Fiche technique

Zscaler Zero Trust SD-WAN

Connectez en toute sécurité les sites distants, les usines et les data centers et étendez la sécurité Zero Trust aux serveurs et dispositifs IoT/OT, n'importe où.

Le travail hybride et la transformation vers le cloud ont bouleversé les modèles de réseau et de sécurité basés sur le périmètre, avec le déplacement des applications privées vers le cloud et l'accès des utilisateurs aux applications via l'Internet public, sur n'importe quel appareil et depuis n'importe quel emplacement.

Dans le paysage actuel, de nombreuses entreprises exploitent également des dispositifs IoT/OT sur différents sites, notamment les sites distants, les usines et les data centers, pour rationaliser leurs opérations. De plus, un nombre considérable de clients s'appuient sur la communication des charges de travail de serveur à client. Les approches traditionnelles qui dépendent des anciens réseaux WAN, VPN maillés et pare-feu pour gérer l'accès aux applications sont devenues inefficaces dans un monde qui privilégie les technologies cloud et mobiles.

Cependant, à mesure que les exigences des entreprises évoluent, les solutions WAN traditionnelles peinent à suivre. Le SD-WAN s'accompagne de divers écueils, tels qu'une sécurité limitée par un accès basé sur le réseau, un élargissement de la surface d'attaque, des privilèges étendus favorisant les déplacements latéraux et des complexités de routage. L'application des principes Zero Trust à ce réseau requiert souvent l'ajout d'appliances de pare-feu supplémentaires, ce qui augmente les coûts et la complexité.

Zscaler Zero Trust SD-WAN:

- **Facilite une connectivité Zero Trust omniprésente** pour tous les utilisateurs, appareils, serveurs et l'IoT/OT, quel que soit l'emplacement.
- **Améliore les performances des applications** en envoyant le trafic des sites distants directement vers Zero Trust Exchange et le trafic des applications fiables directement sur Internet avec des points d'accès directs à Internet.
- **Empêche le déplacement latéral des menaces :** Zero Trust constitue une base pour une connectivité sécurisée qui permet une segmentation est-ouest.
- **Élimine la surface d'attaque** en connectant les sites distants et les data centers via Zero Trust Exchange, indépendamment du transport sous-jacent.
- **Permet la découverte et la classification des dispositifs IoT fantômes** avec une classification automatique des dispositifs basée sur les profils de trafic.
- **Simplifie l'accès sécurisé aux ressources OT** avec un accès par navigateur sans client aux ports SSH/RDP/VNC sur les actifs OT.
- **Applique des politiques de transfert précises** pour le trafic Internet et non Internet à l'aide de ZIA ou ZPA.
- **Propose un déploiement prêt à l'emploi :** le provisionnement sans contact (ZTP) simplifie le déploiement et réduit le temps d'intégration.

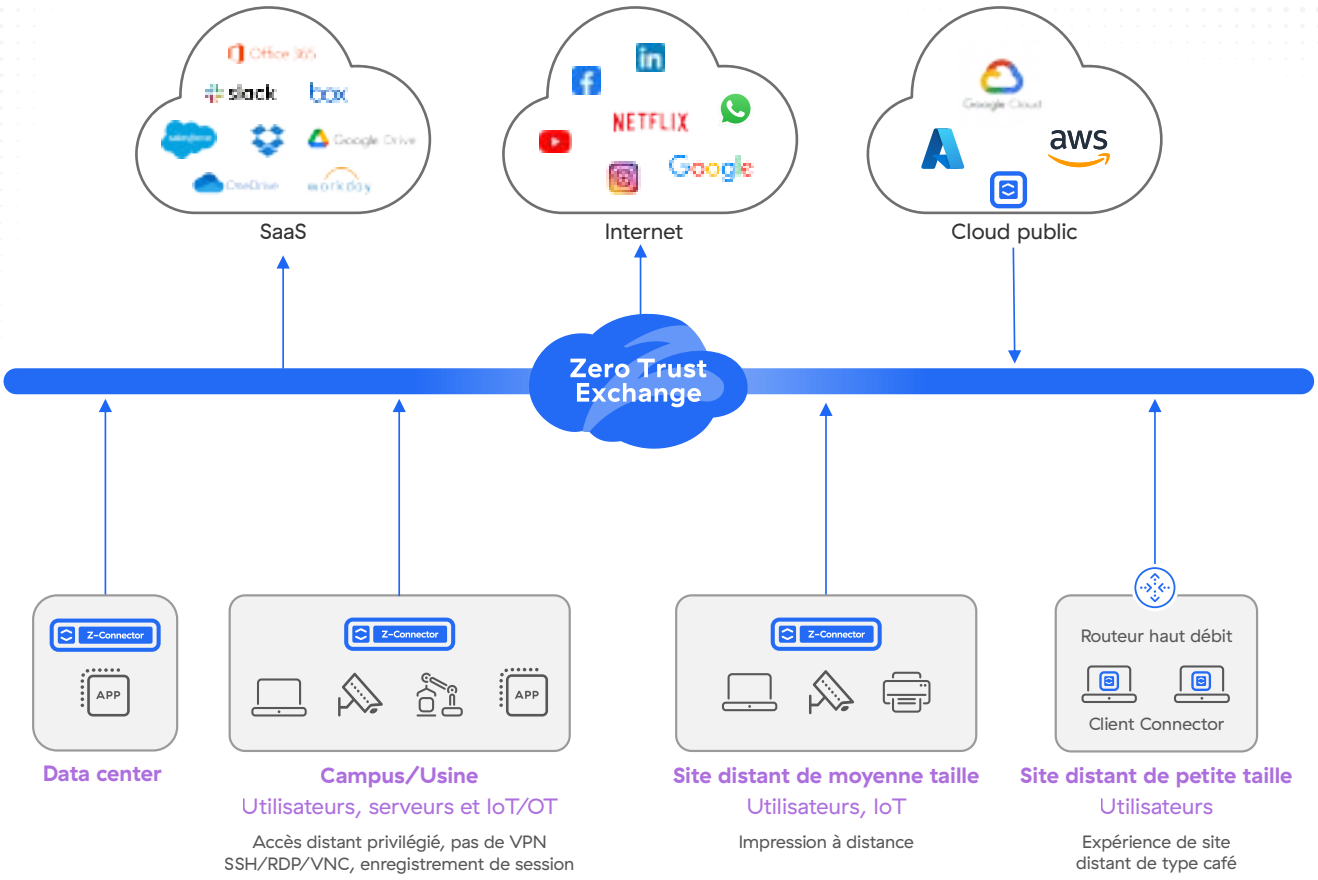

Illustration 1 : SD-WAN Zero Trust

Le SD-WAN Zero Trust connecte en toute sécurité vos sites distants, usines et data centers sans la complexité des VPN, garantissant un accès Zero Trust entre les utilisateurs, les dispositifs IoT/OT et les applications en fonction des politiques de l'entreprise.

Le SD-WAN traditionnel n'est pas le Zero Trust

Les entreprises sont confrontées à plusieurs défis lorsqu'elles utilisent des architectures de réseau et de sécurité traditionnelles pour connecter un site distant à Internet ou à leurs autres applications dans un environnement de cloud public ou de data center, notamment :

- **Augmentation du risque de menaces latérales et d'attaques basées sur Internet** liées à l'utilisation de solutions de connectivité traditionnelles centrées sur le réseau, telles que les VPN site à site, les pare-feu ou les SD-WAN traditionnels. Ces solutions étendent excessivement le réseau de confiance d'un client sur Internet à d'autres environnements cloud et sur site, augmentant ainsi la surface d'attaque. Une mosaïque d'appliances de sécurité, d'outils et de politiques non standard augmente le risque de sécurité en raison de lacunes connues et inconnues dans la couverture de sécurité.

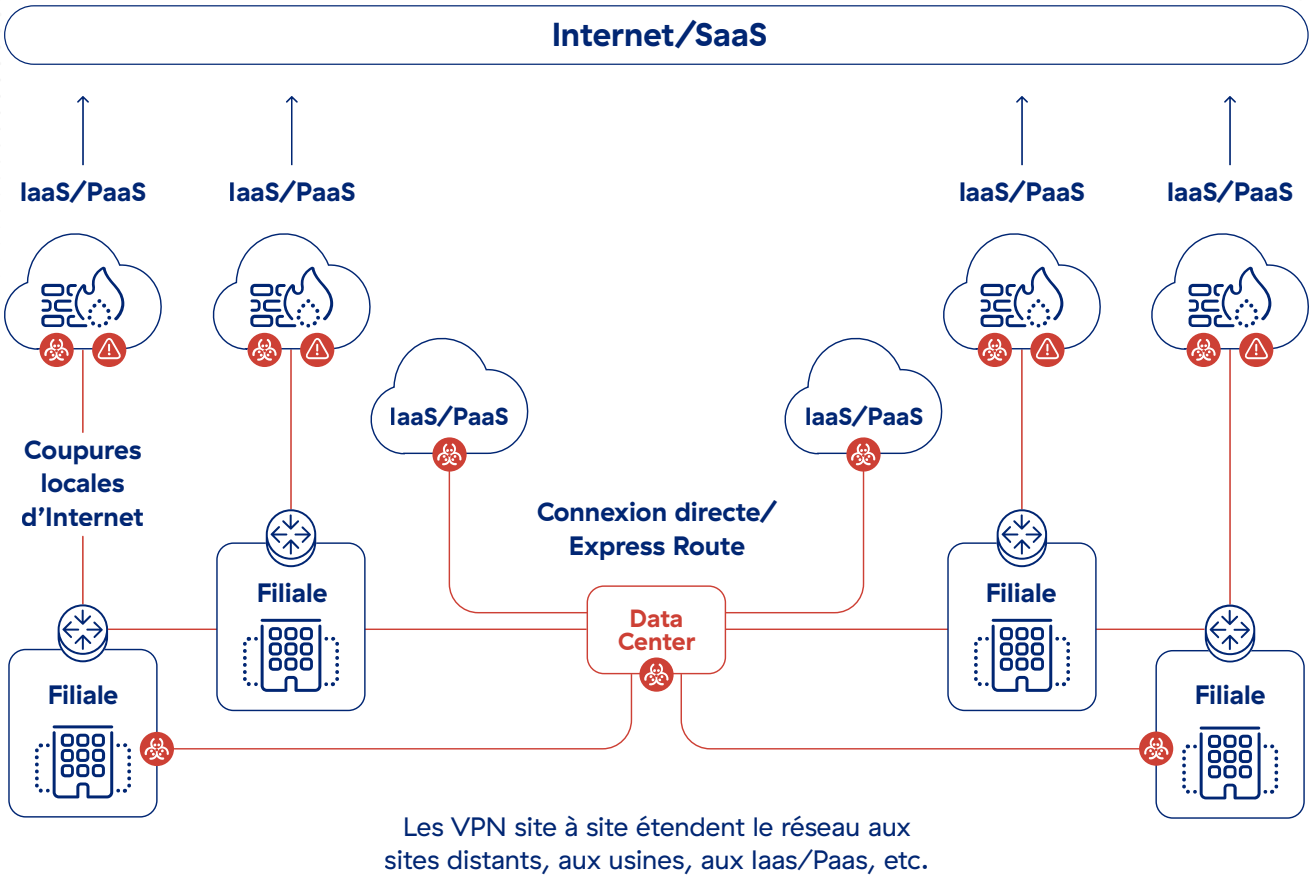

Illustration 2 : Augmentation du risque de menaces latérales et d'attaques basées sur Internet avec les SD-WAN traditionnels

- **Augmentation de la complexité** en raison d'un routage compliqué, de multiples sauts de réseau, de diverses appliances et d'une gestion fragmentée des politiques résultant de l'introduction de modèles traditionnels dans le cloud. La gestion de cette complexité constitue une tâche difficile pour les équipes réseau et sécurité, qui s'efforcent de normaliser la connectivité et d'appliquer les politiques de sécurité dans les sites distants, le cloud et les data centers.
- **Manque de visibilité** sur les chemins de connectivité des sites distants, des data centers et du cloud, ce qui crée des angles morts au niveau du réseau et de la sécurité.
- **Mauvaises performances et évolutivité insuffisante** imputables au nombre croissant de services de réseau et de sécurité dans les sites distants et les data centers, du hairpinning et des congestions du trafic inhérents à l'inspection et au contrôle de sécurité centralisés.
- **Coûts élevés** imputables aux appliances de réseau et de sécurité traditionnelles (par exemple, pare-feu, IPS, routeurs et autres produits ponctuels), au surprovisionnement des services réseau pour compenser le manque d'évolutivité et à l'utilisation accrue de services cloud natifs.

Comment fonctionne le SD-WAN Zero Trust

Le SD-WAN Zero Trust permet aux entreprises de créer un site distant allégé en éliminant plusieurs produits tels que les routeurs, les pare-feu et les VPN au profit d'un simple appareil prêt à l'emploi qui peut être déployé rapidement avec une simple connexion Internet. Cela permet aux entreprises de réduire la complexité associée à la gestion de plusieurs appareils et d'optimiser la fonctionnalité globale du site distant. Le SD-WAN Zero Trust simplifie considérablement les communications des sites distants grâce à une superposition de réseau Zero Trust qui permet un transfert flexible et une gestion simple des politiques en utilisant le cadre de politiques éprouvé de ZIA et ZPA.

Le trafic des sites distants est transmis de manière sécurisée directement vers Zero Trust Exchange, où les politiques ZIA ou ZPA peuvent être appliquées pour une inspection de sécurité complète et un contrôle d'accès basé sur l'identité des communications des sites distants et des data centers. Le trafic des applications fiables peut être envoyé directement sur Internet avec un point d'accès direct à Internet Cette approche unique offre trois avantages majeurs :

- Vous abandonnez la connectivité VPN site à site basée sur le réseau au profit d'une communication basée sur l'identité et les applications pour une véritable sécurité Zero Trust.
- Vous éliminez l'architecture cloisonnée traditionnelle sans compromettre la sécurité ; plus besoin de produits obsolètes, tels que les proxys Squid, les passerelles NAT, les IPS, etc.
- Vous fournissez une connectivité distribuée et évolutive partout où cela est nécessaire, avec une gestion centralisée et automatisée des politiques pour simplifier les communications des sites distants et des data centers.

Cas d'utilisation de SD-WAN Zero Trust

Remplacement du VPN site à site

Connectez vos sites distants directement à des applications privées sans étendre votre WAN ni dépendre de VPN, ces derniers augmentant la surface d'attaque d'un réseau. Les applications sont cachées derrière les sites distants et l'accès est restreint via Zero Trust Exchange à un ensemble d'entités nommées. L'identité, le contexte et le respect de la politique des participants spécifiés sont vérifiés avant que l'accès ne soit autorisé, ce qui interdit tout déplacement latéral ailleurs dans le réseau.

Fusions et acquisitions

La fusion de deux réseaux distincts est complexe et prend du temps. Les problèmes vont des chevauchements IP et des problèmes de routage à l'augmentation des risques de sécurité liés à l'élargissement de la surface d'attaque du réseau. Avec le SD-WAN Zero Trust, les réseaux peuvent rester séparés et les sites distants d'un environnement peuvent se connecter rapidement aux applications privées d'un autre environnement, sans interruption.

Accès direct à Internet pour les sites distants

Les modèles de réseau et de sécurité sur site perdent en efficacité à mesure que les entreprises migrent leurs applications vers le cloud et créent des applications cloud natives. Zscaler Zero Trust SD-WAN est une solution spécialement conçue pour la transformation des sites distants, inaugurant un nouveau modèle qui permet aux sites distants de communiquer avec n'importe quelle destination en toute sécurité et indépendamment du réseau sous-jacent.

Zero Trust pour la connectivité au serveur et aux ressources IoT/OT

Les employés et les fournisseurs tiers doivent accéder régulièrement aux ressources IoT/OT afin de maximiser le temps de production et d'éviter les perturbations dues aux pannes d'équipement et de processus. Le SD-WAN Zero Trust pour l'IoT/OT fournit un accès de bureau à distance entièrement isolé et sans client aux systèmes cibles RDP et SSH, sans avoir à installer un client sur leur appareil à l'aide d'hôtes de saut et des VPN traditionnels.

Découverte et visibilité de l'IoT/OT fantôme

Les équipes informatiques sont confrontées à des angles morts lorsque des dispositifs non autorisés et indétectables se connectent aux réseaux des sites distants. Il en résulte une augmentation de la vulnérabilité des dispositifs et un élargissement de la surface d'attaque. Zscaler identifie et classe les dispositifs pour donner aux équipes informatiques une visibilité plus approfondie sur leur comportement et de meilleures politiques de contrôle d'accès.

Appliances prêtes à l'emploi Z-Connector

Fonctionnalité	ZT 400	ZT 600	ZT 800	Machine virtuelle ZT
				Z-Connector
Type	Sites distants de petite et moyenne taille	Sites distants de petite et moyenne taille	Sites distants de taille moyenne à grande	Sites distants et data center
Débit/ hyperviseur	200 Mbit/s	500 Mbit/s	1 Gbit/s	KVM, ESXi
Ports physiques	4 x GbE	6 x GbE	8 x GbE	S/O
Provisionnement sans contact	✓	✓	✓	✓
Politique de transfert granulaire pour Internet, les applications privées et le trafic WAN direct	✓	✓	✓	✓
Filtrage des URL, contrôle du type de fichier et politiques de pare-feu cloud pour le trafic Internet	✓	✓	✓	✓
Politiques Zero Trust ZPA pour les dispositifs et serveurs IoT	✓	✓	✓	✓
Visibilité et journalisation centralisées	✓	✓	✓	✓

CAPACITÉS SD-WAN ZERO TRUST DE ZSCALER	
FONCTIONNALITÉ	**DESCRIPTION**
Capacités	
Provisionnement sans contact et déploiement automatisé	• Provisionnement sans contact avec des modèles prédéfinis • Déploiement entièrement automatisé • Découverte dynamique de la géolocalisation des sites distants
Politique de transfert granulaire pour le trafic Internet et des applications privées	• Options d'envoi du trafic vers ZIA, ZPA, ou directement vers Internet • Critères flexibles de sélection du trafic : emplacement, sous-emplacement, groupe d'emplacements, objets à cinq tuples ou FQDN
Politiques unifiées de Zero Trust	• Politique unifiée d'utilisateur à application, de dispositif IoT à application et de serveur à serveur grâce à la politique améliorée de ZPA pour inclure de nouveaux types de clients • Politiques basées sur l'emplacement et la géolocalisation • Activation de politiques de sécurité incluant l'IPS, le proxy SSL, le filtrage d'URL et la protection des données • Pile de sécurité complète avec posture configurée pour l'IoT/OT et les serveurs
Haute disponibilité	• Deux instances de SD-WAN Zero Trust en mode haute disponibilité fournissant un support supplémentaire pour les pics de trafic et la redondance en cas de défaillance matérielle • Tolérance de panne active-passive utilisant une adresse IP virtuelle (VIP) basée sur le protocole CARP (Common Address Redundancy Protocol) • Circuits actif-actif (appareil unique) • Circuits actif-actif (double appareil lors de l'équilibrage FHRP)
Visibilité centralisée et journalisation granulaire	• Tableau de bord centralisé pour la surveillance de l'intégrité des appareils et du trafic • Filtrage disponible pour les déploiements dans le cloud, les data centers et les sites distants • Journalisation détaillée de chaque session et transaction pour tous les ports et protocoles, y compris toutes les transactions DNS publiques et privées • Intégration complète avec l'infrastructure Nanolog Streaming Service avec option de diffusion des journaux vers le SIEM du client
Terminaison de l'interface WAN	• Connectivité double FAI (Ethernet) • Connectivité multiple (multi-homing) avec une seule appliance
Gestion de l'interface LAN	• Réseaux LAN L3 multiples • Prise en charge du marquage 802.1q/VLAN • Serveur DHCP • Passerelle DNS
Politiques de pare-feu sur l'appareil	• Contrôle d'accès granulaire pour le trafic local de LAN à LAN (est-ouest) • Listes de contrôle d'accès L3 (ACL)
Sélection du chemin d'accès en fonction de l'application	• Sélection dynamique des chemins d'accès pour les applications SaaS ou privées critiques • Connectivité intelligente Zscaler POP • Surveillance SLA et basculement intégrés
Routage	• Routage statique
Data centers/PoP Zscaler	• Zscaler a construit sa plateforme de sécurité cloud dans plus de 150 data centers à travers le monde, stratégiquement placés au plus près des clients. • Disponibilité intégrée avec basculement transparent vers le prochain service PoP disponible

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients de gagner en agilité, productivité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur SASE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler.**

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.fr