se révéler complexe et gourmande en temps.

Les fournisseurs qui ne proposent pas la prise en charge de l'orchestration et de l'automatisation des politiques (à l'aide d'outils tels que Terraform) risquent d'alourdir davantage le travail manuel des administrateurs, en plus des tâches de configuration déjà nécessaires au niveau du fournisseur d'identité.

L'APPROCHE CLOUDFLARE EN MATIÈRE D'ACCÈS À DISTANCE

Le processus de sécurisation et d'extension de l'accès à distance doit s'effectuer de manière fluide, sans entraîner la nécessité de superposer des solutions de sécurité encombrantes, de faire des compromis en matière de performances ou de faire face à des coûts inutiles. Cloudflare permet aux équipes de traiter tous les scénarios d'utilisation en matière d'accès à distance, avec les avantages suivants :

- **Intégration facile et sans risque pour les utilisateurs et les administrateurs.** Cloudflare s'intègre facilement aux fournisseurs d'identité existants et aux plateformes de protection des points de terminaison, afin de permettre l'application de politiques Zero Trust qui limitent l'accès aux applications et ressources de l'entreprise.
- **Flexibilité des déploiements ZTNA avec ou sans client.** Cloudflare assure la prise en charge du modèle sans client pour les connexions aux applications web, SSH, VNC (et prochainement RDP), ainsi que la prise en charge du modèle avec client des applications non HTTP et le routage privé vers les adresses IP internes.

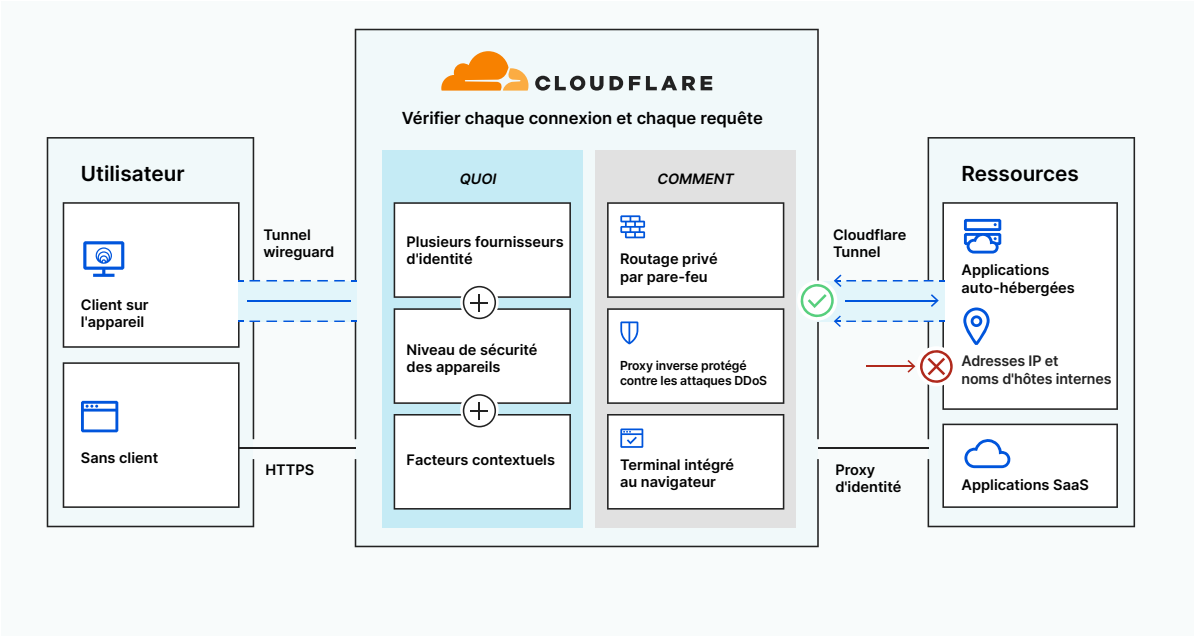


Tableau 1 : comment Cloudflare relève les défis de l'accès à distance

⚠ Problème	✓ Solution	⚙ Déploiement Cloudflare
Solutions difficiles à faire évoluer	Réseau périphérique mondial	Les problèmes d'évolutivité affectent à la fois les VPN et les services ZTNA non cloud-native. Ils compliquent l'accès des utilisateurs distants aux applications et aux données. Le réseau mondial Anycast de Cloudflare permet non seulement d'établir des connexions aux utilisateurs plus vite qu'avec un VPN, mais il garantit également la possibilité pour les équipes distantes de toutes tailles de se connecter rapidement et en toute sécurité aux ressources de l'entreprise, selon les besoins et sans nécessiter de fastidieuses opérations de configuration supplémentaires de la part des administrateurs.
Faible compatibilité avec les appareils mobiles	Client léger	Les solutions VPN et ZTNA mettant en œuvre les protocoles IPSec et SSL s'avèrent souvent peu performantes sur les appareils mobiles et itinérants. Le client Cloudflare WARP s'appuie sur le protocole Wireguard, plus moderne, et exécuté dans l'espace utilisateur, pour prendre en charge un plus vaste choix de systèmes d'exploitation et proposer une expérience utilisateur plus rapide qu'avec les options traditionnelles. Le client WARP de Cloudflare peut être configuré sur les appareils Windows, macOS, iOS, Android et, prochainement, Linux.
Pas de protection intégrée contre les attaques DDoS ou protection insuffisante	Protection contre les attaques DDoS intégrée et à la pointe du marché	En l'absence d'une protection intégrée contre les attaques DDoS, les entreprises se trouvent souvent obligées de chaîner des services de sécurité supplémentaires, une approche susceptible d'entraîner des problèmes de configuration, d'évolutivité et de sécurité. Doté d'une capacité supérieure à 67 Tb/s, le réseau Cloudflare propose une protection intégrée contre les attaques DDoS pour tous les modes ZTNA, afin de défendre les réseaux contre les attaques volumétriques les plus vastes.
Limites liées au protocole	Prise en charge des applications non web	✓ Compatibilité des modes : ZTNA sans client pour les applications SSH/VNC ; ZTNA avec client pour toutes les autres applications non web.
Pas de pare-feu réseau intégré	Pare-feu réseau intégré	La croissance des réseaux d'entreprise conditionne la dilatation de la pile d'équipements de sécurité que les entreprises doivent équilibrer, entraînant ainsi des compromis en termes de coût, de performances et de sécurité. Grâce à Cloudflare, les administrateurs peuvent appliquer des politiques de pare-feu réseau à la périphérie, qui leur confèrent un contrôle précis sur les données autorisées à entrer et à sortir du réseau, tout en améliorant la visibilité sur la circulation du trafic au sein de ce dernier. ✓ Compatibilité des modes : ZTNA avec client
Absence de contrôle précis	Passerelle web sécurisée (SWG) intégrée	L'utilisation non autorisée d'applications peut entraîner d'importants problèmes de sécurité pour les entreprises. En l'absence de politiques rigoureuses, les utilisateurs peuvent accéder à des données sensibles, ainsi qu'à d'autres ressources de l'entreprise, et les altérer. En combinant ZTNA et SWG, Cloudflare permet aux administrateurs d'exercer un contrôle plus précis sur les droits d'accès des utilisateurs et des appareils au sein des applications, afin que les utilisateurs et les groupes basés sur des rôles aient uniquement accès aux ressources nécessaires. ✓ Compatibilité des modes : ZTNA avec client

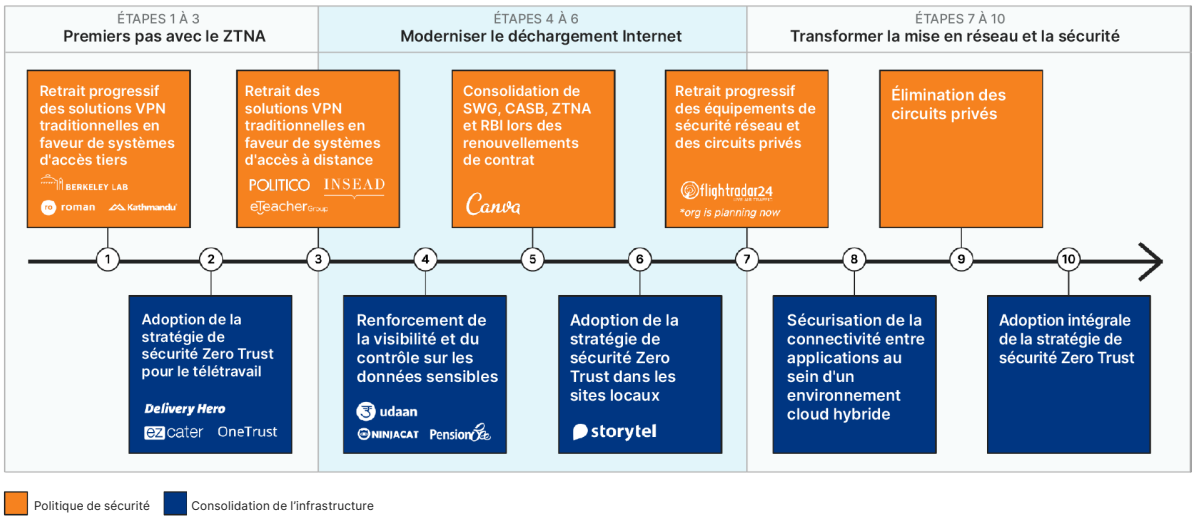
REMPLACEZ VOTRE VPN TRADITIONNEL PAR UN ACCÈS RÉSEAU ZERO TRUST

Les promesses de l'accès Zero Trust peuvent paraître vides pour les responsables de la sécurité informatique occupés par une longue et fastidieuse transition vers une sécurité sans VPN. Il reste néanmoins possible de remplacer votre solution VPN par un accès réseau Zero Trust sans faire de compromis sur la prise en charge des protocoles ou des fonctionnalités.

La méthodologie de migration recommandée varie en fonction des priorités professionnelles accordées à votre projet :

- Si vos priorités penchent vers une connectivité plus rapide aux applications, déployez d'abord un **accès ZTNA avec client pour les applications non web**.
- Si l'amélioration de la sécurité de vos règles d'accès aux applications s'avère plus importante, commencez par des **applications web**.

Le remplacement de votre VPN ne constitue que la première étape d'une transformation complète du réseau. Comme la transition vers un modèle SASE peut s'avérer difficile, nous avons défini une méthodologie commune d'évolution vers la sécurité Zero Trust en nous basant sur l'approche adoptée par nos clients :



Découvrez comment la plateforme Zero Trust de Cloudflare peut vous aider à réduire votre dépendance aux VPN et, à terme, remplacer cette solution.

En savoir plus

Découvrez un comparatif effectué à l'aide de données réelles entre les solutions VPN et ZTNA, ainsi que la manière dont Cloudflare Access renforce la sécurité de la procédure d'accès aux applications.

Regarder la démo

ANNEXE

Moderniser vos déchargements Internet

La mise en œuvre du ZTNA constitue une étape importante dans le déploiement d'un modèle SASE (Secure Access Service Edge, service d'accès sécurisé en périphérie). En tant que solution NaaS (Network-as-a-Service, réseau en tant que service) complète, **Cloudflare One** simplifie et sécurise la gestion des réseaux professionnels pour les équipes de toutes tailles. Grâce à Cloudflare One, les entreprises peuvent :

- **Adopter l'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 position géographique ou de l'identité des utilisateurs.
- **Sécuriser le trafic Internet.** Face à la rapidité de propagation des menaces sur Internet, les moyens de défense que vous employez pour les arrêter se doivent d'être plus proactifs. Cloudflare One protège vos collaborateurs en télétravail contre les menaces et applique des politiques permettant d'empêcher les fuites de données précieuses depuis votre entreprise, grâce à l'application d'une solution Zero Trust d'isolement du navigateur sur tous les sites. Le tout en profitant d'une expérience utilisateur fluide et ultrarapide.
- **Protéger et connecter les bureaux et les datacenters.** La gestion des réseaux d'entreprise est devenue excessivement complexe et le trafic des utilisateurs doit souvent effectuer plusieurs sauts avant d'atteindre sa destination. Avec Cloudflare One, les entreprises peuvent protéger leurs bureaux et leurs datacenters à l'aide d'une plateforme cloud unifiée et cohérente.

Pour en savoir plus sur Cloudflare One, regardez cette vidéo de 10 minutes combinant présentation et démonstration de la solution.

Transformez votre réseau

Les offres Zero Trust et WAN-as-a-Service de Cloudflare convergeront bientôt pour former une offre unique, qui permettra à vos collaborateurs d'accéder en permanence aux ressources de l'entreprise, quel que soit l'endroit où ils travaillent.

À l'heure actuelle, vos produits VPN et WAN permettent à vos employés d'accéder à des ressources situées sur votre réseau d'entreprise privé, mais vous contraignent à gérer de manière distincte les politiques de connectivité et de sécurité.

Cloudflare propose désormais un plan de contrôle unifié, afin de vous offrir davantage de flexibilité concernant l'application des mêmes politiques de sécurité Zero Trust à l'ensemble de votre personnel et sur l'ensemble de votre lieu de travail, sans devoir jongler avec plusieurs produits spécifiques.

Pour en savoir plus, rendez-vous sur https://www.cloudflare.com/fr-fr/cloudflare-one/.