CLOUDFLARE

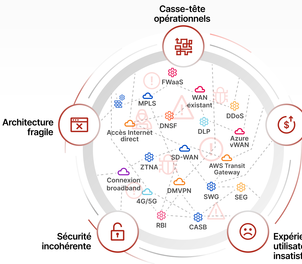
Chaque itinéraire compte

Est-il temps pour vous de rediriger vos flux de trafic réseau ?

Les réseaux d'entreprise d'ancienne génération se concentraient uniquement sur la connectivité et la sécurité internes. Or, le travail hybride, les applications déployées dans le cloud et les investissements rapides en matière de modernisation numérique ont radicalement modifié le lieu et la manière dont les flux réseau circulent.

Qu'arriverait-il si l'infrastructure réseau n'était pas prête à répondre aux exigences opérationnelles d'aujourd'hui ?

Les réseaux d'entreprise existants rencontrent souvent les problèmes ci-dessous :



52 %

52 % des dirigeants déclarent que **la complexité est le principal obstacle** aux opérations de sécurité.[1]

70 %

70 % des CEO à travers le monde déclarent que le niveau de **maturité de leur réseau affecte négativement** la prestation de leurs services.[2]

101 %

Ce chiffre de 101 % constitue le **ROI moyen des entreprises plateformisées** contre 28 % pour celles qui n'ont pas adopté la plateformisation.[1]

Dans les architectures traditionnelles, **l'utilisation de dizaines de solutions différentes pour couvrir les quatre types de flux composant le trafic réseau** ajoute également de la complexité.

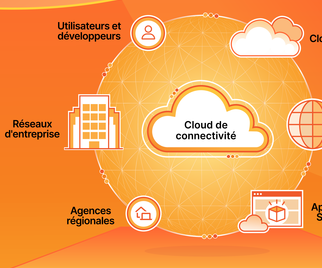
Flux de trafic	Produits requis	Problématiques
Trafic entrant depuis Internet	Trafic traditionnellement protégé par des pare-feu sur site, des VPN, l'infrastructure DMZ et le filtrage par le FAI	• Attaques DoS et DDoS • Exploitations zero-day • Phishing • Logiciels malveillants
Trafic sortant vers Internet et les applications basées sur le cloud	Trafic traditionnellement protégé par des pare-feu et des proxys sur site	• Mouvements latéraux • Exposition des données • Propagation des rançongiciels • Intégration à un botnet
Connectivité WAN dans les campus et les agences régionales	Trafic traditionnellement protégé par la connectivité réseau physique/virtualisée, le SD-WAN, les interconnexions privées et le MPLS	• Augmentation des CapEx/ OpEx • Latence du réseau • Limites de bande passante • Expérience utilisateur insatisfaisante
Multicloud pour les applications déployées sur plusieurs clouds	Trafic traditionnellement protégé par des produits « maison »	• Problèmes de visibilité et d'application des stratégies • Complexité réglementaire

Qu'est-ce qui doit changer ?

Réseaux traditionnels	CONTRE	Réseaux modernes
• L'intégration d'équipements dans le but d'ajouter de nouvelles fonctionnalités ou de couvrir de nouvelles régions géographiques nécessite des épisodes d'indisponibilité et d'interruption de service. • Connexion et sécurisation des utilisateurs et des agences régionales aux applications hébergées au sein du datacenter. • Trafic implicitement considéré comme « fiable » au sein du périmètre. • Ils ont été optimisés de manière à prendre en charge les collaborateurs sur site.		• Déployez des services composables au lieu d'équipements afin de réduire la complexité et les perturbations. • Ils doivent prendre en charge les applications sur cloud, SaaS et cloud privé, partout et à tous les niveaux. • Ils partent du principe que chaque entité est « non fiable », y compris les utilisateurs, les applications, les données et les appareils distribués. • Ils ne peuvent pas présumer de la localisation de l'utilisateur et doivent prendre en charge les utilisateurs, où qu'ils se connectent.

Comment répondre aux exigences modernes tout en prenant en charge l'ensemble des flux de trafic ?

Plutôt que de mettre en œuvre des solutions hétérogènes pour chaque branche du trafic, le cloud de connectivité aborde la modernisation du réseau de manière globale.



Trafic entrant

Protégez votre réseau et vos applications contre les attaques DDoS et les autres menaces circulant sur Internet.

Trafic sortant

Protégez vos utilisateurs et vos bureaux contre les menaces, appliquez des stratégies cohérentes et contrôlez les données au sein de vos applications.

Connectivité WAN

Connectez et sécurisez vos bureaux, vos utilisateurs, vos appareils, vos datacenters et votre infrastructure

Trafic multicloud

Assurez la connectivité réseau afin de connecter, de sécuriser et de développer des applications au sein des environnements sur cloud public/cloud hybride.

Le cloud de connectivité Cloudflare repose sur une architecture composable et programmable pour proposer des services de connectivité réseau et de sécurité à vos utilisateurs sur l'ensemble de votre infrastructure et de vos applications opérationnelles dans le cloud.

Éliminez la nécessité d'étendre ou d'agrandir vos datacenters privés.

Faites appel à des services de connectivité réseau et de sécurité basés sur le cloud, plutôt qu'à des équipements.

Réduisez la « confiance » excessive persistant sur le réseau grâce au Zero Trust.

Découvrez davantage d'informations sur la manière de simplifier et d'accélérer la modernisation réseau.

En savoir plus

1. Ali, Mohamad et Jenkins, BJ. "Capturing the cybersecurity dividend" (Récolter les bénéfices de la cybersécurité) IBM. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform". Dernier accès le 26 juin 2025.
2. "70% Of CEOs Say Their Network Is Slowing Business Growth, New NTT Study Finds" (70 % des CEO déclarent que leur réseau ralentit la croissance de l'entreprise, selon une nouvelle étude de NTT), Business Wire, 20 octobre 2022. https://www.businesswire.com/news/home/20221020005101/en/70-Of-CEOs-Say-Their-Network-Is-Slowing-Business-Growth-New-NTT-Study-Finds. Communiqué de presse.

01 73 01 52 44 | emeanprospect@cloudflare.com | Cloudflare.com

CLOUDFLARE

RÉV. : BDES-7841.2025.JUL.31