FICHE TECHNIQUE

Zscaler Microsegmentation

Les défis liés de la microsegmentation traditionnelle

De nombreuses entreprises font appel à des architectures de segmentation traditionnelles pour sécuriser leurs instances. Ces architectures présentent néanmoins des lacunes : leur déploiement est complexe, elles élargissent la surface d'attaque, permettent les déplacements latéraux et creusent les coûts opérationnels.

- Dresser un inventaire précis des ressources constitue un défi, en particulier pour celles dans le cloud qui sont activées et supprimées de manière dynamique.
- Des solutions telles que les pare-feu étendent le réseau aux instances et aux serveurs, ce qui favorise le déplacement latéral.
- Un mix d'appliances virtuelles, d'outils opérationnels et de politiques non standardisées introduit des vulnérabilités, connues et inconnues, dans la couverture de sécurité, ce qui accroît les risques.
- Le déploiement d'outils de segmentation tiers personnalisés est complexe tandis que l'application des politiques de sécurité n'est pas toujours cohérente sur l'ensemble du périmètre d'une entreprise.

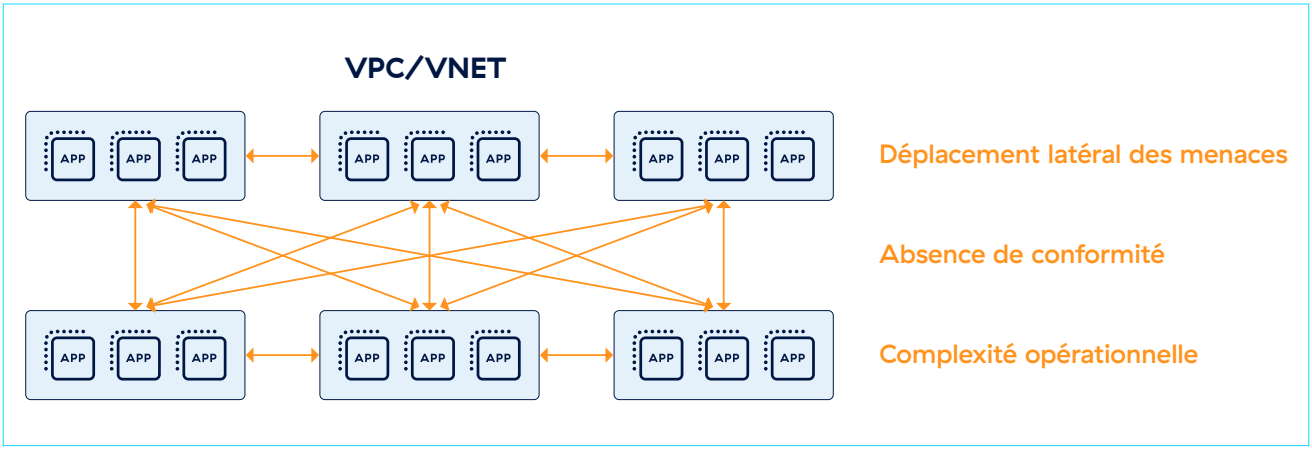

Illustration 1 : Les architectures traditionnelles de protection des instances ne sont pas conçues pour stopper le déplacement latéral des menaces

Le Zero Trust pour segmenter les environnements de cloud public et les data centers sur site

La microsegmentation au niveau des hôtes répond à ces défis, en dissociant le réseau en segments plus restreints et plus simples à gérer. Elle applique des règles de sécurité à chaque segment et ne valide que les accès essentiels. Ainsi, un seul segment compromis ne peut mettre en péril la totalité du réseau. Face à des cybermenaces de plus en plus sophistiquées, la ligne de défense classique, déployée en périphérie de réseau, ne parvient plus à déjouer les attaques sophistiquées.

Zscaler Microsegmentation fournit les fonctionnalités suivantes :

Identification et visibilité en temps réel sur les ressources : vous pouvez dresser rapidement l'inventaire des ressources de votre infrastructure.

- Identifiez les ressources en quasi temps réel. Obtenez un inventaire des ressources, à l'aide de balises définies par l'utilisateur, d'attributs de cloud (VPC/VNET) ou de caractéristiques réseau (IP/sous-réseau).
- Bénéficiez d'une visibilité sur les ressources hébergées dans tous vos clouds publics, data centers et environnements en colocations, à partir d'une seule console.

Recommandation automatisée de politique : la politique de sécurité s'applique à toutes les ressources.

- Tirez parti de recommandations en matière de politique pour segmenter les workflows sur la base d'une analyse des flux de trafic.
- Bénéficiez de suggestions proactives en matière de politique pour protéger les ressources qui ne sont pas segmentées.

Application granulaire de la politique : prévenez le déplacement latéral des menaces.

- Déployez un contrôle d'accès au niveau de l'hôte.
- Définissez une politique de sécurité cohérente pour toutes les ressources des data centers et des clouds publics.

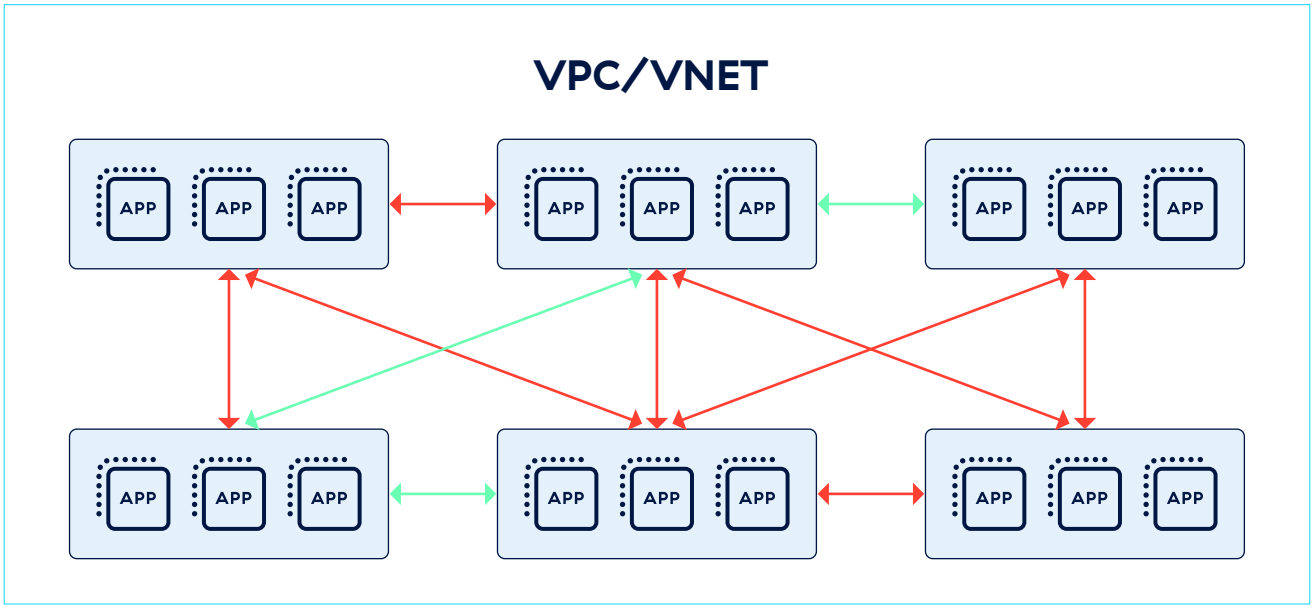

Illustration 2 : La microsegmentation de Zscaler offre une segmentation basée sur le Zero Trust et sur l'hôte

Fonctionnalités de microsegmentation de Zscaler

FONCTIONNALITÉS	DESCRIPTION
Prise en charge du cloud public et des environnements sur site	Sécurisez les instances dans AWS, Microsoft Azure. Les data centers sur site sont également protégés.
Inventaire des hôtes	Bénéficiez d'une visibilité sur vos instances cloud, notamment sur les hôtes, l'environnement cloud et les balises définies par l'utilisateur.
Inventaire des flux	Bénéficiez d'une visibilité granulaire sur les flux : informations détaillées sur les 5 tuples, nom des applications et chemin d'accès aux applications.
Cartographie des applications	Accédez à une carte interactive des flux entre les ressources applicatives au sein de l'environnement.
Politiques de ressources	Créez et appliquez des politiques entre vos ressources applicatives.
Zones applicatives	Contrôlez l'étendue des règles de la politique en fonction des zones applicatives ou des environnements.
Mises à jour simplifiées des agents	Mettez à niveau les agents de microsegmentation Zscaler par groupes, selon leur version.
Tableau de bord analytique	Bénéficiez de tableaux de bord analytiques qui identifient les les principales ressources en tant qu'émetteur ou récepteur de trafic, ainsi que leurs flux vers Internet, sur la base des logs de flux observés.
Compatibilité élargie aux plateformes	Des agents légers peuvent être installés sur les systèmes d'exploitation courants, Windows et Linux notamment.
Streaming de logs	Avec Zscaler Log Streaming Service, consolidez les logs de tous vos instances et serveurs, à l'échelle mondiale, au sein d'un référentiel central défini par votre entreprise. Les administrateurs peuvent afficher et analyser les données des logs de trafic des instances.

zscaler™ | Experience your world, secured.™

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 les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, 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 Twitter **@zscaler**.

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