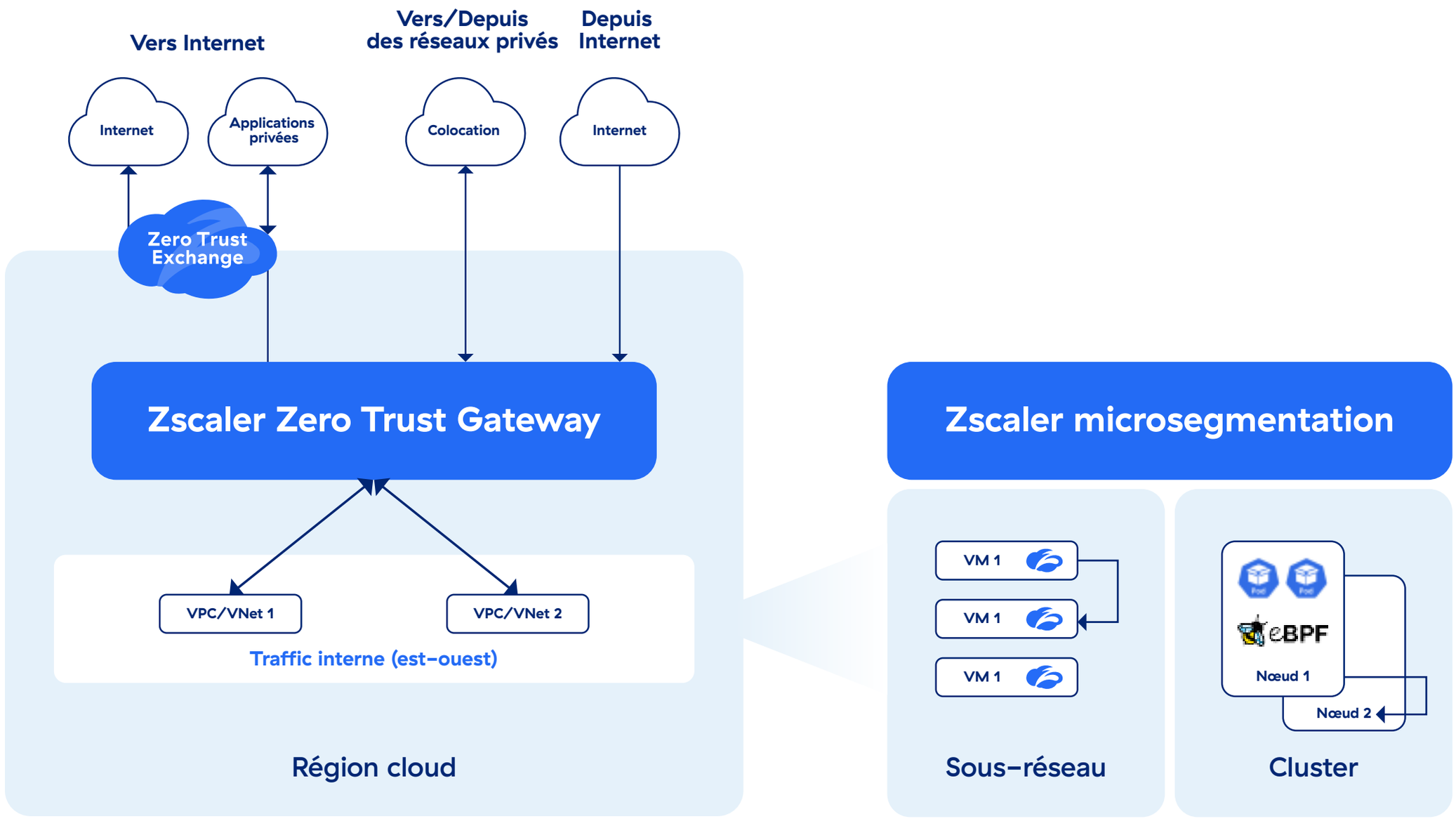
Zero Trust Cloud

Le moyen le plus simple de connecter et de sécuriser les workloads sur n'importe quel cloud

FICHE TECHNIQUE

L'ère du multicloud, impulsée par la transformation numérique, entraîne une explosion des workloads. Pour réussir, votre entreprise doit avoir une visibilité sur ces ressources clés tout en prévenant les cyberattaques et les pertes de données.

Les solutions de sécurité traditionnelles telles que les pare-feu réseau et les VPN IPSec reposent sur des architectures obsolètes présentant des failles inhérentes. Elles ne permettent pas une visibilité sur les actifs en temps réel, offrent une protection incohérente, élargissent la surface d'attaque et permettent les déplacements latéraux. Cela accroît inévitablement la complexité opérationnelle et les coûts.



Sécuriser tous les chemins de trafic grâce à la technologie Zero Trust Gateway/Connector et Zscaler Microsegmentation

Zero Trust Cloud étend la sécurité complète à votre environnement multicloud. Grâce à une visibilité en temps réel, cette solution génère des métadonnées instantanées et des informations au niveau des processus, fournissant un inventaire précis des actifs. Bénéficiez d'une protection homogène des données et contre les menaces sur l'ensemble des chemins de trafic et des clouds, et réduisez vos coûts opérationnels grâce à une plateforme unique. Pour assurer la visibilité et le contrôle des microflux provenant d'une machine virtuelle ou d'un conteneur, cette solution propose une microsegmentation intelligente basée sur l'hôte.

Étendre l'architecture Zero Trust à un environnement multicloud

Avec Zero Trust Cloud, vous pouvez :

OBTENIR UNE VISIBILITÉ EN TEMPS RÉEL SUR LES RESSOURCES CLOUD

Obtenir une visibilité en temps réel sur vos ressources cloud avec Zero Trust Cloud

- **Capture instantanée des métadonnées :** la solution s'intègre parfaitement à l'infrastructure cloud pour collecter automatiquement les métadonnées cloud (balises, étiquettes, attributs) lors de la création, de la modification ou de la suppression d'une ressource.

- **Analyse approfondie des processus :** les agents de microsegmentation Zscaler fournissent des métadonnées granulaires au niveau des processus provenant des environnements de machines virtuelles et de conteneurs.

- **Inventaire précis des actifs :** la solution fournit un inventaire détaillé et précis au niveau régional des VPC/VNet, sous-réseaux et VM/EC2 sans aucune intervention manuelle.

ACQUÉRIR UNE PROTECTION COHÉRENTE ET COMPLÈTE DES DONNÉES ET CONTRE LES MENACES

Appliquer des politiques de sécurité uniformes dans un environnement multicloud

- **Sécurisez tous les chemins de trafic,** y compris le trafic entrant et sortant, le trafic interne (est-ouest), le trafic du réseau privé et les microflux.

- **Prévenez les attaques de type « zero day »** grâce à une inspection TLS et à une protection contre les menaces adaptées au cloud.

- **Empêchez les fuites de données** grâce à la protection des données intégrée.

RÉDUIRE LES COÛTS OPÉRATIONNELS ET LA COMPLEXITÉ

Utiliser une plateforme de sécurité unique pour protéger les workloads dans vos clouds

- **Sécurisez les workloads** sur les principaux fournisseurs de services cloud, notamment AWS, Azure et GCP, à l'aide d'une plateforme unifiée.

- **Automatisez les déploiements de sécurité** via des interfaces programmables, notamment les API Zscaler, Hashicorp Terraform et AWS CloudFormation.

- **Prenez en charge les connexions de cloud à cloud**, de cloud au data center, de région à région, de VPC/VNet à VPC/VNet et de sous-réseau à sous-réseau.

SÉCURISER LES APPLICATIONS CRITIQUES

Répondez aux exigences réglementaires et de conformité, et renforcez la sécurité des workloads grâce à la microsegmentation basée sur l'hôte.

- **Visibilité au niveau des processus :** obtenez une connaissance approfondie des ressources cloud au niveau de chaque processus.
- **Regroupement automatisé des ressources :** exploitez l'apprentissage automatique pour recommander et définir automatiquement des segments de ressources optimaux en fonction de l'analyse du flux de trafic.
- **Application stricte du principe du moindre privilège :** appliquez des règles de sécurité granulaires par segment, en n'accordant que l'accès essentiel et en limitant les déplacements latéraux potentiels.

Fonctionnalités de Zero Trust Gateway/Connector

EDITION	DESCRIPTION
Advanced	• Inspection TLS/SSL • Pare-feu cloud (version Standard) • Protection contre les menaces avancées • Flux de journaux NSS (pas de récupération de journaux) • Diffusion en continu de cloud à cloud • DNS Essentials • Contrôle des fichiers • Politique de sécurité et d'accès dynamique basée sur les risques • Sécurité SaaS (norme CASB) • Segmentation workload à workload (ZPA) • Identification des applications (ZPA) • Protection des données (mode moniteur) • Ancrage IP source Zscaler
Advanced Plus	• Toutes les fonctionnalités disponibles dans la version Advanced • Protection des workloads vers Internet • IPS, protection des données • Flux de journaux NSS (avec récupération des journaux) • DNS avancé (Advanced) • Cloud Sandbox (version Advanced) • Certificat racine personnalisé • Sécurité du SaaS • Pare-feu cloud (version Advanced) • Protection des données (inline) • Exact Data Match (EDM) • Correspondance de documents indexés (IDM) • Reconnaissance optique de caractères (OCR)

Fonctionnalités de Zscaler Microsegmentation

EDITION	DESCRIPTION
Advanced	• Plateformes prises en charge : Windows, Linux et Kubernetes (Amazon EKS) • Visibilité sur les workloads cloud (AWS, Azure, GCP) • Visibilité sur le flux de trafic, y compris les détails de l'application • Cartes de dépendances des applications • Mise en oeuvre des politiques • Zones applicatives pour les périmètres de politique avancés • Mises à niveau d'agent intégrées utilisant des profils de version • Analyse de flux avancée • Intégration avec le SIEM via le service de diffusion de journaux (LSS) • Service d'identification de workloads, intégration de Zero Trust Gateway /Connector pour une visibilité en temps réel des métadonnées multicloud

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 160 data centers dans le monde, Zero Trust Exchange™, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

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

zscaler™

Zero Trust Everywhere