

ZPA™ Private Service Edge

ZTNA (Zero Trust Network Access) est fourni sur site – et maintenant, partout où se trouvent vos utilisateurs

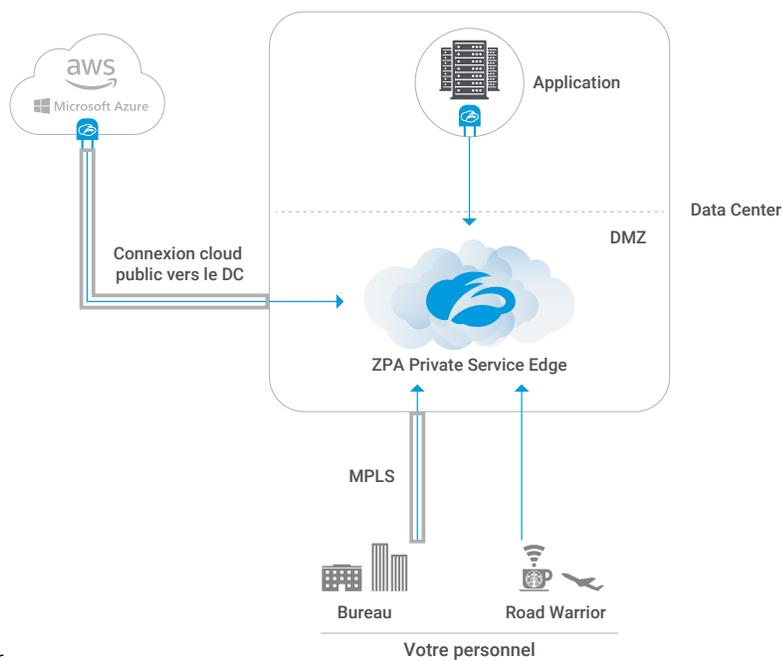


Gartner recommande aux entreprises d'adopter des services d'accès réseau zero trust (ZTNA) pour garantir que l'accès aux applications privées soit basé sur l'identité afin de supprimer le besoin d'accès au réseau et de minimiser l'exposition des applications à Internet. Le besoin d'adopter ZTNA a conduit de nombreuses organisations à déployer Zscaler Private Access™ (ZPA), un service fourni dans le cloud qui permet d'accéder aux applications privées partout où les utilisateurs se connectent – le tout de manière rapide, sécurisée et sans faille.

Mais dans certaines circonstances, les entreprises préféreraient déployer des services de connectivité d'applications dans leurs propres environnements, et c'est la raison pour laquelle nous avons introduit ZPA Private Service Edge. Désormais disponible en tant qu'option supplémentaire du service ZPA, ZPA Private Service Edge est un courtier qui est une instance entièrement fonctionnelle à locataire unique (par client), hébergée par l'organisation cliente et gérée par Zscaler. ZPA Private Service Edge peut être installé sur le site du client ou résider dans un service de cloud public. Comme le service cloud ZPA, le service sur site applique des politiques et établit la connexion entre un utilisateur autorisé et une application privée spécifique.

La fonctionnalité du service cloud ZPA, mais plus à proximité

Avec le service ZPA fourni dans le cloud, lorsqu'un utilisateur demande l'accès à une application privée, le trafic de cet utilisateur est transféré à un data center cloud de Zscaler™ sur Internet. La connexion entre un utilisateur autorisé et une application privée est établie dans le cloud. Voilà qui rend ZPA idéal pour les utilisateurs distants, tels que les télétravailleurs et les prestataires tiers, qui cherchent à accéder aux applications privées fonctionnant sur site ou dans des cloud publics ou privés, ZPA élimine le backhauling. Mais pour les utilisateurs sur site qui cherchent à accéder à une application fonctionnant également sur site, il ne serait pas logique de transiter absolument par Internet. C'est ici qu'intervient ZPA Private Service Edge.



“ ZPA nous permet d'avoir une visibilité immédiate quant à ce qui se passe sur notre réseau, y compris quelles applications sont accessibles et par qui, et d'une manière encore plus détaillée que jamais auparavant ».

Peter Daly, directeur des services de réseau - Global Infrastructure chez Johnson Controls

Comme pour le service cloud, ZPA Private Service Edge gère les connexions entre Zscaler Client Connector (anciennement Z-App) et un App Connector. Lorsqu'il est déployé, il s'inscrit dans le cloud de Zscaler. Cela permet à ZPA Private Service Edge de télécharger les politiques et configurations adéquates afin qu'elles puissent être appliquées. Il met également en cache les décisions relatives à la sélection des chemins. ZPA Private Service Edge se déploie sous la forme d'une machine virtuelle/RPM légère qui est installée par les clients dans leur propre environnement réseau. Une fois configuré, ZPA Private Service Edge fonctionne exactement de la même manière que le service cloud ZPA. Pour les utilisateurs sur site, ou même les utilisateurs distants dans les pays où il n'y a pas de service cloud ZPA, l'accès aux applications privées est négocié via ZPA Private Service Edge et est toujours transparent, rapide et sécurisé.

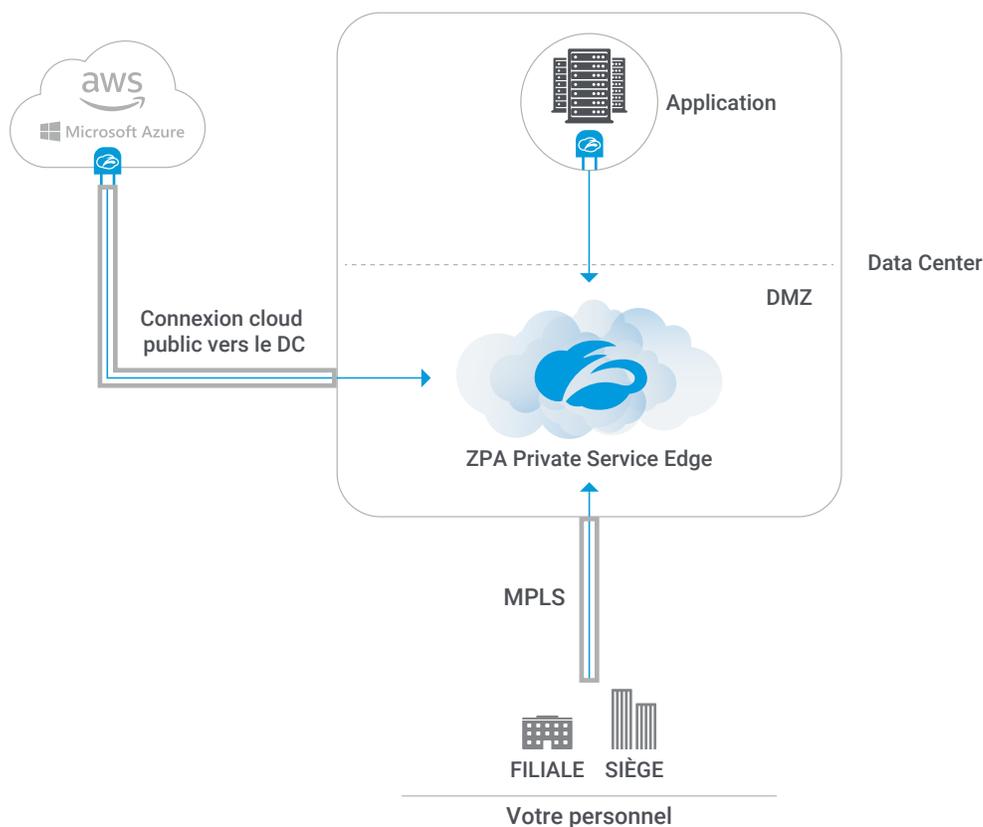
Il est important de noter que les administrateurs peuvent toujours configurer ZPA de sorte que ZPA Private Service Edge et le service cloud ZPA puissent être utilisés pour garantir la meilleure expérience possible aux utilisateurs cherchant à se connecter aux applications privées.

Cas d'usage courants pour ZPA Private Service Edge

L'extension du service ZPA à votre environnement sur site vous aide à réussir dans divers cas de figures:

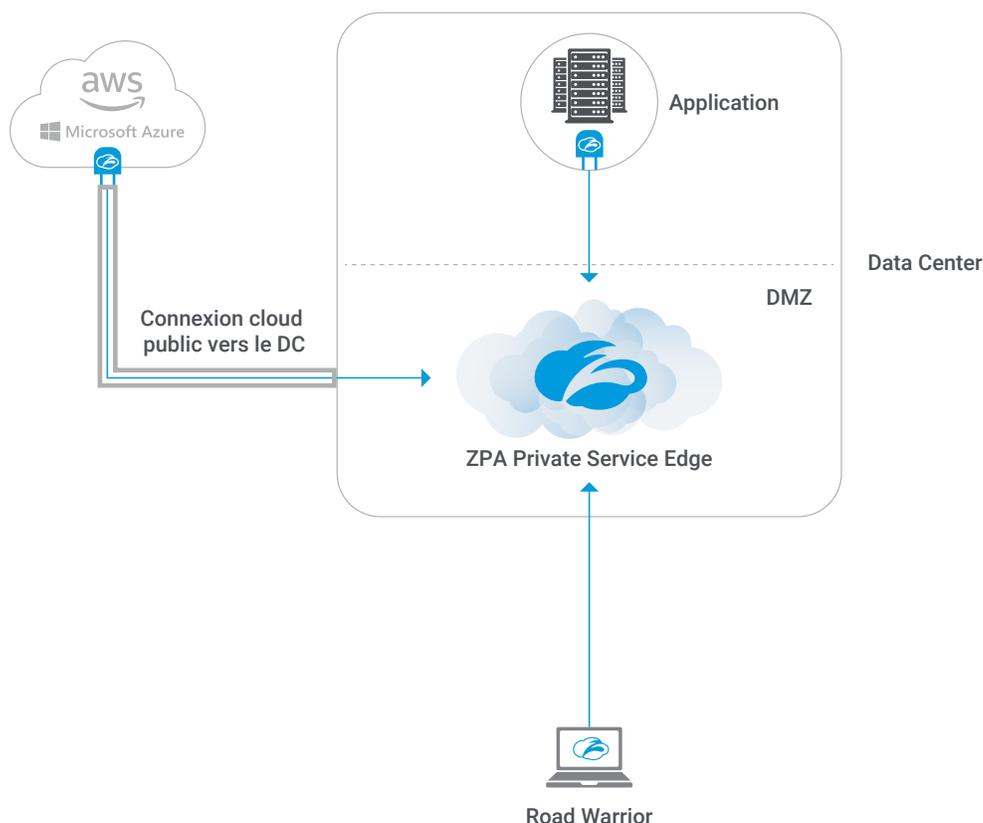
Accès au réseau zero trust pour un personnel sur site

Pour les utilisateurs travaillant au siège social ou dans des filiales et qui cherchent à accéder aux applications s'exécutant sur site ou dans des cloud publics, il n'est pas logique que le trafic sorte d'abord vers un courtier public ZPA, avant de revenir à l'application s'exécutant localement. ZPA Private Service Edge assure le courtage local entre les utilisateurs et les applications sur site, ce qui crée pour les utilisateurs une expérience plus rapide, pour les administrateurs réseau moins de complexité, et moins de risque pour les données commerciales en permettant un accès basé sur le principe du moindre privilège.



Service Edge local pour le personnel en télétravail

Dans des pays (comme l'Algérie) où il n'y a pas de ZPA Public Service Edge, les utilisateurs distants devront se connecter à un ZPA Public Service Edge opérant dans un pays étranger (tel que l'Allemagne) pour pouvoir accéder à une application s'exécutant sur site au siège social. Avec ZPA Private Service Edge, ces utilisateurs distants peuvent accéder aux applications s'exécutant sur site, et ZPA détermine automatiquement le chemin le plus rapide pour chaque utilisateur et sélectionne le courtier le mieux adapté à la tâche.



Infrastructure privée requise pour la conformité

Certains pays, en particulier ceux qui sont sujets aux catastrophes naturelles, et les industries réglementées (comme les banques) exigent que les services de sécurité fonctionnent sur site – non qu'ils soient hébergés dans le cloud – afin de garantir une haute disponibilité. ZPA Private Service Edge permet aux clients de se conformer aux réglementations industrielles en vigueur dans leur pays en opérant localement et en gérant l'ensemble du courtage dans le propre environnement du client.

“ ZTNA fournit un accès contrôlé aux ressources, réduisant ainsi la surface d'attaque. L'isolement offert par ZTNA améliore la connectivité en éliminant la nécessité d'exposer directement les applications à Internet. Internet devient un moyen de transport non fiable, et l'accès aux applications se fait par un intermédiaire. L'intermédiaire peut être un service cloud contrôlé par un fournisseur tiers ou un service auto-hébergé. »

Gartner, Guide du marché pour Zero Trust Network Access | Steve Riley, Neil MacDonald, Lawrence Orans, avril 2019

PRINCIPAUX AVANTAGES DE ZPA PRIVATE SERVICE EDGE

La possibilité d'héberger les services de courtage de ZPA sur site (sur la base de l'identité), sans segmentation du réseau, entraîne une foule d'avantages pour les clients actuels de Zscaler Private Access™ tout comme pour les nouveaux clients.

- **Segmentation simplifiée** – Abandonnez les politiques « IP source vers IP destination » au profit des politiques « utilisateur vers nom d'hôte ». Réduisez la complexité de la segmentation du réseau qui comprend le maintien d'une liste d'adresses IP pour les firewall et la définition de différentes politiques pour les utilisateurs locaux ou distants. Avec ZPA Private Service Edge, le cadre de politique devient plus fixe et plus facile à gérer.
- **Adoption accélérée de l'hybride et du multicloud** – ZPA Private Service Edge peut s'exécuter dans le data center ou dans un cloud public. Cela signifie qu'il n'y a pas de changement dans la politique d'accès, même après la migration d'une application privée vers des services de cloud public comme Azure, AWS et Google.
- **Accès basé sur le principe du moindre privilège pour les utilisateurs locaux** – La possibilité d'activer sur site l'accès au réseau zero trust crée une connexion chirurgicale et négociée 1:1 entre un utilisateur local autorisé et une application spécifique, empêchant l'accès latéral au réseau et minimisant le risque.
- **Haute disponibilité** – Les régions du monde où la connectivité internet est faible peuvent bénéficier de ZPA Zscaler Private Service Edge, qui met en cache les politiques d'accès pendant des semaines, permettant ainsi une connectivité sécurisée même en cas de perte de connectivité internet.
- **Expérience utilisateur rapide et fluide** – L'accès est identique, que l'on travaille à distance ou localement. La double capacité d'accès sur site et dans le cloud public se négociant automatiquement optimise l'expérience des utilisateurs locaux lorsqu'ils accèdent aux applications privées s'exécutant sur site, et des utilisateurs distants dans les pays où il n'y a pas de courtier cloud ZPA.
- **Évitement des coûts** – L'utilisation de firewall internes peut être réduite et la nécessité de nouveaux investissements peut également être évitée. Il n'est pas nécessaire d'acheter des firewall supplémentaires ou de créer de nouveaux segments de réseau juste pour permettre aux utilisateurs locaux d'accéder aux applications.
- **Conformité** – Pour les industries hautement réglementées, cette infrastructure privée peut aider les clients à se conformer à toutes les normes qui empêchent l'utilisation de la technologie hébergée dans le cloud.

Contactez-nous pour toute question concernant le service ZPA ou visitez le site zscaler.com/zpa.
Pour des informations plus approfondies sur ZPA Private Service Edge, lisez la [documentation d'aide Zscaler](#).

À propos de Zscaler

Zscaler (NASDAQ: ZS) accélère la transformation numérique afin que les clients puissent être plus agiles, plus efficaces, plus tenaces et plus sécurisés. La plateforme Zero Trust Exchange de Zscaler 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 en ligne.

