Descriptif de la solution

Les 3 principaux avantages du SASE et comment en profiter

Pourquoi opter pour le Secure Access Service Edge (SASE) ?

Les modèles économiques du monde numérique moderne permettent de nouveaux niveaux d'engagement des clients et des employés en fournissant un accès mondialement disponible et cohérent aux applications et services, peu importe où les employés et les clients se connectent ou quels appareils ils utilisent.

La notion de sécurité des réseaux lorsque vos utilisateurs et vos applications sont disséminés n'est plus viable dans un monde numérique. Gartner a développé un nouveau modèle de mise en réseau et de sécurité qui correspond aux exigences de l'entreprise numérique, connu sous le nom de SASE (Secure Access Service Edge).

> « L'architecture SASE est importante. Idéalement, l'offre est cloud native, construite sur des microservices avec la possibilité d'évoluer selon les besoins. Pour minimiser la latence, les paquets doivent être copiés en mémoire, traités et transmis/bloqués, et non transmis de machine virtuelle (VM) à VM ou de cloud à cloud. La pile logicielle ne doit avoir aucune dépendance matérielle spécifique et être instanciée quand et où cela est nécessaire pour fournir à l'identité du terminal des capacités basées sur la politique et optimisées en fonction des risques. » **Gartner**[1]

#1 Réduction des coûts et de la complexité informatiques

Avec des données réparties entre les applications cloud et les services SaaS, et des utilisateurs travaillant souvent de n'importe où, le modèle de sécurité traditionnel basé sur le réseau a atteint ses limites. Pour compenser, les entreprises ont été obligées de déployer des services supplémentaires pour combler les lacunes au niveau de leur sécurité, tout en augmentant considérablement les coûts de déploiement, de gestion et d'exploitation avec une équipe qui ne se développe pas assez rapidement. Même avec cette augmentation des coûts et de la complexité, le modèle de sécurité réseau ne peut toujours pas évoluer, n'est pas agile et n'est tout simplement pas efficace dans un monde numérique.

Au lieu d'essayer d'utiliser un concept ancien pour résoudre un problème moderne, le SASE Zero Trust réinvente le modèle de sécurité. Alors que les approches traditionnelles se concentraient sur la création de périmètres autour des applications, le SASE se concentre sur les entités, telles que les utilisateurs qui accèdent aux applications, et rapproche la sécurité au plus près de cette entité. En tant que service cloud, le SASE autorise ou refuse de façon dynamique les connexions au service en fonction des règles définies par l'entreprise ou l'agence. Tout cela se fait par l'intermédiaire d'un service unique qui unifie un certain nombre de fonctions auparavant distinctes, telles que SWG, ZTNA, etc.

CE QU'IL FAUT RECHERCHER

La composante la plus importante d'une bonne offre SASE est l'architecture sur laquelle elle est construite. Gartner a précisé le type d'architecture nécessaire pour tenir les promesses du SASE. Plus important encore, elle doit être conçue dès le départ pour répondre à l'échelle requise pour un service de sécurité entièrement fourni dans le cloud.

Par conséquent, cette offre distribuée doit prendre en charge une architecture multi-entité, lui permettant d'évoluer globalement et de façon dynamique en fonction de la demande. Elle doit s'éloigner des concepts traditionnels de mise en réseau de politiques et de couches de politique et se fonder plutôt sur la politique de l'entreprise. Enfin, cette architecture doit prendre en charge une plateforme véritablement intégrée avec une gestion unifiée fournie dans le cloud.

CE QU'IL FAUT ÉVITER

Gartner met spécifiquement en garde contre les approches traditionnelles de sécurité réseau qui utilisent des offres basées sur des machines virtuelles exécutées dans les infrastructures des fournisseurs de cloud. L'utilisation de ces approches basées sur les machines virtuelles dans un environnement informatique IaaS aura des difficultés à évoluer et fournira une expérience utilisateur incohérente en raison de goulots d'étranglement (« hairpinning ») entre les fournisseurs de cloud et les applications auxquelles accèdent les utilisateurs.

Ce modèle repose sur une architecture à entité unique qui tente d'utiliser des politiques d'accès basées sur le réseau dans un modèle SASE basé sur l'accès de l'utilisateur, ce qui crée des déploiements beaucoup plus complexes qui ne correspondent pas à un modèle SASE. En outre, ces approches sont souvent basées sur de nombreux produits qui ne sont pas vraiment intégrés mais plutôt assemblés via une interface utilisateur superposée de services indépendants, souvent achetés par le biais d'acquisitions.

« Le SASE (Secure Access Service Edge) est une offre émergente qui combine des capacités WAN complètes et des fonctions de sécurité réseau complètes (telles que SWG, CASB, FWaaS et ZTNA) pour répondre aux besoins dynamiques d'accès sécurisé des entreprises numériques. » **Gartner**[1]

#2 Expérience utilisateur exceptionnelle

Ce n'est pas pour rien que le SASE se concentre principalement sur l'expérience utilisateur. Il était facile de contrôler et de prévoir l'expérience utilisateur lorsque les utilisateurs étaient sur le réseau, que les applications se trouvaient dans le data center, et que les serveurs et l'infrastructure étaient détenus et gérés par le service informatique. Maintenant que les applications sont réparties sur plusieurs clouds, la méthode d'accès à ces applications est toujours basée sur l'ancien modèle du VPN qui se connecte à un réseau par souci de sécurité. Ce modèle amène l'utilisateur à la sécurité et non la sécurité à l'utilisateur, ce qui est indispensable à une excellente expérience utilisateur. Le SASE Zero Trust impose que la sécurité soit appliquée au plus près des utilisateurs, en gérant intelligemment les connexions des utilisateurs aux points d'échange Internet et en optimisant les connexions directes (peering) aux applications et services cloud pour garantir une bande passante optimale et une faible latence.

CE QU'IL FAUT RECHERCHER

La clé pour d'une expérience utilisateur exceptionnelle consiste à fournir une bande passante optimale avec la plus faible latence possible. La seule façon d'y parvenir efficacement est de réduire le nombre de sauts nécessaires pour atteindre les applications et de veiller à ce que la bande passante appropriée est allouée grâce à des contrôles.

La bonne approche consiste à placer la pile de sécurité le plus près possible de l'utilisateur dans les échanges sur Internet à travers un déploiement géographique largement réparti. L'accès aux applications à partir de ces échanges nécessite la capacité d'acheminer intelligemment le trafic vers l'emplacement géographique le plus proche de l'application grâce à un peering direct.

CE QU'IL FAUT ÉVITER

Les offres basées sur des machines virtuelles exécutées auprès des fournisseurs de cloud ou IaaS nécessiteront un hairpinning du trafic. Il est spécifiquement décrit dans le document SASE que de telles offres ne peuvent pas être définies comme une solution SASE et doivent être évitées.

Cela est principalement dû au fait que les architectures basées sur des VM ne sont pas évolutives et ne contrôlent pas la connexion à partir de l'utilisateur, mais depuis l'environnement informatique de l'application, et ne peuvent par conséquent pas garantir une expérience utilisateur satisfaisante. En outre, ces offres ne peuvent pas évoluer de manière dynamique et nécessitent une planification de l'utilisation qui ne permet pas de modifications ultérieures sans programmer des temps d'arrêt.

« Les capacités de décision et d'application de la politique SASE doivent être présentes partout où se trouvent les identités des terminaux… Les offres SASE qui n'utilisent que la capacité du réseau backbone Internet de l'IaaS, mais sans les capacités locales/de périphérie des points de présence (PoP), encourent des risques de latence et de performances et, par conséquent, l'insatisfaction de l'utilisateur final. » **Gartner**[1]

#3 Réduction des risques

La sécurité est une question d'identification et de prévention des risques. Le SASE Zero Trust en tant que service cloud est conçu pour répondre aux défis uniques liés au risque de la nouvelle réalité d'utilisateurs et d'applications distribués géographiquement. En définissant la sécurité comme une fonction intégrée au cœur du modèle, et non comme une fonction distincte de la connectivité des services, la solution garantit que toutes les connexions sont inspectées et sécurisées, quel que soit l'endroit où les utilisateurs se connectent, les applications auxquelles ils accèdent ou le chiffrement éventuellement utilisé.

CE QU'IL FAUT RECHERCHER

La clé de la réduction des risques réside dans la capacité à abandonner les concepts de connectivité basée sur le réseau pour connecter les utilisateurs aux applications sur la base d'un véritable accès réseau Zero Trust (ZTNA). ZTNA garantit que seuls les utilisateurs autorisés à accéder à une application peuvent le faire, cette autorisation étant définie par le biais de politiques d'entreprise, et non par des définitions complexes de politiques multicouche.

Une autre façon dont une plateforme SASE réduit les risques consiste à supprimer la surface d'attaque. En cachant le réseau de l'entreprise et les identités de source sur Internet, SASE empêche les adversaires de vous cibler avec des attaques telles que DDoS.

Le modèle SASE est fourni via une architecture basée sur un proxy qui gère toutes les communications entre les utilisateurs et les applications. Cette architecture garantit que l'ensemble du trafic peut être déchiffré et inspecté, et fournit une visibilité complète. Enfin, l'architecture SASE est construite avec un contexte complet de données échangées entre les entités et les applications pour garantir que toutes les connexions répondent aux exigences de conformité et de gouvernance des données.

CE QU'IL FAUT ÉVITER

Les approches traditionnelles de sécurité du périmètre reposaient sur un modèle basé sur un pare-feu qui examinait les flux de paquets et déterminait les risques sur la base de l'inspection de ces flux. Bien que ce modèle fonctionne pour une sécurité basée sur le périmètre, il ne répond pas aux nouveaux défis d'un déploiement basé sur le SASE.

Le principal problème est qu'une architecture de pare-feu fonctionnant comme un service détermine les menaces après coup, ce qui leur permet d'atteindre leur destination avant d'être découvertes. La raison est simple : ces approches traditionnelles sont incapables de conserver les données et de déterminer leurs résultats avant de les envoyer. Cette limitation rend le déchiffrement des sessions et la protection des données exceptionnellement difficiles car il s'agit de fonctions qui exigent que le flux soit conservé et réassemblé, comme un proxy.

Avec un service de pare-feu, les fonctions de déchiffrement, d'inspection et de réassemblage nécessitent un processus séparé qui est distinct du service. Cela complique la politique, introduit une latence et entraîne de mauvaises performances, et se traduit souvent par une fonctionnalité limitée lors de la mise en œuvre. En outre, SASE nécessite une architecture à passage unique pour traiter tout le contenu en une seule fois. Les offres de pare-feu basées sur les flux exposent également l'adresse IP source du réseau hôte à de potentiels adversaires, ce qui revient à annoncer la surface d'attaque au profit d'attaques ciblées.

L'approche de Zscaler en matière de SASE

La plateforme de sécurité cloud de Zscaler optimisée par l'IA est un service SASE conçu dès le départ pour les performances et l'évolutivité. En tant que plateforme distribuée à l'échelle mondiale, Zscaler garantit aux utilisateurs un accès rapide à leurs applications ; grâce au peering avec des centaines de partenaires dans les principaux échanges Internet du monde entier, Zscaler offre des performances et une fiabilité optimales à vos utilisateurs, charges de travail, partenaires commerciaux et sites.

Le SASE Zero Trust de Zscaler s'appuie sur la plateforme SSE la plus éprouvée du secteur avec une nouvelle approche du SD-WAN. Aujourd'hui, plus de 30 % des entreprises du classement Forbes Global 2000 font confiance à Zscaler pour les mener en toute sécurité dans l'ère numérique.

La longue présence de Zscaler sur le marché a prouvé que son architecture était conçue pour évoluer, traitant actuellement plus de 360 milliards de transactions par jour et plus de 500 trillions de signaux quotidiens pour l'effet cloud IA/AA.

L'architecture SASE Zero Trust de Zscaler est fournie à travers plus 150 data centers répartis dans le monde, garantissant aux utilisateurs des connexions locales, rapides et sécurisées, peu importe où ils se connectent.

Pour en savoir plus sur l'approche SASE de Zscaler, rendez-vous sur
zscaler.fr/capabilities/secure-access-service-edge

[1] Gartner, Le futur de la sécurité des réseaux se trouve dans le cloud ; Lawrence Orans, Joe Skorupa, Neil MacDonald

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 appareils et les applications, indépendamment de l'emplacement. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SSE 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