Les 3 principaux avantages du SASE et comment en profiter

Pourquoi opter pour le secure access service edge (SASE)?

Les modèles modernes de commerce numérique 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 distribués n'est plus convaincante 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. Ils l'appellent secure access service edge (SASE).

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

AVANTAGE #1

Réduit les coûts et 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 organisations ont été obligées de déployer des services supplémentaires pour combler les lacunes 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, SASE réinvente le modèle de sécurité. Alors que les approches traditionnelles se concentraient sur la création de périmètres autour des applications, SASE se concentre sur les entités, telles que les utilisateurs, qui accèdent aux applications et rapproche la sécurité le plus près possible de cette entité. En tant que service cloud, SASE autorise ou refuse de façon dynamique les connexions au service en fonction des règles définies par une organisation. Tout cela se fait via un simple service qui unifie un certain nombre de fonctions auparavant distinctes telles que SWG, ZTNA, etc.

Ce qu'il faut rechercher

L'élément le plus important d'une grande offre SASE est l'architecture sur laquelle elle est construite. Gartner est précis sur le type d'architecture nécessaire pour tenir la promesse de SASE. Plus important encore, elle doit dès le départ être construite pour répondre à l'échelle requise pour un service de sécurité entièrement fourni dans le cloud.

Cela signifie qu'il doit s'agir d'une offre distribuée qui prend en charge la 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 des politiques et des couches de politique et se fonder plutôt sur la politique des entreprises. Enfin, cette architecture doit prendre en charge une plate-forme véritablement intégrée avec une gestion unifiée dans le cloud.

Ce qu'il faut éviter

Gartner, de manière spécifique, met en garde contre les approches traditionnelles de sécurité réseau qui utilisent des offres basées sur des machines virtuelles (VM) s'exécutant dans des infrastructures de fournisseur de cloud. L'utilisation de ces approches basées sur des VM dans un environnement informatique IaaS aura des difficultés à évoluer et fournira une expérience utilisateur incohérente en raison de l'épinglage nécessaire entre les fournisseurs de cloud et les applications auxquelles les utilisateurs ont accès.

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

> « 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 de backbone Internet de l'IaaS, mais sans les capacités locales des POP / périphériques, encourent des risques de latence, des problèmes de performance et d'insatisfaction des utilisateurs finaux. » **– Gartner**[1]

AVANTAGE #2

Offrir une expérience utilisateur exceptionnelle

Il y a une bonne raison pour laquelle SASE se concentre principalement sur 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, il était facile de contrôler et de prévoir l'expérience utilisateur. Maintenant que les applications sont réparties sur plusieurs cloud, votre méthode d'accès à ces applications est toujours basée sur l'ancien modèle d'un VPN se connectant à un réseau pour la sécurité. Ce modèle amène l'utilisateur à la sécurité et non la sécurité à l'utilisateur, ce qui est nécessaire pour une excellente expérience utilisateur. SASE demande 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 offrir une expérience utilisateur exceptionnelle se résume à fournir une bande passante optimale avec la plus faible latence. La seule façon d'y parvenir efficacement est de réduire le nombre de sauts pour atteindre les applications et de s'assurer que la bonne bande passante est allouée grâce à des contrôles de celle-ci.

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 VM fonctionnant auprès des fournisseurs de cloud ou IaaS nécessiteront l'épinglage trafic. De telles offres sont spécifiquement mentionnées dans le document SASE comme étant non qualifiées pour 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 depuis l'utilisateur, mais le font depuis l'environnement informatique de l'application et ne peuvent par conséquent pas garantir une bonne expérience utilisateur. En outre, ces offres ne peuvent pas s'étendre de manière dynamique et nécessitent une planification de l'utilisation qui ne permet pas de modifications ultérieures sans temps d'arrêt programmé.

> « L'architecture SASE est importante. Idéalement, l'offre est native du cloud, construite sur des micro-services avec la possibilité de s'étendre en fonction des besoins. Pour minimiser la latence, les paquets devraient être copiés dans la 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 doit être instanciée quand et où cela est nécessaire pour fournir à l'identité du terminal les capacités basées sur la politique et optimisées en fonction des risques ». **– Gartner**[1]

AVANTAGE #3

Réduit les risques

La sécurité est une question d'identification et de prévention des risques. SASE en tant que service cloud est conçu pour relever les défis uniques liés au risque dans la nouvelle réalité des utilisateurs et des applications si répandus. En définissant la sécurité comme une fonction intégrée dans le tissu même du modèle et non comme une fonction séparée de la connectivité des services, elle 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 tout chiffrement utilisé.

Ce qu'il faut rechercher

La clé de la réduction des risques est la possibilité d'abandonner les concepts de connectivité basée sur le réseau et de connecter plutôt les utilisateurs à des applications basées sur un véritable accès au réseau zero trust (ZTNA). ZTNA garantit que seuls les utilisateurs qui sont autorisés à accéder à une application peuvent le faire, et cette autorisation est définie par des politiques basées sur les entreprises et non par des définitions complexes de politiques à plusieurs niveaux.

Une autre façon dont une plate-forme 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 tout le trafic peut être décrypté et inspecté, et offre une visibilité complète. Enfin, l'architecture SASE est construite avec un contexte de données complet échangé 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 la sécurité du périmètre utilisaient un modèle basé sur un firewall qui examinait les flux de paquets et déterminait le risque en fonction de l'inspection de ces flux. Alors que ce modèle a fonctionné pour une sécurité basée sur un périmètre, il s'effondre avec les nouveaux défis d'un déploiement basé sur SASE.

Le principal problème est qu'une architecture de firewall 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 : ils 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 firewall, les fonctions de déchiffrement, d'inspection et de ré-assemblage nécessitent un processus séparé qui est découplé du service, ce qui complique la politique, introduit une latence et entraîne de mauvaises performances — et il permet souvent 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 firewall basées sur les flux exposent également l'adresse IP source du réseau hôte à de potentiels adversaires, annonçant efficacement leur surface d'attaque, ce qui peut conduire à des attaques ciblées.

> « De nombreuses fonctionnalités de SASE utiliseront un modèle de proxy pour accéder au chemin des données et sécuriser l'accès. Les anciens fournisseurs de réseaux en ligne et de firewall d'entreprise n'ont pas l'expertise nécessaire pour construire des proxies distribués en ligne à l'échelle, ce qui risque d'entraîner des coûts plus élevés et/ou des performances médiocres pour les utilisateurs de SASE. » **– Gartner**[1]

L'approche de Zscaler en matière de SASE

La plate-forme de sécurité cloud de Zscaler est un service SASE conçu de la base au sommet pour la performance et l'évolutivité. En tant que plate-forme distribuée à l'échelle mondiale, les utilisateurs sont toujours à un clique de leurs applications et, en s'appuyant sur des centaines de partenaires dans les principaux échanges Internet à travers le monde, Zscaler garantit à vos utilisateurs une performance et une fiabilité optimales.

Zscaler, créé il y a plus d'une décennie, bâtit sa plate-forme sur le même principe que SASE. Aujourd'hui, plus de 400 des organisations Forbes Global 2000 font confiance à Zscaler pour les conduire en toute sécurité dans l'ère numérique.

Grâce à son expérience sur le marché, Zscaler a prouvé que son architecture a été conçue pour évoluer, traitant actuellement jusqu'à 80 milliards de transactions aux périodes de pointe et effectuant au quotidien 120 000 mises à jour uniques de sécurité.

L'architecture SASE de Zscaler est fournie à travers 150 data centers à l'échelle mondiale, garantissant aux utilisateurs des connexions locales, rapides et sécurisées peu importe où ils se connectent.

En savoir plus

Pour en savoir plus sur SASE, rendez-vous sur **zscaler.com/gartner-secure-access-service-edge-sase** et lisez ce que Gartner a à dire sur l'avenir de la sécurité réseau.

Pour en savoir plus sur l'approche de Zscaler en matière de SASE, rendez-vous sur **zscaler.com/products/secure-access-service-edge**.

1. Gartner, L'avenir de la sécurité réseau se trouve dans le cloud ; 30 août 2019 ; Lawrence Orans, Joe Skorupa, Neil MacDonald

À propos de Zscaler

Zscaler permet aux entreprises de transformer en toute sécurité leurs réseaux et leurs applications pour s'adapter à la prédominance mobile et cloud du monde actuel. Zscaler connecte les utilisateurs aux applications et aux services cloud, quels que soient le périphérique utilisé, l'emplacement de l'utilisateur ou le type de réseau, tout en offrant une sécurité sans faille et une rapide expérience utilisateur. Et le tout, sans appliances de passerelle complexes et coûteuses.

zscaler™