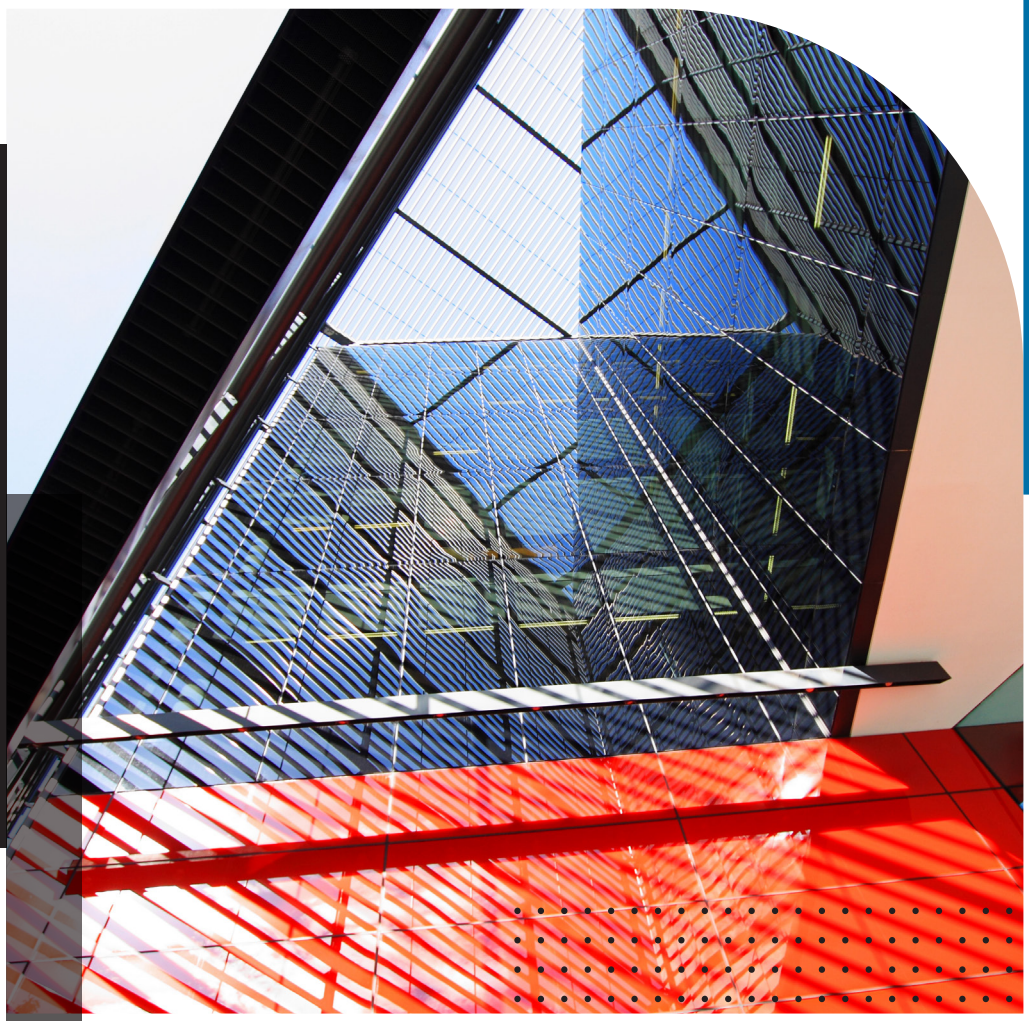
SD-WAN : Performances et Sécurité au Service des Organisations



Devenu incontournable pour accélérer la transformation numérique, le SD-WAN augmente toutefois la surface d'exposition aux risques. Une approche de sécurité «*by design*» est nécessaire pour assurer nativement la protection des données.

L'ACCÉLÉRATEUR DE LA TRANSFORMATION NUMÉRIQUE

Le SD-WAN est un formidable accélérateur de la transformation numérique. En apportant une couche d'abstraction sur l'infrastructure physique, la technologie des réseaux étendus programmables (Software-Defined Wide Area Network) permet de déterminer automatiquement l'itinéraire le plus pertinent pour acheminer le trafic réseau entre les différents datacenters et les sites à relier. En optimisant la bande passante et en offrant un temps de latence réduit et un taux de disponibilité élevé, le SD-WAN améliore l'expérience utilisateur, y compris sur les sites distants.

A l'heure de la généralisation du Cloud, le SD-WAN propose les meilleures performances en fonction du service à fournir. La téléphonie sur IP bénéficiera d'un très faible délai de latence et la sauvegarde en ligne un débit élevé pour ne pas monopoliser des ressources réseaux trop longtemps.

Les entreprises gagnent aussi en agilité et en résilience. La crise sanitaire a servi de révélateur avec le passage au télétravail massif. «*Lors du premier confinement, les organisations ont dû passer le VPN à l'échelle alors qu'il était jusqu'à présent utilisé par les 5 ou 10 % de télétravailleurs habituels*», observe **Christophe Auberger**, Evangéliste Cybersécurité, Fortinet France.

Face aux atouts du SD-WAN, un nombre croissant d'entreprises font appel à cette technologie qui remplace avantageusement l'infrastructure traditionnelle MPLS (MultiProtocol Label Switching), réseau privé de bout en bout mais aux performances limitées. Selon Gartner, 60 % des entreprises auront mis en œuvre le SD-WAN d'ici 2024 contre environ 30 % en 2020.

DU CHIFFREMENT À LA PRÉVENTION DES FUITES DE DONNÉES

Comme toute innovation, le SD-WAN a son revers. En faisant circuler les données sur des infrastructures publiques, il augmente la surface d'exposition aux risques d'une entreprise. «*Les frontières deviennent plus floues avec des données disséminées, en transit ou au repos, sur un poste de travail, un portable à domicile, un cloud public ou chez un éditeur en mode SaaS.*»

Pour **Christophe Auberger**, cet éclatement des données appelle à un changement de paradigme en termes de cybersécurité puisqu'il ne s'agit plus de défendre une zone de confiance à l'aide des traditionnelles protections périmétriques. «*La sécurité doit être prise en compte en même temps que les réseaux de connectivité sont déployés dans une approche de sécurité «by design». Une entreprise ne doit pas avoir à choisir entre sécurité et performances.*» Dans ce contexte, Fortinet, spécialiste mondial de la sécurité réseau, part avec un avantage certain pour développer nativement cette approche.

> *« Une approche de sécurité « by design » est nécessaire pour assurer nativement la protection des données »*

Un SD-WAN doit intégrer des fonctions de base comme un pare feu de dernière génération, un dispositif anti-intrusions et anti-malwares et une solution prévenant la fuite des données (Data Leak Prevention, DLP). Par ailleurs, le chiffrement par défaut des flux (IPSec) est obligatoire pour ne pas envoyer des données en clair sur une infrastructure publique.

«*L'intelligence d'un SD-WAN lui permet d'inspecter une appli suspecte et ne pas l'autoriser,* poursuit **Christophe Auberger**. *Il s'agit aussi d'appliquer différents niveaux de sécurité selon la criticité des données gérées par une application. Un dossier patient d'un établissement de santé sera ainsi jugé plus sensible qu'une application bureautique ne manipulant pas d'informations personnelles*».

BANQUE, SANTÉ, RETAIL… DES EXIGENCES FORTES EN TERMES DE SÉCURITÉ

Si tous les secteurs d'activité sont intéressés par le SD-WAN, certains, fortement régulés, ont des exigences particulièrement élevées en termes de sécurité et de protection des données personnelles. Au-delà du cadre général du RGPD, des normes spécifiques s'appliquent au domaine bancaire (PCI DSS) ou aux établissements de santé (HDS).

Les acteurs de la grande distribution doivent, eux, déployer des réseaux dans un très grand nombre de sites distants généralement dépourvus de compétences réseaux et sécurité. Le déploiement doit se faire en «*Zero Touch provisioning*». L'équipement est envoyé par La Poste et s'autoconfigure sans intervention humaine. Cela suppose donc qu'il intègre nativement toute la panoplie des outils de sécurisation des données.

Les collectivités locales, aux équipes IT parfois réduites, sont également concernées par cette approche. Le conseil départemental des Hauts de Seine fait ainsi appel à la solution Fortinet Secure SD-WAN pour répondre à l'ensemble de ses besoins réseaux qu'il s'agisse de sites de petite taille, comme la Protection Maternelle Infantile, des pôles sociaux multi-services ou encore des sites centraux. Elle permet aussi de fournir rapidement une liaison réseau sécurisée, via un VPN IPSec, aux agents administratifs qui interviennent sur des événementiels, tels que des festivals.

FORTINET®

www.fortinet.com/fr