SASE : allier le meilleur du réseau et de la sécurité

Avec le télétravail, les cyberattaques réussies visant le cloud ont redoublé, montrant le manque de préparation des entreprises en matière de sécurité. Pourtant, il y a déjà plus d'un an, Gartner publiait un rapport sur la stratégie à adopter par les organisations afin de protéger leur cloud, et inventait à cette occasion un terme : le SASE (Service d'Accès Sécurisé Edge).

Ce dernier décrit le besoin de combiner transformation réseau et sécurité en périphérie ; pour permettre aux entreprises de réaliser tous les bénéfices induits par une migration des applications et des workloads sur le cloud, tout en évitant les vulnérabilités induites.

Pour construire une architecture SASE, une entreprise doit tout d'abord commencer la transformation de son réseau étendu (WAN) et de sa sécurité, avec pour objectif final de fournir une stratégie globale sur ces deux aspects. En effet, les réseaux et l'architecture de sécurité traditionnels basés sur les routeurs et les pare-feux dirigent le trafic des applications cloud inutilement vers les datacenters pour les sécuriser. En effet, cela ajoute de la latence qui impacte négativement la performance des applications cloud.

A l'inverse, le SASE permet de repenser l'architecture réseau et de sécurité en dirigeant directement le trafic vers le cloud. Pour ce faire, il utilise internet et les services sécurisés du cloud, afin de limiter les délais induits par le trafic via les datacenters et pare-feux.

Transformation réseau

Le modèle SASE recommande une périphérie WAN simplifiée avec uniquement les fonctions réseau nécessaires. Idéalement, elle sera gérée via une plateforme qui unifie le SD-WAN, le routage, les pare-feux, une segmentation du réseau améliorée, une optimisation du réseau ainsi qu'une visibilité sur les applications et leur contrôle. C'est pourquoi, le SD-WAN continue d'être de plus en plus déployé par les organisations, notamment afin de transformer leur réseau en adéquation avec le modèle SASE.

Transformation de la sécurité

Lorsque les applications sont hébergées et accessibles partout et par n'importe quel appareil, ce qui est d'autant plus le cas avec le recours actuel au télétravail, les modèles de sécurité traditionnels doivent s'adapter. Gartner affirme ainsi que les services cloud de sécurité sont optimaux, et non pas dans des pare-feux complexes et difficiles à gérer. Il est en effet beaucoup plus facile de garder la détection des menaces à jour lorsqu'elle est centralisée dans le cloud.

Or, grâce à ses fonctionnalités permettant une priorisation des trafics, le SD-WAN remplace les routeurs. De ce fait, il permet de diriger directement les données vers le cloud grâce à l'évasion locale. En supprimant les routages inutiles vers les datacenters, les latences sont diminuées et, ainsi, les performances applicatives sont améliorées. Aussi, puisque les informations transitent

directement vers le cloud avec le SD-WAN, les services de sécurité internes suppriment le besoin de pare-feux dans les bureaux distants.

Ces derniers mois, de nombreux professionnels et experts ont affirmé que le SASE remplacerait le SD-WAN, et que la sécurité était la fonction principale de ce dernier. Ces incompréhensions ont conduit à de la confusion et nécessitent une clarification des objectifs du SASE. Ce dernier réside en une combinaison de SD-WAN et de services de sécurité hébergés sur le cloud ; le SD-WAN est donc une composante fondamentale de l'architecture SASE, mais n'est pas son seul composant.

Commencer la transition vers le SASE

Il est recommandé d'utiliser une plateforme de SD-WAN innovante, qui a fait ses preuves et comporte toutes les fonctions réseau recommandées par Gartner, afin d'offrir ensuite une architecture SASE solide.

Tout d'abord, le SD-WAN doit pouvoir identifier les applications dès le premier paquet et conduire les organisations à imposer une qualité de service et les règles de sécurité préétablies dans l'objectif commercial. Aussi, les applications cloud et les adresses TCP/IP doivent être mises à jour automatiquement et quotidiennement, pour permettre une évasion internet locale optimale, et en continu.

Le SASE nécessite en outre une orchestration automatique entre le SD-WAN et les services de sécurité cloud. De plus, une bascule automatique vers un second point de sécurité cloud est primordiale, si le premier n'est pas disponible, afin d'éviter une interruption applicative, mais aussi pour limiter les latences si un nouveau point plus proche des bureaux distants est déployé. La plateforme doit permettre aux entreprises d'adopter le SASE à leur propre rythme, et donner la possibilité d'adopter de nouveaux services de sécurité dès qu'ils sont disponibles.

Enfin, il est clé que les entreprises partenaires puissent facilement évaluer et intégrer n'importe quel service de sécurité si besoin. En effet, la plupart des déploiements de SASE requièrent actuellement deux fournisseurs, respectivement pour le SD-WAN et la sécurité. Ces déploiements duals, qui permettent de nombreuses intégrations complémentaires, sont fonctionnels et éliminent le besoin de mettre en place un pare-feu dans les bureaux distants.

Si une entreprise veut implémenter une architecture SASE, elle peut facilement le faire dès aujourd'hui en déployant une solution qui combine un SD-WAN et un service de sécurité situé sur le cloud. Par conséquent, en dirigeant le trafic directement vers le cloud, le SD-WAN permet d'éviter les latences liées à des routages inutiles vers les datacenters. Ainsi, la performance de chaque application hébergée sur le cloud sera optimale.