Zscaler Private Access

Solution révolutionnaire pour l'accès à distance sécurisé à vos applications internes, qu'elles résident dans un centre de données ou chez des fournisseurs de services cloud comme AWS ou Azure.

Zscaler Private Access (ZPA) est un service cloud pour l'accès sécurisé aux applications internes. Le modèle zero trust simplifie votre architecture réseau.

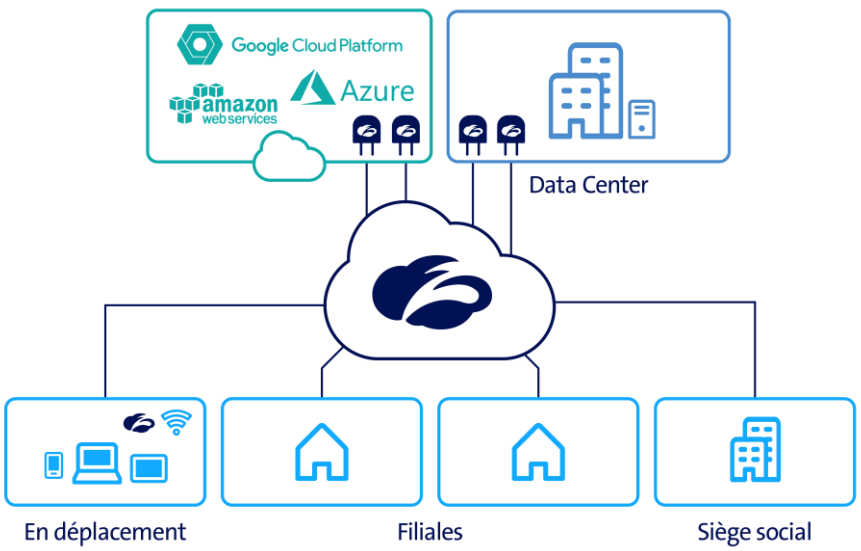
Zscaler Private Access, qu'est-ce que c'est?

Vous octroyez aux utilisateurs de votre choix un accès à vos applications internes via des connecteurs ZPA. Absolument invisible à tout utilisateur non autorisé, cet accès ne transite pas par Internet. Vos applications accèdent au cloud ZPA au moyen de connecteurs. Cette connectivité bidirectionnelle évite la création de zones de vulnérabilité dans votre centre de données.
Vos utilisateurs se connectent au cloud au moyen de l'appli Z. Le modèle zero trust vous permet d'attribuer les autorisations d'utilisateurs aux applications au lieu de gérer des réseaux, zones et autres pare-feux. Le service vous procure une restriction logicielle qui fonctionne dans tous les environnements informatiques, sur tous les appareils et toutes les applications internes.

Vos avantages avec Zscaler Private Access

- Architecture simple et économique
  Pas de liaison des applications internes avec des tunnels réseau onéreux. Réduction du nombre de pare-feux et zones pour une architecture plus simple.
- Accès uniformisé
  Vos utilisateurs bénéficient d'un accès permanent à toutes les applications, sur tous les appareils.
- Segmentation en fonction des applications
  Des microtunnels vous permettent de gérer directement l'accès des utilisateurs aux applications.
- Les utilisateurs n'accèdent jamais au réseau
  Vos utilisateurs autorisés accèdent aux applications sans liaison au réseau. On évite ainsi tout espionnage ou accès non autorisé.
- Performances de pointe pour les applications cloud
  ZPA assure performance et évolutivité au niveau de votre centre de données et des fournisseurs cloud, sans la moindre exigence en matière de hardware.

swisscom.ch/zscaler



swisscom

Swisscom (Suisse) SA, Enterprise Customers, case postale, CH-3050 Berne, tél. 0800 800 900, www.swisscom.ch/enterprise

Faits et chiffres

Zscaler Private Access (ZPA)	Professional suite	Business suite	Enterprise suite
Visibilité mondiale des utilisateurs et applications Visualisation sur portail de tous les utilisateurs et applications internes	●	●	●
Accès sécurisé aux applications internes Accès à une quantité illimitée d'applications internes privées (cloud public/privé/hybride ou ancien centre de données). Pas d'accès utilisateurs au réseau ou de visibilité des applications sur Internet	●	●	●
Découverte des applications et serveurs Une règle joker met en évidence les sites d'applications et de serveurs sur la base des requêtes initiales émises par les utilisateurs	●	●	●
Entreprise DarkNet avec protection DDoS des applications Les applications internes ne sont visibles que par les utilisateurs autorisés	●	●	●
Configuration et définition centralisées des règles Règles et configurations peuvent aussi être centralisées pour tous les utilisateurs dans le cadre d'une utilisation au niveau mondial	●	●	●
Passive health monitoring Surveillance passive de la disponibilité des applications internes	●	●	●
Appli Zscaler Application client pour l'accès à Zscaler Internet Access et Zscaler Private Access	●	●	●
Microsegmentation en fonction des applications Contrôle d'accès granulaire en fonction des utilisateurs et groupes pour cinq définitions d'application au maximum. Chacune d'entre elles peut comprendre une quantité d'hôtes et/ou de ports	●	—	—
Microsegmentation en fonction des applications Comme ci-dessus. Pour un maximum de 10 000 définitions d'applications spécifiques	—	●	●
Continuous health monitoring La surveillance des applications internes vérifie que l'utilisateur peut accéder aux ports et à l'application	—	●	●
Device posture enforcement Vérifie l'identité et les certificats de l'appareil ainsi que d'autres caractéristiques	●	●	●
PKI client spécifique Les certificats mis à disposition par le client assurent une confidentialité optimale des données pour toutes les applications	○	○	●
Cryptage redondant Pour le verrouillage de tous les microtunnels grâce au matériel de cryptage fourni par le client	○	○	●
Real-time transaction view Journalisation en temps réel de l'assistance à l'utilisateur	—	—	●
Log streaming service Envoi des journaux en temps réel à un SIEM	○	●	●

● = Standard (compris dans le prix) ○ = Supplément de prix — = Non disponible