Magic WAN

Magic WAN simplifie le parcours d'adoption SASE grâce sa connectivité point à point (any-to-any)

Évolution des architectures réseau

Internet est le nouveau réseau d'entreprise

Avec le travail hybride comme nouvelle norme et les applications en pleine migration vers le cloud, les équipes informatiques sont aux prises avec les problèmes suivants :

- **Complexité du réseau :** le provisionnement du MPLS et l'ajustement des solutions dédiées demandent trop de temps.
- **Failles en matière de sécurité :** l'accès direct à Internet contourne les mesures de sécurité et les politiques d'utilisation acceptable. Les utilisateurs et les données se trouvent dès lors en danger.
- **Coûts élevés :** les liens MPLS et les solutions de sécurité dédiées entraînent des dépenses inutiles.
- **Expérience utilisateur médiocre :** la redirection du trafic vers une pile de sécurité basée sur le périmètre engendre de la latence.

Le service Magic WAN simplifie la connectivité réseau des sites des agences régionales, des VPC multicloud ou des datacenters vers la plateforme SASE Cloudflare One. Il permet ainsi une connectivité sécurisée, performante et efficace sur le plan des coûts, capable de relever les défis du travail hybride et des déploiements multicloud pour les équipes informatiques.

Contrairement aux services rigides et coûteux, comme la connectivité réseau MPLS ou les déploiements SD-WAN bâtis sur des pare-feu sur site, la solution Magic WAN adopte une approche « léger sur le régional, fort sur le cloud » afin d'améliorer/remplacer votre architecture actuelle. Facile à déployer, elle évolue pour répondre aux divers changements des exigences opérationnelles, grâce à sa sécurité intégrée.

La solution Magic WAN connecte les emplacements réseau à la plateforme SASE de Cloudflare, de manière physique ou virtuelle. Les agences régionales, les ateliers d'usine, les magasins, les sièges sociaux et les datacenters constituent de bons exemples de sites physiques. Les emplacements virtuels, quant à eux, incluent les services de cloud public, comme AWS, Azure, GCP et OCI.

Meilleure agilité opérationnelle

Gérez la sécurité réseau et la connectivité de manière centralisée, à partir d'une seule interface. Accès direct au trafic en quelques minutes grâce à un processus de configuration sans intervention.

Une sécurité intégrée, pas ajoutée a posteriori

Bénéficiez d'une protection contre les attaques DDoS cloud-native, d'un pare-feu réseau, du SSE et d'une fonctionnalité Zero Trust, le tout étroitement intégré et proposé en tant que service.

Coûts réseau réduits

Réduisez au minimum l'empreinte de vos agences régionales et déplacez les fonctions réseau vers le cloud afin de réduire la dépendance aux déploiements MPLS coûteux et d'abandonner votre SD-WAN.

Principaux scénarios d'utilisation de Magic WAN

Rationaliser la connectivité réseau

- **Simplifiez la connectivité régionale** : remplacez les assemblages hétéroclites de circuits propriétaires et d'équipements réseau afin de router le trafic de manière sécurisée entre les agences régionales et les datacenters. Facilitez la connectivité site à site sur l'ensemble de vos emplacements grâce à l'Anycast IPSec.
- **Simplifiez la connectivité hybride et multicloud** : les entreprises disposent d'instances cloud de différents fournisseurs (p. ex. AWS, GCP, Azure, Oracle, IBM) *et* de datacenters sur site. Utilisez des mesures de contrôle centralisées pour acheminer et sécuriser le trafic sur ces divers environnements.

Renforcer la sécurité sans sacrifier les performances

- **Connectivité WAN sécurisée :** sécurisez les connexions en appliquant une politique de sécurité réseau entre vos sites (agences régionales, datacenters, etc.) reposant sur des mesures de contrôle SWG et un pare-feu proposés via le cloud.
- **Faites évoluer les performances de votre WAN :** les déploiements MPLS sont coûteux, rigides et lents. La migration vers Cloudflare vous permet de diminuer les coûts et de profiter d'un déploiement plus agile, grâce à sa sécurité intégrée.

Approcher le déploiement de Magic WAN

La transformation réseau est un parcours

La solution Magic WAN assure performances et fiabilité par l'intermédiaire de la connectivité Internet. De même, elle aide les entreprises à abandonner les architectures réseau d'ancienne génération. Commencez par déployer progressivement Magic WAN en mettant en place un parcours de transition au fil du temps. En combinant l'approche « léger sur le régional, fort sur le cloud » de la connectivité au dernier segment et des performances, de la fiabilité et de la sécurité du segment intermédiaire, Cloudflare vous aide à mieux vous connecter et à sécuriser le travail hybride. Notre architecture prend en charge le déploiement en parallèle d'une infrastructure existante afin de vous permettre de migrer à votre rythme.

Comparaison de Cloudflare One par rapport au MPLS et au SD-WAN

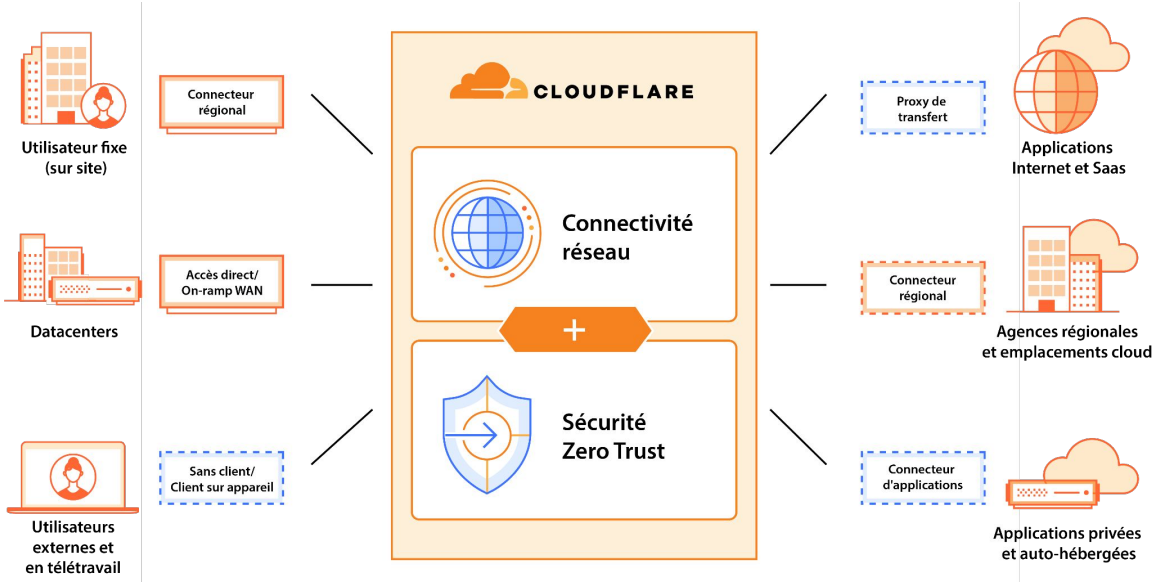
Maintenant que les applications ont migré vers le cloud et que les entreprises adoptent le travail hybride, les architectures réseau traditionnelles constatent un repli en termes de performances et de sécurité. La redirection du trafic nuit aux performances et à l'expérience utilisateur, tandis que le déchargement vers le local affecte la cohérence et l'efficacité de la sécurité. Aucun de ces scénarios n'est désirable et, en conséquence, les modèles de conception réseau doivent effectuer des compromis qui ne permettent plus de satisfaire les besoins organisationnels et individuels.

Plus récemment, le SD-WAN a ajouté des surcouches permettant de gérer le trafic dans l'espoir de proposer une alternative au MPLS. Quoi qu'il en soit, le SD-WAN dépend toujours largement d'appareils en périphérie de réseau pour mettre en œuvre la sécurité et les équipes doivent donc s'en remettre à un ensemble hétéroclite d'outils physiques, virtualisés et basés sur le cloud bricolé à la va-vite. En conséquence, la complexité accrue contrebalance bon nombre des avantages prévus.

La plateforme SASE de Cloudflare fait converger la sécurité et les fonctions réseau au sein de notre cloud de connectivité afin de permettre aux entreprises d'utiliser notre réseau comme une extension du leur. La gestion simplifiée, la fiabilité des performances, la sécurité Zero Trust moderne et la réduction du coût total de possession ne sont possibles simultanément que via une approche véritablement réinventée vers le SASE.

Critères	MPLS/Service VPN	SD-WAN	SASE avec Cloudflare One
Configuration Nouvelle installation de site, configuration et gestion	Via MSP par le biais d'une requête de service	Orchestration et gestion simplifiées via un contrôleur centralisé	Orchestration automatisée via un portail SaaS. Tableau de bord centralisé
Contrôle du trafic sur le dernier segment Équilibrage du trafic, qualité de service et basculement	Scénario couvert par les SLA du MPLS	Sélection du meilleur chemin disponible dans l'équipement SD-WAN	Déploiement minimal sur site pour contrôler le processus de prise de décision à l'échelon local
Contrôle du trafic sur le segment intermédiaire Redirection du trafic autour des perturbations du segment intermédiaire	Scénario couvert par les SLA du MPLS	« Spaghettis de tunnels » et aucun contrôle sur le segment intermédiaire	Gestion du trafic intégrée et mesures de contrôle de l'infrastructure privée dans la même interface
Intégration cloud Connectivité pour la migration cloud	Déchargement centralisé	Déchargement décentralisé	Connectivité native grâce à Cloud Network Interconnect
Sécurité Filtrage du trafic Internet entrant et sortant à la recherche de logiciels malveillants	Assemblage hétéroclite de mesures de contrôle physiques	Assemblage hétéroclite de mesures de contrôle physiques et/ou logicielles	Intégration native aux utilisateurs, aux données, aux applications et aux outils de sécurité réseau
Coûts Optimisation du ROI pour les investissements réseau	Coût élevé des équipements physiques et de la connectivité	Optimisation des coûts de connectivité aux dépens d'un accroissement du coût des équipements physiques et logiciels	Diminution des coûts liés aux équipements physiques et à la connectivité

Orienter le trafic vers la plateforme SASE de Cloudflare



Le connecteur Magic WAN facilite la connexion de vos emplacements réseau à Cloudflare. Utilisez le connecteur régional logiciel préinstallé et configuré sur un équipement physique certifié par Cloudflare pour bénéficier d'un déploiement simplifié, ou déployez vos équipements physiques ou virtuels sur des équipements Linux au sein de votre environnement.

Une solution faisant partie d'une famille grandissante de services d'accès direct (on-ramp) flexibles

La première étape vers l'adoption du SASE consiste à établir une connexion, c'est-à-dire établir un chemin sécurisé de votre réseau existant au site le plus proche dans lequel vous comptez déployer des politiques de sécurité Zero Trust. Cloudflare propose une vaste sélection de services « d'accès direct » (on-ramp) pour mettre en œuvre cette connectivité, notamment des options d'accès avec ou sans client pour les utilisateurs hybrides, des tunnels en couche applicative déployés par l'intermédiaire de connecteurs logiciels légers, une connectivité en couche réseau basée sur des tunnels Anycast GRE ou IPsec, ainsi qu'une interconnexion physique ou virtuelle, à la fois pour les datacenters privés et les clouds publics.

Afin de faciliter encore l'adoption du SASE, le connecteur Magic WAN peut être déployé sur n'importe quel emplacement réseau physique ou cloud afin d'assurer une connectivité automatique au datacenter optimal du réseau Cloudflare, en tirant parti de la connectivité Internet existante sur le dernier segment et en supprimant la nécessité, pour les équipes informatiques, de configurer manuellement l'équipement réseau afin d'établir la connexion.

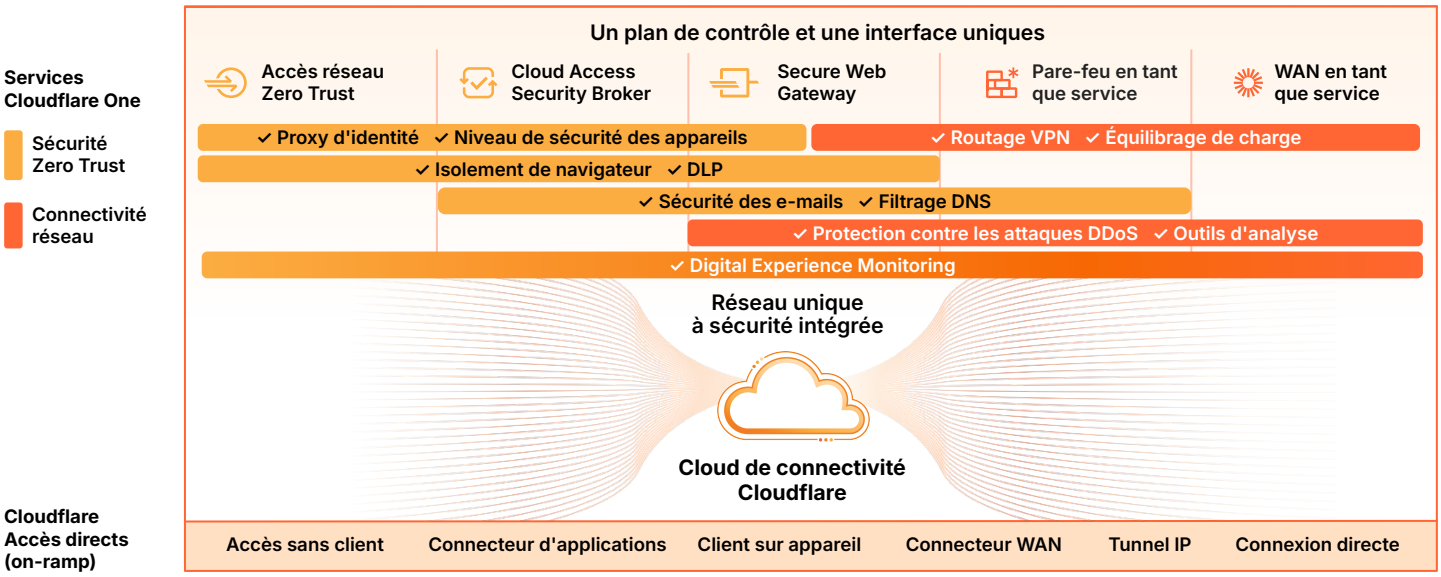
Fonctionnalités logicielles et spécifications des équipements physiques

Fonctionnalités logicielles de Magic WAN[1]	
Installation du connecteur WAN	Appareil(s) CPE plug-and-play, sans interaction, provisionnés et gérés de manière centralisée via le tableau de bord Cloudflare ou par API. Configuration automatique des tunnels IPsec et acheminement en trafic direct vers le réseau Cloudflare pour les fonctions de connectivité et de sécurité. Mises à jour logicielles automatiques (au sein de la période de service définie par le client).
Configuration du site du connecteur WAN	Prise en charge du WAN/LAN pour les configurations avec adresse IP statique ou DHCP. Prise en charge des VLAN et de la segmentation réseau locale.
Approche « léger sur le régional, fort sur le cloud »	Connecteur WAN léger et à haute disponibilité, avec équilibrage de charge et basculement sur plusieurs circuits WAN en fonction des contrôles d'intégrité. Services de sécurité (comme le pare-feu et les fonctionnalités SSE Zero Trust) proposés via le cloud de connectivité Cloudflare.
Intégration tierce	Configurez vos points de terminaison de tunnel Anycast IPsec ou GRE à l'aide de vos VPC cloud existants, comme Amazon AWS Transit Gateway ou de vos équipements chez le client, comme vos SD-WAN, vos pare-feu et vos routeurs. Configurez des itinéraires statiques grâce au transfert de paquets ECMP vers le réseau Cloudflare.
Sécurité intégrée	Mesures de détection d'intrusions et pare-feu de couche 3 intégrés. Intégration parfaite aux autres fonctionnalités de sécurité/SSE et accès direct (on-ramps) comme une passerelle web sécurisée en couche 4-7, un client sur appareil, un connecteur d'applications, etc.
Visibilité et contrôle	Détection et routage du trafic basé sur application. Contrôle de la bande passante. Visibilité/analyses pour les indicateurs liés aux tunnels, au trafic et aux appareils disponibles via tableau de bord, API, journaux ou GraphQL. Gestion via tableau de bord Cloudflare, API or Terraform.
Spécifications des options matérielles pour le connecteur Magic WAN[2]	
Spécifications des appareils	• **Ports :** (6□ × 1G Copper RJ45) + (2 × 10G SFP+) + (2 USB 3.0 Type A) • **Dimensions :** 20,57 × 17,78 × 5,08 cm ; 1,5 RU ; **Poids :** 1,30 kg • **Options de montage :** sur bureau, montage mural ou montage en rack (avec plateau) • **TPM :** 2.0, monde, sauf Chine • **Processeur :** Denverton 4 Core C3558 • **Disque :** SSD M.2 120 avec 16 Go de mémoire flash eMMC • **RAM :** 8 Go de DDR4 • **Wi-Fi et Bluetooth :** 802.11ac, 2 × 2 MIMO, débit physique maximum : 866,7 Mo/s • **Ventilateur :** un

[1] Vous retrouverez toute la documentation concernant les fonctionnalités de Magic WAN dans Cloudflare Docs.
[2] Matériel certifié par Cloudflare avec logiciel Magic WAN préinstallé : Dell VEP 1425, vendu via un partenaire (livré avec une interface de montage pour rack).

Connectivité réseau et la voie vers le SASE

Le cloud de connectivité de Cloudflare assure à votre déploiement la simplicité, la résilience réseau et la rapidité d'innovation nécessaires pour conserver une longueur d'avance pendant votre parcours de consolidation de vos solutions dédiées et de convergence vers une stratégie informatique unifiée.



Cloudflare One permet aux entreprises de toutes les tailles d'effectuer leur transition vers le SASE en connectant n'importe quelle source de trafic et n'importe quelle destination à un réseau mondial sécurisé, rapide et fiable, sur lequel toutes les fonctions de sécurité sont mises en œuvre et le trafic optimisé pendant l'acheminement vers sa destination, à la fois au sein d'un réseau privé ou sur l'Internet public.

Que votre entreprise décharge du trafic depuis des déploiements MPLS ou SD-WAN matures, ou qu'elle approche la modernisation de son réseau pour la première fois, le service Magic WAN peut vous aider à simplifier le processus. Cloudflare One propose à la fois une sécurité Zero Trust et un WAN-as-a-Service afin d'atteindre le SASE à fournisseur unique, mais peut également compléter une stratégie multi-fournisseurs afin de vous aider dans votre parcours SASE.

Discutons de la connectivité réseau de votre entreprise

Demander un atelier

CLOUDFLARE

Vous n'êtes pas encore prêt à avoir une discussion en direct ?

Vous trouverez davantage d'informations dans notre architecture SASE de référence.