Un SD-WAN adapté pour une meilleure intégration des services managés

Aujourd'hui, le Secure Access Service Edge (SASE) est au cœur des stratégies informatiques de nombreuses entreprises. Ce modèle est un cadre architectural, conçu par Gartner, qui décrit la transformation des technologies de réseau étendu (WAN) et de sécurité traditionnelles en une périphérie unique gérée dans le cloud. Cette dernière prend par conséquent en charge les besoins d'accès sécurisé dynamique des entreprises digitalisées. L'occasion de définir et formaliser une offre de SASE se présente donc aux fournisseurs de services managés (MSP).

Les MSP pourraient ainsi distribuer des services d'infogérance pour répondre à la demande de réseau intégré et d'évolution de la sécurité. En effet, les directeurs informatiques préfèrent souvent souscrire à une infrastructure clé en main plutôt que d'élaborer seul leur WAN ou leur sécurité. Les fournisseurs de services conçoivent des offres alliant un service de sécurité managé clés en main et un réseau étendu défini par logiciel (SD-WAN) entièrement géré.
Pour ce faire, de nombreux MSP choisissent la meilleure sécurité réseau disponible sur le marché et font de même avec les technologies SD-WAN.

SD-WAN managé et services de sécurité

Une entreprise peut vouloir un service entièrement managé, où le fournisseur s'occupe de tout : le déploiement, la gestion, la surveillance ou la résolution des incidents. A l'inverse, il est possible de préférer une cogestion, qui permet de conserver certaines capacités en libre accès ; comme changer les règles des firewalls, ajouter de nouvelles applications SaaS, configurer la politique d'objectif commercial ou mettre à jour la liste des proxys autorisés.

Qu'elle soit entièrement, partiellement ou pas du tout managé, il est important d'examiner attentivement les accords de niveau de service (SLA) de chaque nouvelle offre de SASE en infogérance. En effet, il est impératif de savoir les solutions mises en place lorsqu'un problème survient, puisqu'il arrive toujours ; mais également si le fournisseur aide à développer et à implémenter les règles de sécurité, et s'il prendra en charge de potentielles futures applications SaaS à travers tous les sites du réseau.

Seulement, tous les MSP n'ont pas la volonté d'aider les organisations à engager leur transformation de sécurité et réseau sur le long terme. Les résultats d'infogérance SASE se révèlent en outre parfois décevants, comparés aux promesses précédant le déploiement.

Par exemple, les solutions SASE « tout en un » induisent souvent une offre SD-WAN et sécurité unique, et donc des compromis à effectuer. Cela signifie se contenter d'un minimum, en termes de réseau ou de sécurité, pour implémenter l'architecture SASE.

La convergence du SD-WAN, des MSP et du SASE

Il est nécessaire en effet que les MSP repensent leurs structures organisationnelles en silo, afin de pouvoir fournir un réseau intégré et des services de sécurité à leurs entreprises clientes, ce qui est le fondement du SASE. Pour ce faire, ils doivent collaborer étroitement avec leurs partenaires réseau et sécurité, pour tirer profit des interfaces de programmation d'application (API) ouvertes, de l'automatisation, de l'intégration de l'approvisionnement/déploiement et du service chaining.

Les fournisseurs d'infogérance simplifient par conséquent l'intégration des services et un éventuel passage au SASE. Cette nouvelle structuration permet aussi aux entreprises de sélectionner en toute simplicité son réseau étendu préféré ainsi que le fournisseur de sécurité, en adéquation avec ses objectifs commerciaux.

Toutefois, pour réaliser la promesse d'une architecture SASE, une solution SD-WAN traditionnel, aux capacités Edge limitées, ne pourra simplement pas offrir la performance applicative et la qualité d'expérience nécessaires pour une migration complète vers le cloud. Les fournisseurs de services devraient donc s'associer avec un fournisseur de SD-WAN innovant, qui pourra délivrer les promesses d'une architecture SASE.

Pour ce faire, les capacités clés à prendre en compte sont variées et comprennent notamment l'identification et la classification des applications de premier paquet pour un pilotage automatique et granulaire du trafic ; mais aussi la définition quotidienne des applications et la mise à jour des tableaux d'adresse TCP/IP dans tous les sites présents sur le réseau.

De plus, la plateforme, dans un souci de performance optimale, doit basculer les connexions automatiquement vers un second point d'exécution, dès lors que le premier est indisponible, tout en ayant la possibilité de procéder à une reconfiguration sans intervention vers le point de connexion performant le plus proche. Finalement, il est indispensable que l'architecture SASE offre la possibilité d'adopter de nouvelles innovations de sécurité dès qu'elles émergent, afin d'optimiser là aussi la performance du réseau.

Les entreprises qui ont débuté leur évolution vers le SASE doivent donc s'assurer qu'elles conservent la « liberté de choix » pour sélectionner une plateforme SD-WAN avancée et ouverte et une cybersécurité optimale. Grâce à cette alliance, les organisations s'adapteront à l'évolution de leurs besoins applicatifs et à un paysage de menaces en constante mutation. In fine, cela leur permettra en outre de mettre en œuvre le SASE à leur propre rythme