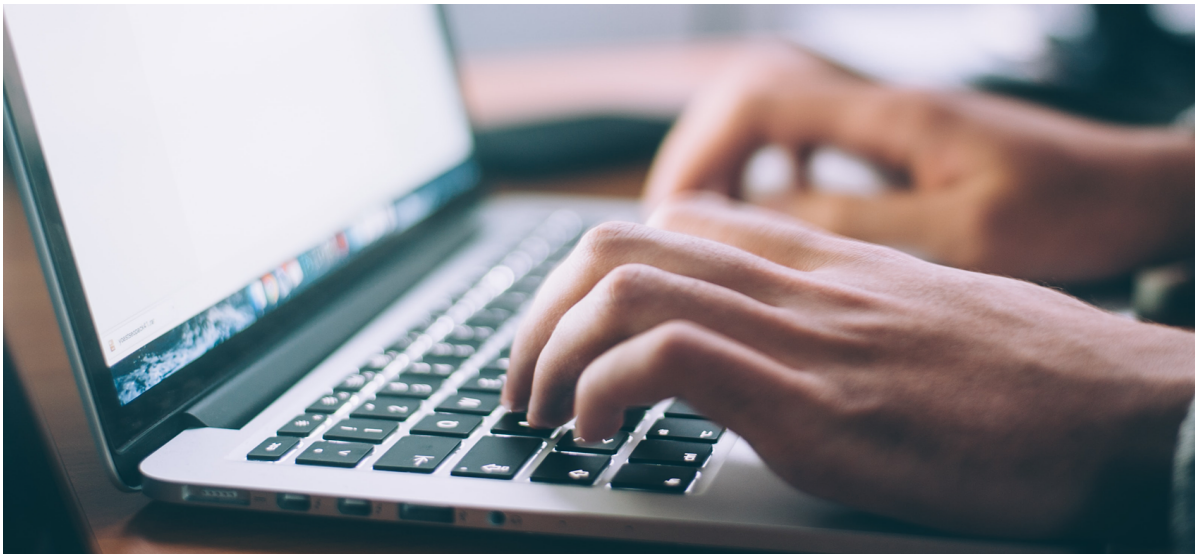
L’essor de l’accès réseau Zero Trust

Une alternative au VPN résultant d’une nécessité



Les pièges liés aux VPN d’entreprise

La pandémie mondiale a accéléré un processus de modification radicale de notre façon de travailler. Il en a résulté une demande accrue pour un accès plus rapide, plus sûr et plus fiable aux applications et aux données internes des entreprises. Conséquence directe de la COVID-19, une enquête réalisée en mai 2020 auprès d’employeurs américains montre que 53 % des employés à temps plein travaillent désormais à domicile.

Ce chiffre a été multiplié par sept par rapport à l’année 2019. Après la pandémie, 22 % des personnes interrogées prévoient de continuer à travailler à distance. Cette explosion mondiale du travail à distance a révélé les failles des réseaux privés virtuels (VPN, Virtual Private Network). Les VPN d’entreprise sont lents, fonctionnent mal sur les appareils mobiles et constituent un environnement propice aux infections.

Un VPN permet aux utilisateurs d’accéder à un réseau interne en reliant un client VPN (logiciel installé sur l’ordinateur ou l’appareil de l’utilisateur) à un serveur d’accès au réseau sur site (un serveur dédié ou un logiciel installé sur un serveur partagé) situé derrière un portail VPN, ou dans le cloud dans le cas des VPN fondés sur le cloud. Son fonctionnement repose sur l’établissement de connexions chiffrées afin de protéger les biens et de gérer l’accès des utilisateurs à un réseau interne.

Tous les appareils qui se connectent au VPN sont dotés de clés de chiffrement, qui servent à coder et décoder toutes les informations échangées entre ces appareils et le serveur d'accès au réseau. Ce processus ajoute une légère latence aux connexions réseau, avec pour résultat un ralentissement du trafic sur le réseau.

De manière générale, les performances des VPN engendrent bien souvent des répercussions particulièrement exaspérantes sur la productivité et l'expérience utilisateur. Les employés sont tenus d'utiliser un ensemble distinct d'identifiants pour se connecter aux appareils, ce qui peut interrompre les flux de travail. La connexion aux applications est lente, réduisant ainsi l'efficacité, et lorsque le VPN est en panne, le travail s'arrête brutalement. Lorsque le VPN est situé loin de l'utilisateur et du serveur auquel il tente d'accéder, ce dernier subit alors une dégradation des performances et une augmentation de la latence. Par exemple, si un utilisateur de San Francisco essaie d'accéder à un site web hébergé sur un serveur situé dans la même ville, mais que le service VPN se trouve au Japon, la demande de l'utilisateur doit parcourir la moitié du monde et revenir avant de se connecter au serveur local. Dans le cas d'un VPN fondé sur le cloud, le serveur d'accès au réseau se situe dans un datacenter différent de celui qui abrite le réseau interne de l'entreprise. Cette étape supplémentaire peut ajouter une latence supplémentaire à chaque requête entre les utilisateurs et le réseau.

La prolifération des appareils mobiles présente un autre défi : le volume des appareils qui accèdent au réseau et doivent être gérés, notamment les appareils personnels des employés. Pour les travailleurs en déplacement, l'accès au réseau peut parfois être affecté par les clients VPN mobiles, ainsi que par la distance entre l'appareil et le bureau à domicile. En outre, l'expérience peut se révéler lente et peu fiable, même en cas d'établissement d'une connexion sécurisée. En fin de compte, les entreprises et leurs employés souffrent de latence, de difficultés de connexion et d'une baisse de productivité.

Les VPN ne sont pas idéaux pour gérer les accès sécurisés des utilisateurs au niveau de granularité exigé par l'environnement de travail dispersé à l'échelle mondiale d'aujourd'hui, car ils présentent des failles de sécurité importantes. Les pirates ne peuvent pas voir ni intercepter le trafic VPN de l'extérieur, mais s'ils parviennent à passer le portail VPN et à prendre le contrôle d'un ensemble d'identifiants ou d'un appareil, ils ont alors la possibilité de compromettre l'ensemble du réseau de l'entreprise et de provoquer une grave fuite de données. Cette préoccupation se révèle encore plus grave de nos jours, car les pirates tirent parti de la pandémie.

De nombreuses applications professionnelles sont aujourd'hui hébergées dans le cloud ou fournies sous forme de logiciel en tant que service (SaaS, Software-as-a-Service), ce qui les rend incompatibles avec les VPN. Ces applications s'appuient généralement sur leurs propres outils et protocoles de sécurité pour offrir un accès sécurisé. Comme elles ne peuvent pas contrôler totalement ces outils et protocoles, les équipes informatiques peuvent éprouver des difficultés à savoir qui accède aux applications.

Approche Zero Trust

Les VPN n'ont pas été conçus dans l'optique de déployer et de gérer efficacement un niveau d'accès utilisateur sécurisé aussi granulaire pour les équipes de travail disséminées. La sécurité Zero Trust représente une solution beaucoup plus intéressante et s'appuie sur une procédure stricte de vérification de l'identité pour chaque personne et appareil tentant d'accéder aux ressources d'un réseau privé, qu'ils se situent à l'intérieur ou à l'extérieur du périmètre du réseau. Aucune technologie spécifique n'est associée à l'architecture Zero Trust.

Il s'agit d'une approche holistique de la sécurité des réseaux intégrant plusieurs technologies et principes différents. Afin de réduire efficacement vos risques de sécurité grâce à l'accès réseau ZTNA (Zero Trust Network Access), vous devez dissimuler les applications au public et mettre en place un mécanisme permettant de vérifier chaque requête, idéalement sur un réseau mondial hautement performant.

La solution Cloudflare Access offre un accès ZTNA sur un réseau massif indépendant du cloud et véritablement mondial, couvrant 200 villes et 100 pays. Elle remplace le VPN d'entreprise par une couche de protection avec gestion de l'identité placée en amont des ressources internes et vérifie les identifiants d'authentification unique (Single Sign On, SSO) des employés à la place d'un client VPN. Plutôt que de voir leur trafic dirigé vers un appareil connecté à un réseau VPN, les employés qui accèdent aux applications internes sont connectés au datacenter le plus proche de leur position. Comme elle a lieu à la périphérie du réseau (à 100 ms seulement de toute personne ou de tout équipement connecté à Internet), cette procédure permet d'accélérer l'authentification et de sécuriser l'accès.

La proximité des datacenters de Cloudflare permet à Access d'authentifier les utilisateurs plus rapidement sans recourir à un VPN, tout en protégeant les applications internes et le réseau grâce aux mécanismes d'authentification les plus rapides et les plus sûrs du marché. Les problèmes liés à la latence du réseau s'évanouissent. Le processus laborieux de gestion des contrôles utilisateur se voit facilité. L'accès à distance est sécurisé, évolutif et mondial. De plus, vous n'avez plus à héberger vos applications et ressources internes sur un réseau privé. Vous pouvez à la place les déployer où bon vous semble, au sein d'un environnement sur site, hybride ou multicloud, et ce en toute sécurité.

Cet article fait partie de notre série consacrée aux dernières tendances et évolutions susceptibles qui peuvent intéresser les décideurs en matière de technologies d'aujourd'hui.

Approfondir le sujet

Consultez le rapport Gartner sur le marché de l'accès réseau Zero Trust en 2020. Obtenir l'e-book.