Zscaler Private Access pour Microsoft Azure

Accès distant sécurisé aux applications internes dans Azure

zscaler™

ACCÈS SÉCURISÉ À L'ÈRE DU CLOUD MODERNE

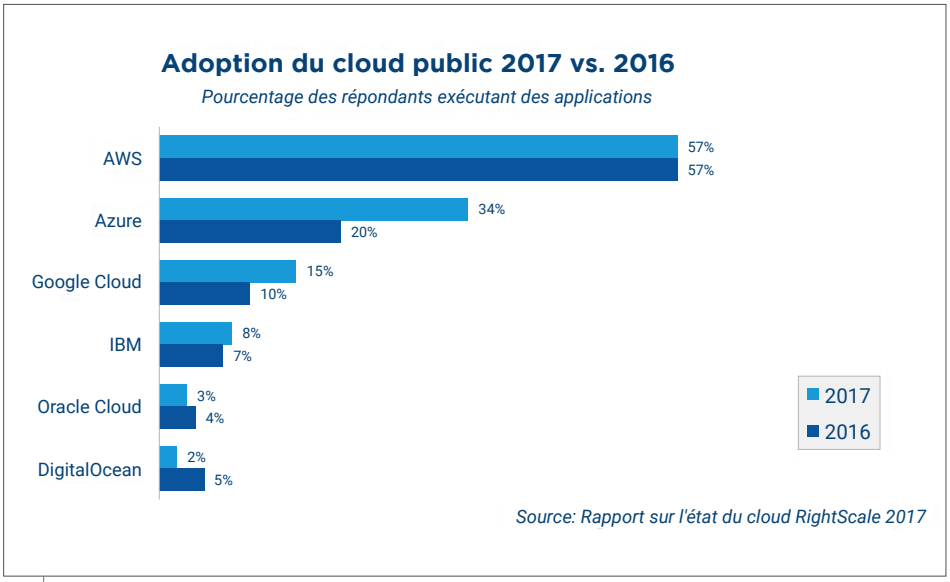
Pourquoi les entreprises migrent vers Azure

Microsoft Azure est devenu partie intégrante de la transformation informatique mondiale. Avec Azure, les entreprises peuvent tirer parti d'un réseau Microsoft mondial, hautement flexible et interconnecté, les aidant à réduire les coûts et la complexité en s'exécutant sur l'infrastructure en tant que service. Le cloud Azure habilite les entreprises en leur donnant de l'agilité, ce qui leur permet d'évoluer de manière élastique et de rester à l'avant des demandes changeantes des entreprises.

Les entreprises sont de plus en plus nombreuses à réaliser ces bénéfices et poursuivent activement les initiatives de transformation des applications centrées sur la migration des applications internes vers Azure. Cette migration a conduit à la croissance rapide d'Azure au sein de l'entreprise et 43% des entreprises exécutent désormais des applications sur Azure.

Azure est également très utile pour les utilisateurs, car il facilite pour les utilisateurs mobiles l'accès aux applications et aux services, quel que soit leur emplacement ou leur fuseau horaire. En plus de maximiser la productivité des utilisateurs, la commodité du cloud a conduit à un changement de statu quo en termes d'attentes des utilisateurs. Les utilisateurs distants, ayant fait l'expérience d'un accès transparent aux applications cloud, s'attendent désormais à bénéficier d'une expérience de type « cloud » pour toutes les applications, y compris les applications gérées en interne et hébergées dans le cloud Azure.

Pour que les entreprises et leurs utilisateurs profitent des avantages du transfert d'applications vers le cloud, le moment est venu de redéfinir l'accès à distance.



L'utilisation de Microsoft Azure a fait un bond dans l'entreprise en 2017, selon le rapport RightScale 2017 State of the Cloud.

Les applications ont migré vers le cloud. Pourquoi l'accès distant dépend-il toujours du data center?

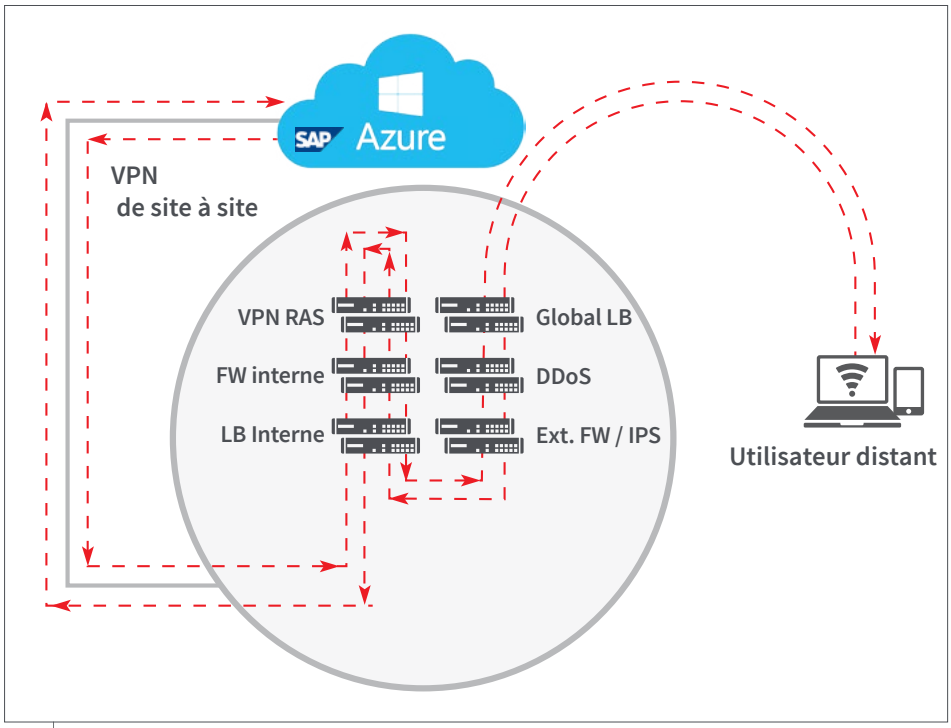
Dans les premiers temps de la sécurité, l'accent était mis sur la protection des données et des applications internes fonctionnant dans le data center. Les architectes de sécurité ont déterminé que la meilleure façon de garantir cette protection était de construire un périmètre sécurisé autour du réseau. Et ainsi, l'architecture cloisonnée que de nombreuses équipes de sécurité connaissent aujourd'hui est née.

Du point de vue de la mise en réseau, l'hébergement d'applications internes dans un seul data center s'inscrivait naturellement dans l'architecture de sécurité cloisonnée. Cela signifiait que tout le trafic provenant d'utilisateurs distants ou de filiales serait redirigé vers ce data center afin d'accéder aux applications. Dans de nombreux cas, ce data center était situé dans une autre partie du monde.

Désormais, les applications qui résidaient autrefois dans le data center sont délocalisées vers le cloud Azure. Cela brise l'idée d'un périmètre sécurisé, car les applications et les données qui doivent être protégées se trouvent désormais à l'extérieur du périmètre. La stratégie en étoile consistant à acheminer le trafic vers un data center central devient inefficace avec les applications exécutées dans Azure. Pourtant, les solutions d'accès à distance d'aujourd'hui dépendent toujours du routage du trafic vers le data center en premier. Mais, compte tenu du manque d'alternatives viables, les entreprises continuent d'utiliser le VPN d'accès distant.

Depuis les années 1990, il n'y a qu'une seule façon de fournir un accès distant aux applications internes: le réseau privé virtuel (VPN) d'accès distant. Mais avec les applications internes migrant vers des fournisseurs de cloud comme Azure, tout en étant accessibles à un nombre toujours croissant de travailleurs distants, il n'est plus logique d'acheminer le trafic via le data center.

> “Les DMZ et anciens VPN ont été conçus pour les réseaux des années 1990 et sont devenus obsolètes, car ils n'ont pas l'agilité nécessaire pour protéger les entreprises numériques.”
>
> *Gartner*
> septembre 2016



Le trafic lié à Internet provenant d'utilisateurs distants prend un chemin lent et indirect, car il est acheminé via la pile de sécurité du data center avant de pouvoir se diriger vers le cloud ou Internet ouvert, puis revient à travers la pile lors de son trajet retour.

Défis de l'accès distant VPN

Mauvaise expérience utilisateur

Les utilisateurs tentant d'accéder aux applications s'exécutant dans le cloud Azure sont obligés de se connecter à un VPN d'accès distant. Leur trafic est ensuite acheminé via le data center, au lieu d'aller directement à Azure.

Coût et complexité élevés

Les VPN d'accès à distance nécessitent plusieurs appliances de passerelle. Cela rend difficile la mise à l'échelle sur plusieurs zones géographiques, car les équipes devraient répliquer les passerelles dans chaque data center. Les VPN d'accès à distance nuisent à la valeur du cloud, telle que son élasticité, sa simplicité et ses économies de coûts.

Risque d'attaque

Les VPN d'accès à distance placent les utilisateurs distants sur le réseau d'entreprise. Cela peut exposer le réseau à des programmes malveillants ou à d'autres attaques de sécurité provenant d'appareils utilisateur non fiables. Le mouvement latéral facilite la propagation des attaques à plusieurs applications.

Accès direct au cloud avec Zscaler Private Access

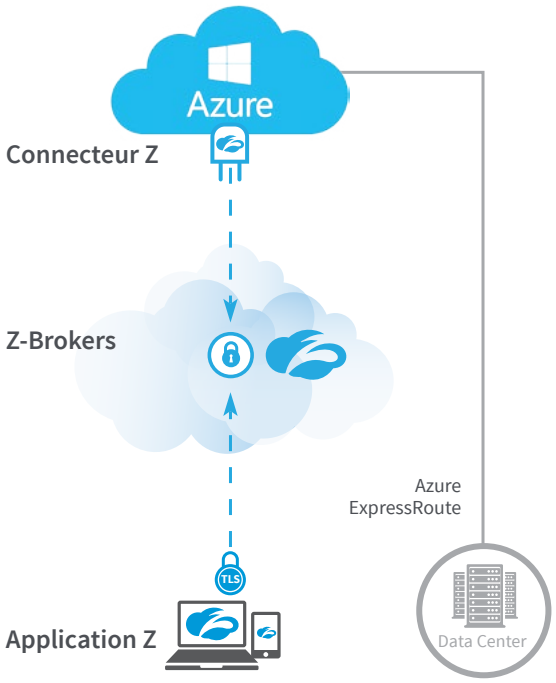
Zscaler Private Access (ZPA™) est un service révolutionnaire de Zscaler qui utilise le cloud Zscaler pour fournir un accès distant sécurisé aux applications internes. ZPA permet aux entreprises de s'affranchir de la mentalité d'accès distant basé sur VPN, qui est centrée autour du data center, pour une approche plus moderne basée sur le cloud.

La clé de sa valeur réside dans la capacité de ZPA à offrir aux utilisateurs distants l'expérience transparente qu'ils souhaitent lorsqu'ils accèdent aux applications internes, tout en donnant aux entreprises la sécurité dont elles ont besoin et la simplicité nécessaire pour faire de la transformation du réseau une réussite.

Z-Connector:
Se situe devant les applications (connexions de l'intérieur vers l'extérieur)

Z-Brokers:
Connexion sécurisée utilisateur-application

Z-App:
Demande l'accès à une application



Zscaler Private Access for Azure

Désormais, les entreprises peuvent combiner les avantages du cloud Azure avec la sécurité renforcée et le périmètre défini par logiciel fournis par ZPA. L'utilisation de ZPA élimine le besoin d'appliances d'accès distant VPN — et les pièges qui leur sont associés. La solution ZPA offre une expérience directe vers le cloud pour tous les utilisateurs, les amenant rapidement et de manière transparente à l'application qui s'exécute dans Azure, plutôt que de les acheminer via une passerelle d'accès distant VPN.

Accès rapide aux applications dans Azure pour les utilisateurs distants

La solution conjointe permet à Zscaler de tirer parti de l'empreinte mondiale de Microsoft pour fournir un accès direct vers le cloud plus rapide aux applications dans Azure pour les utilisateurs distants. Les ZEN (Zscaler Enforcer Nodes), un composant de la solution ZPA, s'exécutent sur le réseau Azure, composé de centaines de data centers et d'équilibreurs de charge mondiaux. Le ZEN est utilisé pour négocier une connexion entre un utilisateur mobile et une application, puis achemine ce trafic. Les Z-connectors, qui se situent devant les applications, s'exécutent également dans Azure, fournissant aux ZEN des connexions de l'intérieur vers l'extérieur.

La combinaison de ZPA et Azure garantit que le trafic utilisateur traverse toujours le chemin optimal en fonction de l'emplacement de l'utilisateur. Étant donné que les utilisateurs distants accèdent à l'application la plus proche d'eux, l'expérience utilisateur s'améliore, tout comme la productivité.

Outre des performances rapides, les utilisateurs bénéficient d'une expérience transparente. Avec un VPN, les utilisateurs doivent se connecter chaque fois qu'ils souhaitent accéder à une application. Mais avec Z-app, qui est installé sur l'appareil mobile de l'utilisateur, les utilisateurs authentifiés ne se connectent qu'une seule fois. Ainsi, les utilisateurs se connectent plus rapidement à leurs applications dans Azure.

Pourquoi ZPA pour Azure?

Zscaler Private Access, associé à l'approche de sécurité d'Azure basée sur le cloud, permet aux entreprises de déterminer qui a accès à quelles applications internes, même lorsqu'elles sont en migration du data center vers Azure. La solution conjointe repose sur les quatre principes clés de Zscaler Private Access.

1 | **Les utilisateurs ne sont pas sur le réseau –** Les utilisateurs ne sont jamais autorisés à accéder au réseau d'entreprise. L'accès est spécifique à l'application, sans qu'il soit nécessaire de définir une politique par adresse IP ou ACL.

2 | **Les applications sont invisibles –** Les adresses IP internes ne sont jamais exposées à Internet. Les applications internes sont sur un « dark-net » d'entreprise et sont complètement invisibles pour les utilisateurs, à moins que ces derniers ne soient autorisés à y accéder.

3 | **Internet devient le nouveau réseau sécurisé –** Zscaler Private Access exploite Internet pour un chiffrement de bout en bout dynamique, spécifique à l'application et basé sur TLS. Toutes les données restent privées et les clients peuvent utiliser leur propre PKI.

4 | **Les politiques fournissent une segmentation au niveau de l'application –** Il n'y a pas d'accès utilisateur-réseau. Les utilisateurs ont un accès direct uniquement aux applications spécifiques et chaque session d'application a son propre micro-tunnel.

Une meilleure expérience pour les utilisateurs distants

- Accès plus rapide aux applications sur Azure
- Plus de client VPN pour chaque session de connexion
- Expérience transparente pour les applications dans Azure ou le data center

Complexité réduite pour les administrateurs

- Facile à mettre en œuvre en une heure; pas besoin de configurer de passerelles VPN
- Segmentation d'applications, non la segmentation réseau
- S'intègre à Azure AD
- S'intègre aux fournisseurs d'authentification unique (SSO), tels que Okta
- Fonctionne de concert avec Azure ExpressRoute

Accès distant sécurisé aux applications internes sur Azure

- Les utilisateurs ne sont jamais sur le réseau
- Accès basé sur des politiques aux applications spécifiques sur Azure
- Aucun accès latéral aux applications internes supplémentaires
- Visibilité sur toutes les applications exécutées dans Azure
- Visibilité sur l'activité des utilisateurs en cours

Valeur commerciale accrue

- Pas besoin d'achat de matériel, donc économies de coûts
- Augmentation de la productivité d'utilisateurs distants
- Le modèle de service convertit la sécurité en une simple et prévisible dépense d'exploitation

> Zscaler contribue à simplifier le parcours de l'entreprise vers les environnements publics Azure Cloud et hybrides…

Yousef Khalidi
Vice-président, Microsoft Azure Networking

Premiers pas avec Zscaler Private Access et Azure

ZPA et Azure ont redéfini la façon dont les applications internes sont accessibles d'une manière qui a été conçue pour permettre l'adoption des technologies cloud et un personnel mobile. Avec cette nouvelle solution, la sécurité — souvent considérée comme un inhibiteur du changement — devient le mécanisme qui accélère la migration des applications internes vers Azure.

Pour plus d'informations ou pour voir une démonstration en direct, veuillez contacter Zscaler par e-mail sur **zpa@zscaler.com** ou visitez **zscaler.com/zpa-for-azure**.

zscaler™

ACCÈS SÉCURISÉ À L'ÈRE DU CLOUD MODERNE