Zscaler Zero Trust SD-WAN

Interconnectez en toute sécurité vos sites distants, usines et data centers sans réseau overlay ni déplacement latéral des menaces.

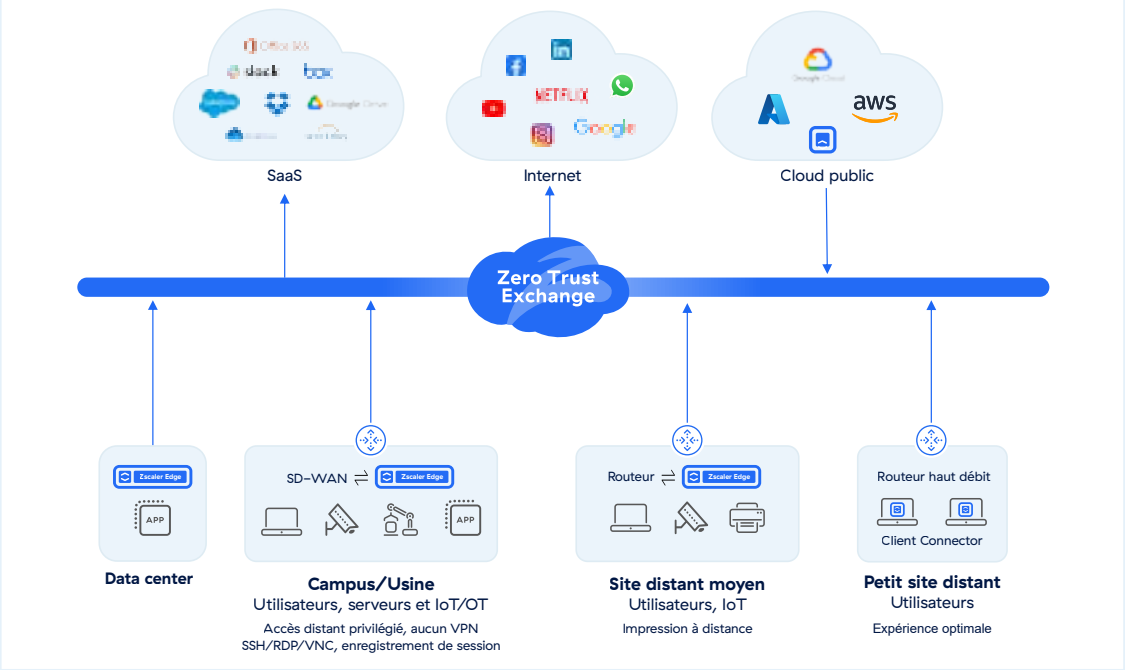
Les SD-WAN traditionnels étendent votre réseau vers les sites distants et le cloud. La surface d'attaque s'étend, les menaces peuvent se déplacer latéralement et les attaques de ransomware ont de meilleures chances de réussir.

La sécurisation des réseaux traditionnels nécessite un panel complexe de pare-feu, de proxys, de passerelles NAC et d'agents sur les terminaux, ce qui renchérit les coûts et accentue la complexité. Vous restez malgré tout vulnérable, face à des attaques de ransomware toujours plus impactantes et nombreuses.

Zscaler Zero Trust SD-WAN offre aux utilisateurs, aux dispositifs et aux instances un moyen plus simple, sécurisé et économique de communiquer, sans la complexité et les défis de sécurité inhérents aux réseaux overlay de routage.

Avantages de Zscaler Zero Trust SD-WAN :

- Interconnecte simplement les sites distants et permet de contrôler l'extension de votre réseau
- Maîtrise le risque de ransomware en éliminant le déplacement latéral des menaces
- Réduit la surface d'attaque en se passant des ports VPN et de pare-feu vulnérables
- Allège les coûts d'infrastructure en simplifiant radicalement l'architecture de votre réseau
- Améliore les performances applicatives en éliminant le backhauling vers les data centers
- Protège les données et neutralise les cyber-menaces en inspectant l'ensemble du trafic



Les SD-WAN traditionnels facilitent les attaques de ransomware

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

- **Expansion de la surface d'attaque :** l'extension du réseau vers les sites distants offre aux hackers davantage de possibilités d'infiltrer votre entreprise. Chaque pare-feu ou passerelle VPN est un point d'entrée potentiel, tandis que les vulnérabilités de type « zero day » sont à la merci d'un exploit.
- **Déplacement latéral des menaces :** un utilisateur ou un appareil IoT infecté, présent sur un site distant est capable de scanner le réseau et de se déplacer latéralement vers d'autres sites, data centers et clouds privés virtuels. Lors de récentes attaques par ransomware, il ne s'est écoulé que 45 minutes entre l'intrusion initiale et les dysfonctionnements majeurs, ce qui laisse trop peu de temps aux équipes opérationnelles pour réagir.
- **Coût et complexité :** le mix de pare-feu, de proxys, d'agents NAC et de politiques basées sur l'IP, conçu pour sécuriser et segmenter les SD-WAN, accentue la complexité, creuse les coûts et pèse sur l'agilité de votre entreprise.
- **Performances et expérience utilisateur médiocres :** le backhauling du trafic vers les data centers et via de nombreux points d'inspection de sécurité se solde souvent par des performances applicatives médiocres et une expérience variable pour les utilisateurs.

Le SD-WAN Zero Trust élimine le déplacement latéral des menaces

Le SD-WAN Zero Trust connecte en toute sécurité vos sites distants, vos usines et vos data centers sans la complexité des VPN ou d'un routage via un réseau overlay. Cette solution garantit un accès Zero Trust entre les utilisateurs, les dispositifs IoT/OT et les applications en fonction des politiques de l'entreprise. En associant la puissance de la plateforme Zero Trust Exchange de Zscaler, leader du secteur, à une connectivité transparente pour les sites, les clouds et les utilisateurs, les entreprises peuvent adopter un cadre SASE (Secure Access Service Edge) et optimiser l'expérience utilisateur sur les sites distants.

- Le SD-WAN Zero Trust fournit aux sites distants, aux campus et aux sites de production un accès rapide et fiable à Internet, au SaaS et aux applications privées, grâce à une architecture direct-to-cloud qui renforce la sécurité et simplifie l'opérationnel.
- Cette solution prévient le déplacement latéral de menaces et réduit considérablement les risques liés aux ransomwares pour votre entreprise.
- Elle allège les coûts d'infrastructure et d'exploitation en éliminant le routage complexe, les VPN et les pare-feu, tout en garantissant une protection complète des données et contre les cybermenaces.

Comment fonctionne le SD-WAN Zero Trust

Le SD-WAN Zero Trust fait appel à une appliance physique ou virtuelle active au niveau du site distant, du campus ou d'une usine, pour gérer les connexions des FAI et transférer le trafic vers Zero Trust Exchange, en fonction des politiques en vigueur. Le trafic des sites distants est relayé en toute sécurité via des connexions DTLS temporaires vers Zero Trust Exchange, où il peut être inspecté pour détecter les cybermenaces et les fuites de données à l'aide de politiques de sécurité qui prennent en compte les éléments de contexte.

Zero Trust Exchange facilite la communication bidirectionnelle entre les dispositifs et les applications Internet ou privées hébergées sur d'autres sites, dans des data centers ou dans le cloud.

Par exemple, un serveur d'impression présent dans un data center peut envoyer, via Zero Trust Exchange, des tâches d'impression à une imprimante située sur un site distant, sans que cette requête ne transite par un réseau routé, un VPN ou des ports potentiellement vulnérables. Le trafic des applications de confiance peut être acheminé directement via Internet grâce à un accès local direct à Internet.

Cette approche unique offre trois avantages majeurs :

- **Une entreprise mieux sécurisée :** les ransomwares ne peuvent pas se déplacer latéralement entre les sites ; les appareils infectés ne peuvent mener des scans de reconnaissance que sur le périmètre restreint de leur réseau local
- **Simplicité et maîtrise des coûts sur les sites distants :** les couches overlay de routage, les pare-feu ou les VPN de site à site ne sont plus nécessaires.
- **Meilleure expérience utilisateur :** les applications sont plus rapides, sans backhauling du trafic et sans congestion au niveau des points d'inspection de sécurité.

Cas d'utilisation de Zero Trust SD-WAN

- **Remplacement du VPN :** éliminez la complexité liée aux VPN site à site et aux réseaux overlay grâce à une solution Zero Trust plus simple et mieux sécurisée.
- **Mise à niveau du SD-WAN :** simplifiez la connectivité sur les sites distants et maîtrisez les risques liés aux ransomwares.
- **Fusions et acquisitions :** intégrez les utilisateurs et les applications sans la complexité et le coût liés à l'intégration des réseaux.
- **Usines sécurisées :** éliminez le déplacement latéral de menaces entre les usines et sécurisez les environnements IT/OT.

Modèles matériels et logiciels de Branch Connector

CARACTÉRISTIQUES	ZT 400	ZT 600	ZT 800	ZT VM
				Zscaler Edge
Type	Site distant petit à moyen	Site distant petit à moyen	Site distant moyen à grand	Sites distants et data center
Performances avec chiffrement	200 Mbit/s	500 Mbit/s	1 Gbit/s	Variable
Ports physiques	4 x RJ45 GbE	6 x RJ45 GbE	6 x RJ45 GbE, 2x SFP	N/A
Provisioning automatisé	✓	✓	✓	N/A
Mode passerelle avec sélection du chemin en fonction de l'application	✓	✓	✓	N/A
Politiques de transfert granulaires	✓	✓	✓	✓
Politiques de protection des données et contre les menaces pour le trafic Internet	✓	✓	✓	✓
Accès privé sécurisé pour les dispositifs IoT/OT	✓	✓	✓	✓

TABLEAU 1 : FONCTIONNALITÉS DE ZSCALER ZERO TRUST SD-WAN	
FONCTIONNALITÉS	**DESCRIPTION**
Fonctionnalités	
Provisioning et déploiement automatisés	• Provisioning automatisé grâce à des modèles prédéfinis • Déploiement entièrement automatisé • Identification dynamique des sites distants par géolocalisation
Politique de transfert granulaire pour le trafic Internet et celui des applications privées	• Options d'acheminement du trafic vers ZIA, ZPA ou Direct (contournement des services Zscaler) • Critères flexibles de sélection du trafic : emplacement, sous-emplacement, groupe d'emplacements, 5 tuples ou FQDN
Politiques unifiées de Zero Trust	• Politique unifiée pour les liens "utilisateur à application", "dispositif IoT à application" et "serveur à serveur", grâce à la politique de ZPA capable de prendre en charge de nouveaux types de clients • Politiques basées sur le lieu et la géolocalisation • Activation de politiques de sécurité incluant l'IPS, le proxy SSL, le filtrage d'URL et la protection des données • Stack de sécurité complet avec posture configurée pour l'IoT/OT et les serveurs AD
Haute disponibilité	• Basculement automatique avec redondance N+2 qui assure la continuité de service • Deux instances de Branch Connector pour prendre en charge les pics de trafic et assurer la redondance en cas de défaillance matérielle • Un équilibreur de charge configuré pour une tolérance de panne en mode actif-passif utilisant une adresse IP virtuelle (VIP) basée sur le protocole CARP (Common Address Redundancy Protocol)
Visibilité centralisée et mise en log granulaire	• Tableau de bord centralisé pour surveiller l'intégrité des appareils et du trafic • Filtrage disponible pour les environnements cloud, les data centers et les sites distants • Mis en log détaillée de chaque session et transaction pour tous les ports et protocoles, y compris les transactions DNS publiques et privées • Intégration complète avec l'infrastructure NSS : une machine virtuelle de pare-feu NSS peut être utilisée pour transmettre les logs vers le SIEM
Terminaison de l'interface WAN	• Connectivité double pour FAI (Ethernet) • Connectivité multiple (multi-homing) avec une seule appliance
Gestion de l'interface LAN	• Réseaux LAN L3 multiples • Prise en charge du tagging 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 • Listes de contrôle d'accès (ACL) L3/L4
Sélection du chemin d'accès en fonction de l'application	• Sélection dynamique du chemin d'accès pour les applications SaaS ou privées critiques • Connectivité intelligente via les POP de Zscaler • Monitoring des SLA et failover
Routage	• Routage statique
Data centers/PoP Zscaler	• La plateforme de sécurité cloud de Zscaler s'adosse à plus de 150 data centers dans le monde, stratégiquement positionnés au plus près des clients • Haute-disponibilité avec basculement transparent vers un autre service PoP disponible

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation digitale de ses clients pour qu'ils gagnent en agilité, efficacité, 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 appareils et les applications, quelle que soit leur localisation. Adossée à plus de 150 data centers dans le monde, Zero Trust Exchange est la plus vaste plateforme cloud de sécurité et SSE active en mode inline. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur Twitter**@zscaler**.

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