Une intégration réseau et sécurité maximale pour l'adoption du SASE

Les réseaux des entreprises et la cybersécurité sont de plus en plus intégrés, et cette tendance a des avantages majeurs pour les équipes IT. En répondant au besoin critique de transporter de façon fiable et rapide le trafic des applications et des clients, cette intégration va en outre s'accélérer avec le Secure Access Service Edge (SASE). Celui-ci n'est pas une technologie particulière, mais plutôt la description d'une plus forte communion des services réseaux et sécurité pour les appareils connectés à la périphérie. De plus, cette infrastructure est hébergée sur le cloud et peut inclure une variété de fonctions réseau mais aussi de sécurité.

Le SASE suit le chemin du réseau étendu défini par logiciel (SD-WAN), qui, d'après Gartner, devrait être mis en œuvre par 60 % des entreprises d'ici 2024. Le SD-WAN est populaire car il adopte un concept simple : faciliter la vie des équipes IT, en leur permettant de gérer leurs réseaux sur le cloud via une plateforme edge centralisée. Grâce à ses fonctions d'automatisation et d'orchestration, il sera d'ailleurs en mesure de faire de même pour les fonctions SASE.

La plateforme SD-WAN fournira, en effet, aux responsables de l'infrastructure une appliance plus simple d'utilisation et définie par logiciel pour des services de sécurité et de réseau intégrés, tous gérés de manière centralisée par le cloud.

Toutefois, la volonté d'accélérer la transformation numérique et d'adopter les services cloud ne change pas seulement la mise en réseau, mais aussi la sécurité. Avec le SD-WAN, les clients passent de WAN centrés sur le datacenter et connectés en MPLS, à des réseaux étendus centrés sur le cloud qui exploitent pleinement Internet.

Désormais, les clients demandent à tirer parti d'une plateforme edge, afin de quitter un modèle de sécurité traditionnel en périphérie et d'adopter une approche SASE. Ainsi, une plateforme WAN zero-trust sur site peut compléter les services de sécurité fournis dans le cloud par n'importe quel fournisseur, toutes les politiques de sécurité étant contrôlées via un seul orchestrateur.

Le SD-WAN, la fondation du SASE

Le réseau étendu défini par logiciel devient aujourd'hui une plateforme programmable sur le cloud pour la sécurité et les composants du SASE. Il est, de ce fait, le « couteau suisse » de l'edge d'une entreprise. Avec l'explosion des terminaux et des services cloud, les équipes IT sont submergés par le nombre d'outils de sécurité et d'alerte qu'ils doivent gérer. En parallèle, ces employés désirent la liberté d'investir à la fois dans des technologies – réseau et sécurité – qui s'adaptent le mieux possible à leurs besoins changeants. C'est pour cette raison qu'il est nécessaire de combiner les efforts et d'ajouter de l'automatisation et de l'intégration à ces deux domaines en même temps.

Il n'y a en effet aucune raison pour que la sécurité soit séparée du réseau. Ce dernier transporte toutes les données connectées aux applications cloud, il représente donc une ressource riche pour de l'analyse et des corrélations. Avec cette approche moderne, les solutions de sécurité peuvent

être déployées dans le réseau directement afin de détecter et répondre aux anomalies présentes.

De ce fait, le SASE soutenu par le SD-WAN permet d'offrir tous les avantages induis par l'adoption d'un WAN défini par logiciel : une sécurité améliorée, une meilleure gestion / agilité, une bande passante optimisée, des économies et une performance optimale des applications cloud.

L'association des meilleures technologies possibles

L'un des plus grands avantages de la convergence du SASE et du SD-WAN est la liberté de choix des organisations pour l'adoption de leur solution de sécurité. Elles peuvent en effet intégrer n'importe quelle solution populaire dans leur SD-WAN.

En adoptant une plateforme edge de SD-WAN, les utilisateurs finaux peuvent organiser, orchestrer, et manager leur logiciel de sécurité cloud tiers, puisqu'il est directement intégré dans le processus de distribution du réseau. Cela permet de gagner un temps précieux en configuration et en gestion des règles de sécurité, tout en étendant les options permises par la prise en compte la sécurité comme un service délivré par le cloud.

En outre, les nouvelles solutions de sécurité hébergées sur le cloud sont en pleine expansion, et les architectures SaaS facilitent l'intégration et le déploiement des applications de sécurité tierces grâce à l'orchestration permise par le SD-WAN.

Certaines fonctionnalités SaaS peuvent être rapidement adoptées dans une architecture SD-WAN ; comme les courtiers de sécurité d'accès au cloud (CASB), la passerelle Web sécurisée (SWG), le FWaaS (Firewall as a Service) et l'accès zero-trust au réseau (ZTNA) – également appelés logiciels Périmètre défini (SDP).

Cet écosystème permet donc aux entreprises de développer l'innovation, en utilisant les meilleurs composants SASE, tout en consolidant leurs couches de gestion et d'orchestration au niveau du réseau. Le marché SASE se développe déjà rapidement, grâce à des alliances technologiques, et devrait atténuer les problèmes d'interopérabilité à mesure que les programmes de test et de certification des partenaires arrivent sur le marché.

Certains fournisseurs ont déjà étendu leurs capacités d'orchestration pour intégrer des services de sécurité cloud, permettant aux entreprises d'automatiser des politiques de sécurité cohérentes à l'échelle du réseau. De ce fait, l'architecture combine les avantages d'une périphérie WAN Zero-Trust avancée sur site avec une sécurité fournie par le cloud du fournisseur de leur choix.
Une chose est certaine : on n'a pas fini d'entendre parler du SASE !