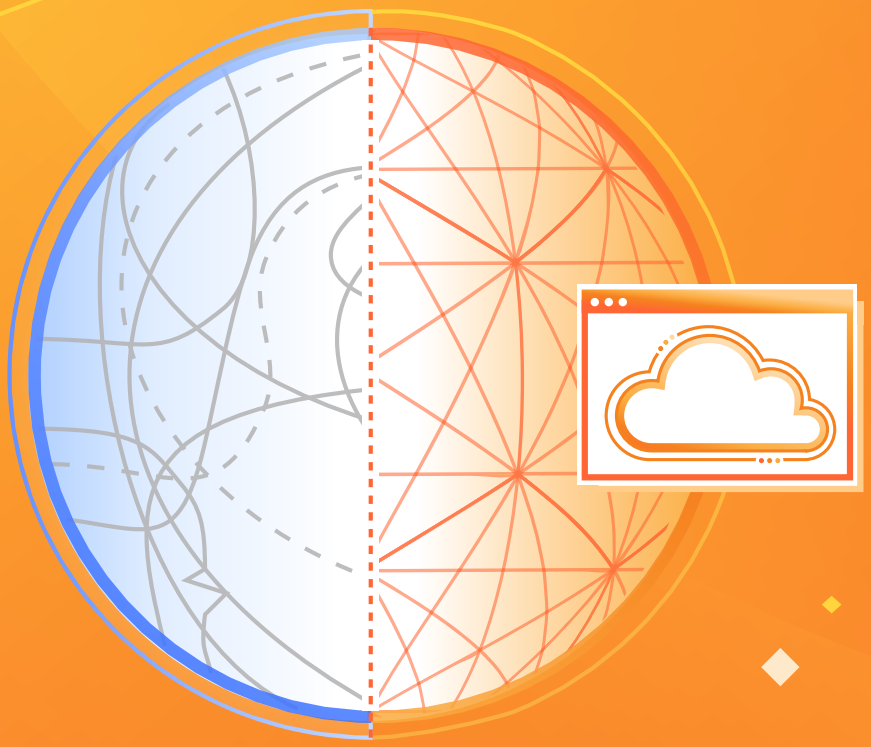
CLOUDFLARE

LIVRE BLANC

Développer une stratégie pour la modernisation de votre réseau



Sommaire

Les solutions de connectivité réseau existantes : un obstacle à la modernisation numérique

L'agilité est essentielle pour exceller dans un monde dans lequel les conditions opérationnelles évoluent très rapidement. Cependant, l'agilité n'est pas qu'une question de leadership et de prise de décision : l'agilité dépend également de la capacité d'une entreprise à embrasser le changement. Les systèmes doivent être configurés de façon à allier flexibilité et adaptabilité, sans risque de défaillance. L'entreprise doit être en mesure de s'adapter à de nouveaux modèles de revenus, de prendre en charge de nouvelles applications et de connecter ses effectifs dans le monde entier.

Lors des projets de modernisation numérique, l'agilité est l'un des premiers résultats recherchés, tandis que les entreprises se rééquipent dans le but de remporter un avantage concurrentiel. C'est particulièrement évident lorsque l'on considère l'état du réseau d'entreprise traditionnel, qui joue un rôle essentiel dans la mise en œuvre des communications et le renforcement de la collaboration. Le réseau d'entreprise est resté obstinément réfractaire au changement, et ce, pour de bonnes raisons. Il a été conçu pour résister aux chocs subis par le système, et tout changement implique des coûts élevés et des efforts considérables.

Parfois, les changements peuvent être anticipés, car ils se déroulent au fil du temps, comme les effets du cloud sur le datacenter. Avec la connectivité réseau, les forces exogènes du marché provoquent des changements rapides, parfois du jour au lendemain. Par exemple, la pandémie a donné lieu à de douloureux enseignements sur la difficulté, pour certaines entreprises, d'accroître rapidement leur capacité de télétravail, de préserver la productivité de leurs effectifs et de maîtriser leurs dépenses au regard de ce que coûtaient les réseaux inactifs déployés dans des locaux vides.

Ces épreuves ont également révélé que certaines entreprises étaient non seulement capables de s'adapter, mais également de prospérer. La solution ne tenait pas seulement à la capacité des dirigeants à prendre les bonnes décisions, mais également à la capacité de transformation et d'exécution des entreprises. Pour un DSI, il est nécessaire d'élaborer des stratégies permettant de faire face au changement, de rééquiper l'entreprise en fonction des besoins à venir et d'élever l'informatique au rang d'accélérateur du changement, plutôt que de retardateur.

Compte tenu de l'importance des investissements consacrés aux réseaux sur site, la modernisation n'est pas une décision simple. Pour optimiser les avantages de la modernisation du réseau, il est nécessaire d'examiner les objectifs à atteindre afin de définir la nature des changements à apporter.

Comprendre le parcours

Lorsque l'on examine les bonnes pratiques en matière de conception de réseaux au fil des ans, il est facile de comprendre d'où provient la complexité. Pendant des décennies, les entreprises ont élargi et fortifié leurs réseaux, ajoutant à ceux-ci des couches successives de nouvelles technologies. À chaque nouvelle génération d'architecture de réseau et chaque innovation, le réseau a gagné en complexité. Il n'existait pas de solution permettant d'aller vers la simplicité, et souvent, l'ajout de nouvelles technologies rendait la vitesse, la résilience et la sécurité encore plus difficiles à assurer.

Les services de connectivité réseau et de sécurité étant désormais fournis depuis le cloud, nous assistons actuellement aux prémices de la prochaine génération des réseaux d'entreprise. En utilisant les services mis en œuvre depuis le cloud comme une extension du réseau, les entreprises peuvent envisager de nouveaux scénarios d'utilisation, élargir leur couverture et sécuriser les applications bien au-delà du datacenter. Cette évolution leur offre l'opportunité de simplifier considérablement leur réseau, car la fourniture de services repose sur la connexion du réseau existant au point de présence (PoP, « Point of Presence ») du fournisseur de services cloud ; il n'est plus nécessaire d'interrompre la connexion pour insérer un nouvel équipement. La connectivité réseau entre le réseau sur site et le service cloud reste inchangée à mesure de l'insertion et de la consommation des services au sein du service cloud.

Le problème est que toutes les plateformes de connectivité et de sécurité des réseaux mises en œuvre depuis le cloud sont différentes, et il n'est pas toujours facile de distinguer ce qui les différencie les unes des autres. Nombre d'entre elles n'offrent qu'une marge de manœuvre limitée en matière de modernisation. Pour comprendre les différences, il est nécessaire d'établir clairement vos objectifs en matière de modernisation du réseau afin d'éviter de remplacer une source de complexité par une autre.

Les quatre principaux chemins du trafic réseau

Lorsque vous déterminez la portée de votre projet de modernisation du réseau, tenez compte du fait que votre réseau couvre un grand nombre de points d'interaction, dont certains cohabitent sur la même infrastructure (par exemple, le trafic sur votre réseau central peut être entrant, sortant ou en transit), tandis que d'autres opèrent hors de cette infrastructure (par exemple, votre connectivité réseau avec le cloud public).

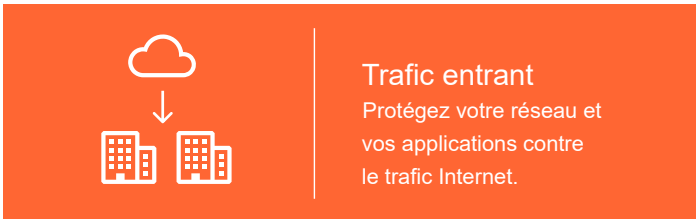
Trafic entrant : dans la mesure où certaines parties du réseau sont exposées à Internet, il est nécessaire de déployer des défenses du trafic entrant capables d'assurer une protection contre les tentatives de neutralisation ou d'exploitation de l'activité, sans entraver l'acheminement du trafic des utilisateurs légitimes. Les défenses périmétriques traditionnelles peuvent être saturées, et elles nécessitent des fonctionnalités permettant de réagir aux dénis de service distribués.

Trafic sortant : les connexions à Internet et aux applications cloud exigent des politiques offrant des garde-fous permettant une utilisation professionnelle sûre, à l'image d'une protection contre les menaces et l'exfiltration des données. Pour répondre à la variabilité de l'emplacement des utilisateurs, les entreprises ont mis en œuvre un ensemble de technologies de protection des communications sortantes réunissant des équipements sur site, tels que des pare-feu (lorsque l'utilisateur est présent sur le réseau), des résolveurs DNS, ainsi que des proxys dans le cloud, à l'image des solutions SWG (Secure Web Gateway) et CASB (Cloud Access Security Broker) (lorsque l'utilisateur travaille à distance).

Connectivité aux réseaux WAN : les réseaux étendus (WAN, Wide Area Network), ainsi que les limites qu'ils englobent (notamment les campus et les succursales), sont en train d'être repensés afin de prendre en charge les initiatives priorisant le cloud et les équipements compatibles avec l'Internet des Objets (IoT). Ainsi, la topologie traditionnelle des réseaux se défait de la redirection des données vers le datacenter au profit d'architectures permettant un accès direct à Internet. À l'heure où la connectivité réseau accomplit des progrès rapides dans ces domaines, l'intégration de solutions de sécurité est, quant à elle, devenue plus complexe. Dans de nombreux cas, les chemins de trafic internes restent tributaires des équipements de sécurité déployés à la périphérie, ce qui grève le déroulement de la transformation des entreprises.

Connectivité réseau au cloud public : tandis que les entreprises développent leurs applications sur une multitude de clouds, il devient de plus en plus difficile d'établir et de gérer des configurations réseau et de sécurité ponctuelles. La configuration et la gestion du réseau consomment du temps et des ressources qu'il serait plus judicieux de consacrer au développement de projets.

Chacun de ces chemins de trafic repose sur un certain nombre de technologies que les entreprises mettent en œuvre au sein de leur réseau ou consomment depuis le cloud. Dans la mesure où les projets de modernisation englobent des chemins de trafic établis dans une multitude de directions, il est nécessaire de planifier l'ensemble du parcours de modernisation du réseau dans les quatre directions, afin d'éviter toute erreur architecturale susceptible de limiter les bienfaits de la transformation ou d'imposer le recours à une multitude de technologies disparates pour gérer des scénarios d'utilisation non traités.

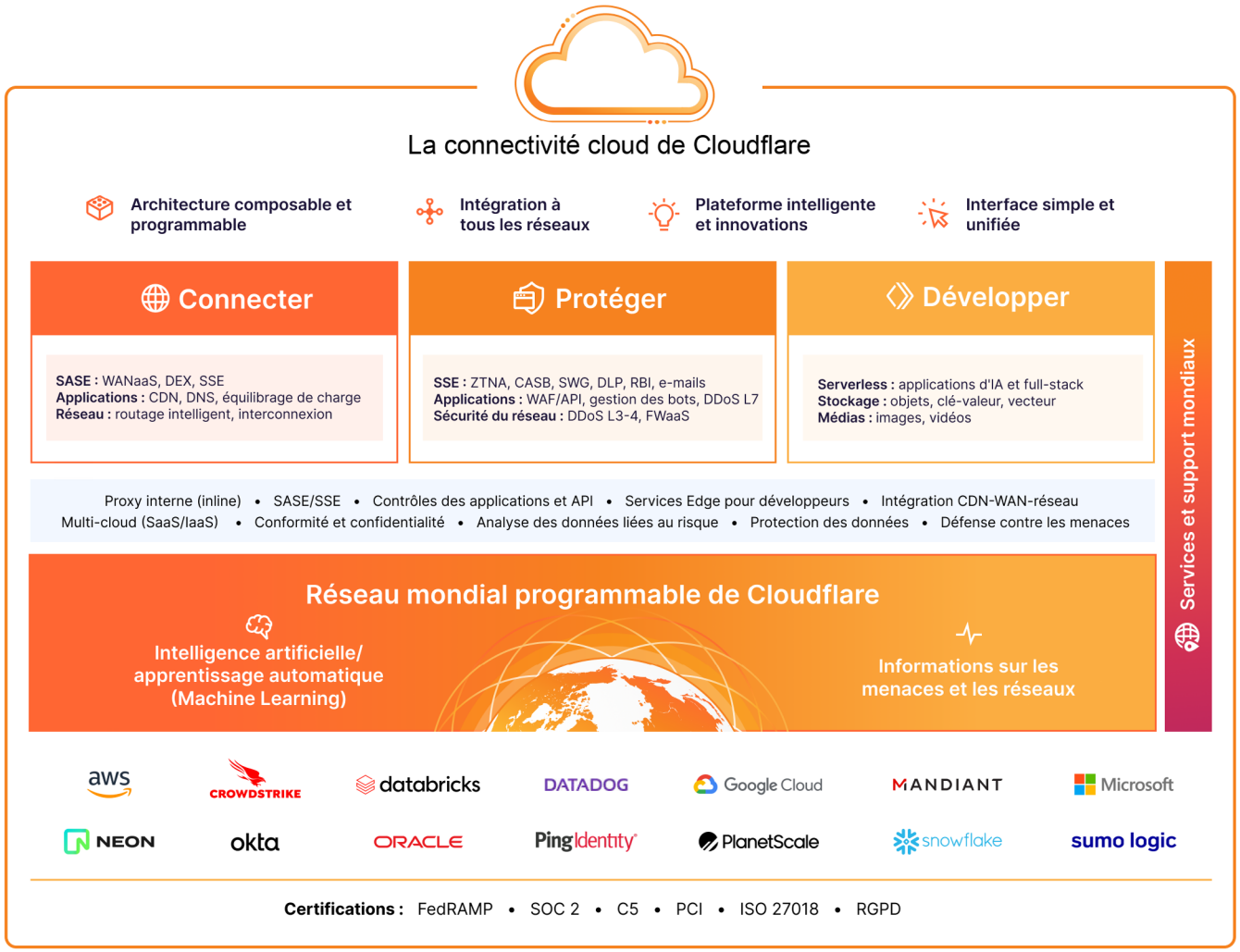


La connectivité cloud de Cloudflare

Réfléchissez à la solution de connectivité cloud de Cloudflare pour la modernisation de votre réseau. La solution est fondée sur une philosophie d'utilisation d'une architecture composable et programmable, permettant de fournir 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. Elle répond ainsi aux besoins actuels et futurs de votre parcours de modernisation.

Avec Cloudflare, vous pouvez ajouter des fonctionnalités et prendre en charge de nouveaux scénarios d'utilisation en activant des services, plutôt qu'en insérant des équipements. La connexion à un datacenter Anycast de Cloudflare demeure inchangée, tandis que vous configurez et déployez, depuis l'interface de gestion unifiée, des services permettant de traiter le trafic. Vous pouvez répondre aux besoins actuels de l'entreprise, tout en déployant la plateforme qui servira de fondation à vos futurs scénarios d'utilisation et accompagnera l'ensemble de votre parcours de modernisation du réseau.

Au lieu d'étendre votre infrastructure à l'échelle mondiale, utilisez la nôtre. Votre entreprise bénéficiera de la vitesse fulgurante qu'offre le réseau mondial de Cloudflare. Grâce à des connexions directes à la quasi-totalité des fournisseurs d'accès Internet et de cloud, le réseau Cloudflare peut atteindre 95 % de la population mondiale connectée à Internet en moins de 50 ms.



Principaux scénarios d'utilisation de la modernisation des réseaux

Pour vous lancer, privilégiez les scénarios d'utilisation qui ont une incidence sur l'activité de votre entreprise et lui confèrent les avantages les plus significatifs. Rien ne préconise de suivre ces scénarios d'utilisation dans un ordre particulier, car les priorités de chaque entreprise lui sont propres. L'important est de répondre aux besoins à court terme de votre entreprise, tout en bâtissant une architecture qui contribuera à la modernisation de votre réseau, quelle que soit la voie que vous emprunterez.

	Projets de modernisation
Connectivité des bureaux régionaux Réduire les coûts, améliorer l'expérience utilisateur	• Réaliser la transition de la technologie MPLS vers la connectivité cloud • Réaliser la transition des réseaux SD-WAN vers la connectivité cloud
Protéger votre infrastructure accessible au public Prolonger la durée de vie de vos investissements dans les systèmes de pare-feu et les DMZ	• Réduire la charge qui pèse sur les pare-feu réseau • Transférer la sécurité de la DMZ vers la solution de connectivité cloud
Simplifier votre réseau d'entreprise Déployer la sécurité Zero Trust pour améliorer la sécurité et réduire les dépenses d'investissement	• Réduire/éliminer la DMZ • Remplacer le VPN par la sécurité ZTNA • Abandonner le niveau élevé de confiance sur le réseau local • Accélérer la connectivité lors des fusions et acquisitions
Connecter et sécuriser vos clouds Utiliser le meilleur de chaque cloud dans vos applications	• Développer et sécuriser des applications • Utiliser les services pour développeurs afin de centraliser les fonctions essentielles

Connectivité des bureaux régionaux

Une composante essentielle de la connectivité des réseaux WAN tient à leur capacité à relier des sites plus petits, tels que des succursales ou des points de vente, qui dépendent de la connexion des utilisateurs et des équipements aux applications. Les architectures en étoile traditionnelles permettaient de connecter les sites au datacenter au moyen de circuits MPLS coûteux ; cependant, devant la nécessité croissante de prendre en charge les applications cloud, un nombre grandissant d'entreprises déploie des architectures offrant une connexion directe à large bande à Internet.

L'architecture SD-WAN aspirait à rendre la connectivité réseau plus fiable, mais sa relation avec l'intégration d'équipements de sécurité n'est pas parfaite. La plupart des architectures SD-WAN sont tributaires d'équipements lourds à la périphérie et de pare-feu locaux pour l'application de la politique de sécurité sur l'infrastructure SD-WAN, et n'utilisent l'intégration SSE/SASE que pour le trafic sortant.

Utilisez la connectivité cloud de Cloudflare pour mettre en œuvre la connectivité des succursales et accompagner l'intégralité de votre parcours de migration, qu'il s'agisse d'enrichir ou de remplacer les services existants. Cloudflare utilise une architecture fondée sur une philosophie « périphérie légère/cloud lourd » pour fournir des services de connectivité réseau et de sécurité. Facilitez la connectivité de site à site entre différents emplacements réseau (bureaux régionaux, points de vente ou ateliers de production) avec Cloudflare Magic WAN. La solution offre des fonctionnalités de connectivité et de routage sécurisées et performantes pour l'ensemble de vos besoins de connectivité réseau d'entreprise, réduisant ainsi les coûts et la complexité opérationnelle. Pour la sécurité, Cloudflare Magic Firewall offre un déploiement fluide avec Magic WAN, vous permettant d'appliquer des stratégies de contrôle du réseau Nord/Sud ou Est/Ouest lorsque le trafic transite sur le réseau de Cloudflare.

Protéger votre infrastructure accessible au public

Le réseau d'entreprise et la DMZ sont adressables et accessibles depuis Internet, et nécessitent l'adoption de mesures destinées à empêcher les acteurs malveillants de provoquer des dommages. Dans un monde parfait, les pare-feu réseau traditionnels pourraient inspecter et éliminer tout le trafic indésirable ; toutefois, chaque pare-feu possède des capacités limitées (bande passante disponible, utilisation/puissance de traitement, nombre de sessions, etc.). La capacité de l'acteur malveillant à exécuter ses plans est simplement une question d'ampleur ; en effet, il lui suffit de générer suffisamment de bruit pour saturer, sur différentes couches du protocole réseau, la capacité de l'entreprise à gérer son activité.

Il ne s'agit pas uniquement du volume de trafic. L'acceptation du trafic entrant expose la surface d'attaque au trafic non authentifié/préauthentifié. Les failles dans les applications et les systèmes d'exploitation peuvent être exploitées par un acteur malveillant qui ne possède même pas de compte sur le système. Les attaques par bourrage d'identifiants (« credential stuffing », c'est-à-dire l'utilisation de noms d'utilisateur et de mots de passe connus, divulgués lors d'autres violations) constituent également un facteur de risque important. L'application des principes de la sécurité Zero Trust aux applications de la DMZ permet aux entreprises de réduire l'exposition à Internet, voire de l'éliminer, lorsque c'est possible.

Les entreprises peuvent améliorer la protection de leur réseau en appliquant les principes de la défense en profondeur afin d'absorber le trafic malveillant en amont de leur infrastructure accessible au public. Déployée sur l'ensemble du réseau Anycast de Cloudflare, l'intégration de Cloudflare Magic Transit et de Magic Firewall se comporte comme la porte d'entrée de l'entreprise ; elle filtre le trafic malveillant et inutile et achemine uniquement le trafic entrant légitime.

Lorsque les pare-feu réseau procèdent à l'atténuation des attaques DDoS sur un équipement, celui-ci doit encore traiter la connexion avant de pouvoir l'interrompre. Avec Cloudflare, notre réseau diffuse le préfixe du client, attirant ainsi le trafic qui serait autrement destiné au pare-feu périmétrique. Anycast permet à notre réseau d'absorber efficacement l'attaque DDoS en répartissant la charge sur l'ensemble de nos datacenters. Les composants du botnet repèrent le point de présence (PoP) Anycast le plus proche, qui traite le trafic conformément aux politiques de Magic Transit et de Magic Firewall.

Simplifier votre réseau d'entreprise

La simplification offre un certain nombre d'avantages en matière de modernisation. Les équipes informatiques peuvent rendre le réseau plus fiable en réduisant le nombre de composants faillibles au sein de leur architecture, et elles peuvent le rendre plus sûr en adoptant une approche Zero Trust qui exclut tous les privilèges d'accès.

Pour simplifier votre réseau, vous pouvez envisager les méthodes suivantes :

Effectuer une migration depuis la DMZ

Les DMZ du réseau constituent un casse-tête opérationnel, car elles sont particulièrement sensibles aux exploitations de vulnérabilités zero-day. Un acteur malveillant n'a pas besoin d'accéder au réseau interne pour communiquer avec les serveurs de la DMZ, et les entreprises doivent donc rester vigilantes si elles veulent éviter tout risque d'exploitation et d'utilisation abusive.

Toutefois, si les DMZ ont joué un rôle important dans le passé, sont-elles nécessaires aujourd'hui ? La DMZ étant un concept lié au réseau, elle perd désormais de son importance, car il existe d'autres solutions permettant de créer et d'héberger des applications.

- Pour les applications publiques, le transfert des charges de travail vers le cloud public présente des avantages économiques et techniques.
- Avec la méthode SaaS, de nombreux types d'applications publiques et privées n'ont pas besoin de s'exécuter sur une infrastructure gérée par le client.

Il est donc pragmatique, du point de vue de la sécurité et de la conception du réseau, de commencer à réfléchir à la manière de réduire ou d'éliminer la nécessité d'une DMZ. Cette démarche est non seulement logique d'un point de vue opérationnel, mais elle simplifie également considérablement l'architecture en éliminant l'infrastructure réseau sur laquelle elle repose, à l'image du pare-feu, du pare-feu WAF et des solutions d'équilibrage de charge.

Qu'en est-il des applications privées déployées dans la DMZ pour élargir l'accès aux collaborateurs, aux partenaires et aux sous-traitants ? Il serait plus sûr de les isoler sur un réseau privé et d'étendre l'accès aux collaborateurs et aux partenaires en optant pour une approche fondée sur l'accès réseau Zero Trust (ZTNA, Zero Trust Network Access).

Avec l'architecture ZTNA, vous réduisez efficacement la surface d'attaque en éliminant le trafic réseau entrant vers l'application. L'architecture ZTNA emploie un accès contextuel aux ressources via la solution de connectivité cloud de Cloudflare, éliminant ainsi la nécessité d'ouvrir des ports dans le pare-feu réseau, tout en offrant à l'équipe de sécurité une visibilité totale sur les utilisateurs ayant accès à chaque ressource.

Remplacer le VPN par l'architecture ZTNA

L'époque où les entreprises utilisaient des VPN pour permettre au personnel d'accéder aux applications est désormais révolue. Du point de vue de l'architecture du réseau, il est peu pratique de connecter les utilisateurs par l'intermédiaire d'un très long tunnel afin de leur permettre d'accéder à Internet et au cloud. L'accès au réseau d'utilisateurs (et des terminaux potentiellement compromis) à l'aide d'un VPN constitue également un risque majeur pour la sécurité.

L'accès aux applications ne constitue pas non plus la seule fonction d'un VPN. Dans certains cas, les entreprises ont besoin d'une connectivité réseau plus large avec un point de terminaison, par exemple, aux fins de l'administration du point de terminaison et des communications initiées par le serveur. Ces scénarios d'utilisation tirent traditionnellement parti de la connectivité réseau du VPN dans les deux directions et ont compliqué la tâche des premiers produits ZTNA proposés sur le marché. En l'absence d'alternatives, les entreprises ont dû déployer parallèlement des solutions ZTNA et VPN.

Pour moderniser l'infrastructure réseau, les entreprises peuvent réunir les fonctions avec ZTNA de Cloudflare. En effet, avec Cloudflare, les entreprises peuvent prendre en charge les scénarios d'utilisation classiques de l'architecture ZTNA, ainsi que le trafic établi par le serveur et le trafic bidirectionnel. Ces fonctions aident les entreprises à réduire leurs besoins d'accès aux applications en éliminant le VPN, et contribuent à améliorer la sécurité et la simplicité.

Abandonner le niveau élevé de confiance sur le réseau local

Avec le travail hybride, la différence entre la façon dont le personnel travaille au bureau et la façon dont il travaille sur d'autres sites est de moins en moins marquée. En réalité, cela se vérifie particulièrement lorsque les utilisateurs travaillent fréquemment sur les réseaux publics non fiables déployés dans les cafés et les espaces de travail partagés.

Sous certains aspects, le réseau public ouvert est l'incarnation de la sécurité Zero Trust : personne ne dispose d'un accès privilégié, et aucun utilisateur ni ressource n'est digne de confiance. Si ce modèle peut en principe fonctionner dans un espace de travail partagé, un bureau à domicile ou un café, pourquoi ne serait-il pas possible d'éliminer la confiance également au sein du réseau de l'entreprise ?

L'abandon de la confiance ne nécessite pas de faire évoluer la conception du réseau, mais plutôt de la simplifier. Au lieu de prévoir un accès très permissif pour les utilisateurs authentifiés et d'utiliser des politiques réseau pour établir des connexions aux ressources, il est beaucoup plus sûr de partir du principe qu'aucun utilisateur présent sur le réseau n'est digne de confiance. Avec l'expression de la sécurité par le biais de l'architecture SASE, les entreprises bénéficient de l'accès aux applications dont elles ont besoin, avec la sécurité adéquate pour en garantir la protection, sans qu'il soit exigé une confiance par défaut sur le réseau lui-même. La sécurité Zero Trust ne consiste pas à ajouter de la confiance au réseau, mais à la supprimer jusqu'à atteindre une situation préférable et plus sécurisée, débarrassée des autorisations explicites et excessives du passé.

Accélérer la connectivité pour les activités de fusion et acquisition

Les entreprises utilisent les fusions-acquisitions pour obtenir des ressources et des capacités opérationnelles qui ne leur seraient autrement pas immédiatement accessibles. Pour tirer parti au mieux de cette opportunité, les entreprises doivent agir rapidement, afin que l'entreprise issue de la fusion soit meilleure que la somme de ses parties. Toutefois, les services informatiques ne sont pas toujours capables d'agir rapidement, car les applications et l'infrastructure réseau sous-jacente de deux entreprises ne s'articulent pas souvent de manière harmonieuse.

Pour accélérer la connectivité dans le cadre des fusions et acquisitions, les entreprises peuvent envisager l'accès aux applications comme une tâche distincte de l'intégration du réseau. Le calendrier de conception d'une architecture réseau convergente peut s'étendre sur plusieurs années ; cependant, l'accès aux applications ne doit pas être lié à une échéance aussi lointaine.

En effet, la situation au premier jour est concrètement un scénario d'utilisation Zero Trust dans lequel les utilisateurs de confiance présents sur des réseaux non fiables ont toujours besoin d'accéder aux applications. Étendez l'accès avec Cloudflare One qui vous permet de déployer la connectivité nécessaire aux fusions et acquisitions sans dépendre d'un accès réseau convergent.

Connecter et sécuriser vos clouds

Au fur et à mesure que le développement du cloud évolue, il peut être intéressant de réutiliser les composants d'un cloud dans un autre cloud. Chaque entreprise adoptera, au fil du temps, une architecture multi-cloud et, de la même façon, chaque entreprise devra, au fil du temps, gérer la connectivité réseau au cloud public. Le développement d'applications a tendance à être propre à chaque équipe par nature, les équipes DevOps au sein des différentes parties de l'entreprise préférant les outils avec lesquels elles sont le plus familières. Le développement de capacités organisationnelles permettant de gérer la connectivité entre les clouds est toutefois complexe, car le travail couvre des ensembles d'outils développés sur des infrastructures entièrement différentes.

La complexité de l'architecture multi-cloud se retrouve également dans le domaine du cloud hybride. Le cloud hybride associe un cloud privé sur site et des clouds publics virtuels. Ces réseaux reposent parfois sur une connectivité réseau dédiée, comme AWS Direct Connect, mais ce modèle peut s'avérer coûteux et se limiter à un cloud seulement. Lorsque les entreprises développent des applications multi-cloud, elles ne veulent pas nécessairement assumer les coûts d'une connectivité réseau dédiée pour chaque cloud.

Au lieu de développer la connectivité réseau et la sécurité directement d'une application à une autre, utilisez Cloudflare pour orchestrer et connecter les services de connectivité réseau pour le cloud public. Nous pensons que la solution de connectivité cloud de Cloudflare joue un rôle idéal dans une telle architecture ; elle est en effet idéalement située pour permettre l'acheminement du trafic entre les clouds sur le vaste réseau de Cloudflare. Avec l'ajout de capacités de gestion de la connectivité réseau du cloud public, les clients peuvent désormais orchestrer la configuration de la connectivité des charges de travail via Cloudflare également.

Notre solution de connectivité réseau pour le cloud public ne se limite pas à l'orchestration des circuits sous-jacents. Notre architecture va encore au-delà en fournissant des services pour développeurs que ceux-ci peuvent utiliser pour créer et intégrer des applications multi-cloud. La plateforme pour développeurs de Cloudflare offre un riche écosystème de technologies fondamentales suivant sur le principe de l'open source et des normes ouvertes. Vous pouvez choisir d'utiliser tous les éléments de la plateforme pour développeurs ou seulement ceux que vous souhaitez, sans être limité aux services particuliers d'un cloud donné.

Prochaines étapes

Pour franchir les prochaines étapes de la modernisation de votre réseau, contactez Cloudflare et nous vous aiderons à concevoir une stratégie. Nous avons travaillé en étroite collaboration avec des milliers de clients pendant la transition de leur architecture vers la solution de connectivité cloud de Cloudflare.

Pour plus d'informations, consultez http://www.cloudflare.com.

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

RÉV : BDES-5122.2024JAN04