Accès Zero Trust aux applications privées depuis le bureau et en dehors avec Zscaler™

Des milliers d'entreprises ont adopté avec succès le télétravail, surmontant de nombreux défis liés à la protection des données, à l'accès distant sécurisé et à la mise à l'échelle pour assurer la continuité des activités. Certes, beaucoup ont été surpris par l'urgence et la rapidité requises pour faire passer la majorité de leur personnel au télétravail à plein temps, mais au cœur de ce chaos, beaucoup se sont tournés vers les services Zero Trust pour accéder aux ressources de l'entreprise comme alternative aux méthodes traditionnelles centrées sur le réseau. Aujourd'hui, alors que les équipes informatiques commencent à planifier les années à venir, beaucoup se demandent à quoi ressemblera l'avenir du travail et si le télétravail, ou le travail hybride partagé entre le bureau et la maison, est appelé à devenir la norme.

zscaler™

Du point de vue de la sécurité, les utilisateurs qui se connectent à partir de leur ordinateur portable au bureau et en dehors de celui-ci peuvent accroître les risques de sécurité, surtout s'ils sont automatiquement considérés comme fiables et se voient accorder un accès au réseau. Du point de vue de l'utilisateur, la facilité d'accès doit être la même, quel que soit l'endroit où il travaille.

Trois considérations pour les équipes informatiques

Alors que les gouvernements prennent les mesures adéquates pour rouvrir les sites physiques, les responsables de la sécurité et/ou du réseau doivent tenir compte de trois éléments clés avant la réouverture.

1 Fournir un accès Zero Trust aux applications privées depuis n'importe quel emplacement

De nombreuses sociétés pensent à tort qu'une stratégie Zero Trust n'est indispensable que pour fournir un accès distant à des applications privées. Elles utilisent les services Zero Trust comme une alternative aux technologies d'accès à distance telles que le VPN ou le VDI, qui placent les utilisateurs sur le réseau. Les employés au bureau sont la plupart du temps autorisés à se connecter aux ressources du réseau parce qu'ils se trouvent déjà à l'intérieur du périmètre et qu'ils jouissent d'une confiance implicite. L'équipe peut avoir procédé à une segmentation du réseau comme mesure de sécurité supplémentaire, ce qui rend le réseau extrêmement complexe. Cela dit, la segmentation du réseau n'est plus nécessaire si les services Zero Trust appropriés sont mis en œuvre. Le même service Zero Trust peut être utilisé pour un utilisateur distant ou travaillant au bureau, et peut être utilisé pour fournir un niveau de segmentation de l'application, sans avoir à gérer ou à faire face à la complexité de la segmentation du réseau sur site.

2 Proposer la meilleure expérience utilisateur possible en privilégiant la cohérence

Plusieurs enquêtes ont révélé que les employeurs et les employés étaient favorables au télétravail. De nombreuses entreprises affirment que leur productivité continue de croître malgré le fait que leurs effectifs de base travaillent à distance, tandis que les employés (le plus souvent) apprécient la liberté de pouvoir travailler de n'importe où. C'est pourquoi de nombreux clients avec qui nous travaillons se penchent sur un modèle de travail hybride, les employés partageant leur temps entre le bureau et leur domicile. Par conséquent, les responsables du réseau et de la sécurité doivent s'assurer que les employés bénéficient d'une expérience fluide et cohérente lorsqu'ils accèdent aux applications depuis n'importe quel endroit, y compris au bureau.

3 Empêcher les appareils compromis d'accéder au réseau de l'entreprise

La popularité croissante des services de sécurité des terminaux comme CrowdStrike, Microsoft et Carbon Black dans le cadre du télétravail est également essentielle. Depuis un certain temps déjà, les utilisateurs d'ordinateurs portables et de smartphones accèdent à des applications sur leurs réseaux personnels lorsqu'ils sont chez eux. Ces mêmes appareils étant emmenés au bureau, dans le bâtiment, il est important que les responsables informatiques les empêchent d'accéder au réseau de l'entreprise. Le service informatique doit s'assurer que chaque appareil qui revient au bureau est propre, afin de réduire la surface d'attaque globale et de minimiser les menaces. Ainsi, la compréhension de la posture de l'appareil et de la santé de celui-ci est essentielle, en particulier lorsque le concept de travail hybride commence à se concrétiser.

Utiliser Zero Trust pour travailler à l'intérieur comme à l'extérieur du bureau

Zero Trust repose sur deux éléments fondamentaux : l'identité et les politiques de l'entreprise.

Au lieu d'utiliser une adresse IP, c'est l'identité qui fournit le contexte de l'utilisateur. Les politiques d'entreprise, qui sont définies par l'équipe chargée du réseau ou de la sécurité, déterminent à quelle application privée un utilisateur autorisé peut accéder. La plateforme Zscaler Zero Trust Exchange™ héberge ces politiques, les applique et, si elle est autorisée, sert de courtier pour la connexion entre l'application et l'utilisateur sur une base égale par application et par session.

Étant donné que l'emplacement des utilisateurs ne cessera de changer, il n'est plus nécessaire de se focaliser sur le réseau. À l'heure où les utilisateurs se préparent à retourner au bureau, il est encore plus impératif de s'affranchir de la confiance implicite et de mettre en œuvre des politiques Zero Trust. L'accès réseau Zero Trust garantit sécurité, rapidité, cohérence et commodité aux utilisateurs, et procure flexibilité et évolutivité aux services informatiques.

Zscaler Private Access pour l'accès des employés au bureau ou à distance à des applications privées

Zscaler Private Access™ (ZPA™) est un service cloud de Zscaler qui fournit un accès Zero Trust transparent aux applications privées exécutées sur le cloud public ou au sein du data center. Il peut prendre en charge aussi bien les applications traditionnelles que les applications basées sur le Web. Le service exploite les informations d'un fournisseur d'identification basé sur SAML et connecte l'utilisateur autorisé à une application spécifique en fonction des politiques d'entreprise définies par le client. Contrairement au VPN ou au VDI, cette opération s'effectue sans placer l'utilisateur sur le réseau de l'entreprise, ce qui supprime la nécessité de la pile de passerelles entrantes. Le service n'expose jamais l'application sur Internet, de sorte qu'elle est invisible pour les attaquants, ce qui est particulièrement important pour l'accès à distance.

ZPA utilise des tunnels internes chiffrés, l'un provenant de l'application, l'autre de l'utilisateur, puis négocie les connexions en temps réel dans l'un de ses emplacements de Service Edge en fonction de l'emplacement de l'utilisateur et de l'appareil. Ceci permet d'assurer le chemin le plus rapide possible entre l'utilisateur et l'application, et supprime le besoin de backhauling vers un data center central. Le Service Edge est soit hébergé publiquement par Zscaler, soit hébergé en privé par le client, auquel cas il est étendu à la filiale ou au data center sur site du client pour une exécution locale. Dans les deux cas, les Service Edge sont gérés par Zscaler.

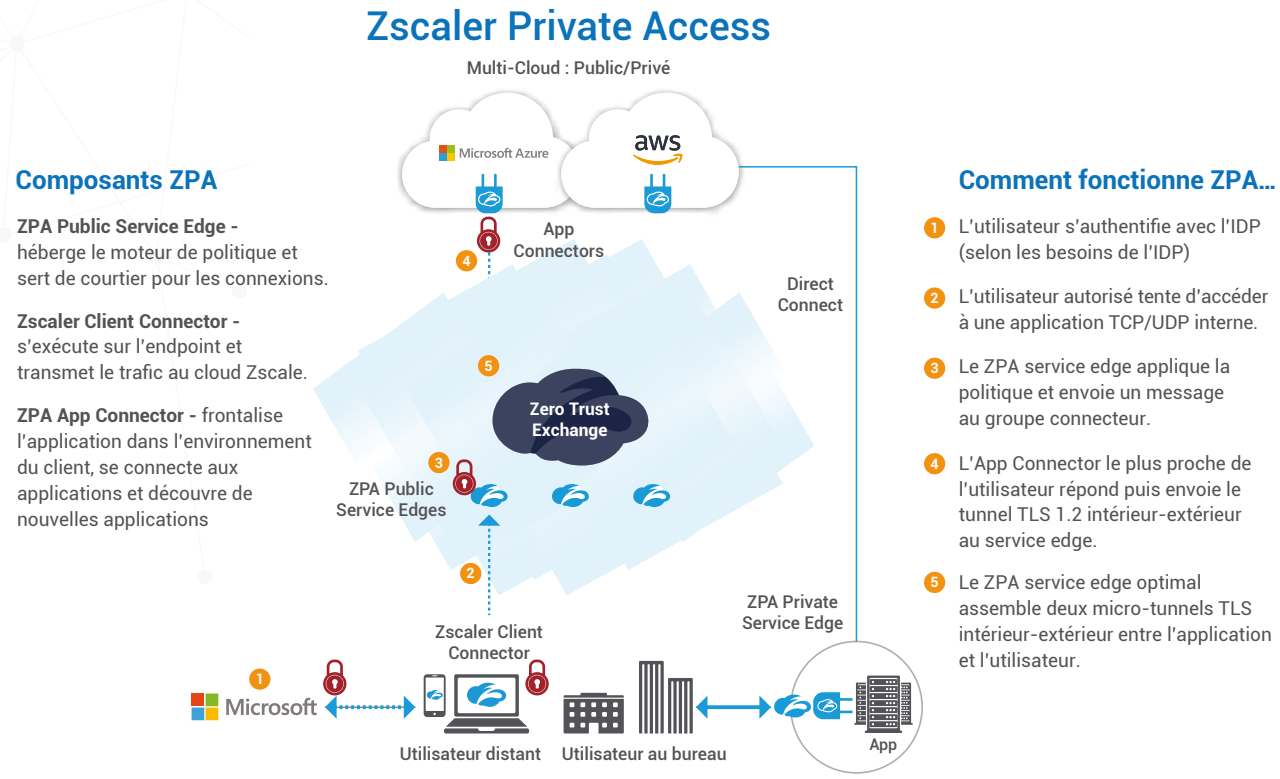
Puisque le service se connecte en fonction de l'utilisateur et de l'application, il permet de segmenter les applications sans devoir recourir à la segmentation du réseau. Cela simplifie la segmentation, permettant au service informatique de définir des politiques par nom d'utilisateur et nom d'hôte plutôt que par IP source et IP de destination.

ZPA utilise des tunnels internes chiffrés, l'un provenant de l'application, l'autre de l'utilisateur, puis négocie les connexions en temps réel dans l'un de ses emplacements de Service Edge en fonction de l'emplacement de l'utilisateur et de l'appareil.

Même avantage qu'une architecture Zero Trust plus hébergement sur site

Pour les sociétés qui préfèrent héberger elles-mêmes un Service Edge ZPA, nous avons conçu ZPA Private Service Edge. ZPA Private Service Edge est une instance privée, à entité unique, qui fournit la fonctionnalité complète d'un Service Edge ZPA public dans l'environnement propre de l'entreprise. Le client héberge ZPA Private Service Edge sur site ou sur un service cloud, qui est géré par Zscaler. ZPA Private Service Edge télécharge les politiques et les configurations appropriées depuis le cloud, de sorte qu'il peut appliquer toutes les politiques ZPA localement.

ZPA Private Service Edge et les services ZPA classiques hébergés par Zscaler peuvent être utilisés conjointement. ZPA choisira automatiquement le chemin le plus rapide entre l'utilisateur et la destination afin d'éliminer la latence.



Principaux avantages de ZPA Private Service Edge

Réduction de la complexité et des coûts

Avec ZPA Private Service Edge, plus besoin de pare-feu internes et autres appliances supplémentaires. Cela réduit non seulement les coûts, mais aussi la nécessité de créer des segments de réseau complexes destinés à fournir un accès aux applications à des utilisateurs locaux.

Haute disponibilité

ZPA Private Service Edge met les politiques d'accès en cache pendant des semaines, permettant aux utilisateurs de se connecter en toute sécurité, même en cas de perte de connectivité Internet. Cela garantit la disponibilité continue de l'accès aux applications, indépendamment de la connectivité.

Expériences utilisateur rapides

ZPA détermine automatiquement le chemin le plus court et le plus rapide permettant à l'utilisateur de se connecter aux applications, en donnant la priorité au Service Edge local de ZPA. Les capacités de double accès du courtage sur site et dans le cloud public optimisent automatiquement les performances pour l'utilisateur, quel que soit l'endroit où se trouvent l'utilisateur et les applications.

Conformité

Des secteurs tels que les services bancaires et financiers exigent des directives strictes concernant l'utilisation des services basés sur le cloud. ZPA Private Service Edge aide les entreprises à se conformer à ces réglementations en leur permettant d'héberger le service sur site.

Politique centralisée avec application locale

ZPA Private Service Edge se synchronise avec les politiques de l'entreprise en se connectant au service cloud de ZPA. Cela garantit que toutes les politiques et configurations pertinentes sont appliquées. En prévision d'une éventuelle défaillance d'Internet, ZPA Private Service Edge met toutes les politiques en cache pendant 14 jours afin de garantir un accès permanent des utilisateurs locaux aux applications privées.

ZPA Private Service Edge offre un moyen plus simple de permettre un accès sécurisé aux applications privées et permet une expérience identique aux utilisateurs (qu'ils soient locaux ou distants qui accèdent aux applications dans le centre de données ou dans le nuage.

Vous souhaitez en savoir plus sur ZPA ? Contactez notre équipe à tout moment : **sales@zscaler.com**.

En savoir plus sur **ZPA Private Service Edge**

Solliciter une démo

À propos de Zscaler

Zscaler (NASDAQ: ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients et plus en sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.fr