C’est le bon moment pour penser au monde d’après le VPN

Beaucoup d’entre elles n’ont pas anticipé, lors des premières mesures de confinement, que l’affaire allait durer aussi longtemps. Il semblait donc acceptable de mettre en place des mesures provisoires, rapides à déployer (mais hélas pas toujours très sûres ou bien configurées). Surtout pour des entreprises où le télétravail était tabou.

Cela a fonctionné un moment : dans l’urgence, il est légitime de rester sur un modèle connu et maîtrisé (l’accès distant par VPN, en l’occurrence) et l’étendre, ici en ajoutant au plus vite des boîtiers ou des licences.

Oui, mais voilà : un boitier VPN supplémentaire, c’est entre 30 à 60 minutes de déploiement et de configuration pour une DSI déjà très sollicitée. Et c’est aussi un modèle qui date d’une époque où toutes les ressources nécessaires aux collaborateurs se trouvaient dans le *datacenter*, et où les utilisateurs du VPN étaient peu nombreux (essentiellement des forces commerciales et des cadres en déplacement).
Appliqué du jour au lendemain à l’ensemble des collaborateurs depuis leur domicile, le modèle ne tient plus : les coûts et les temps de déploiement et d’administration explosent, et en prime les accès VPN, qui centralisent toutes les connexions vers le seul datacenter, deviennent alors souvent un point de ralentissement majeur.

Mais les VPN ont également montré leurs limites en matière de sécurité. Beaucoup d’entre eux présentent des vulnérabilités alors que les vols de certificats et clés privées se sont multipliés. Cette année plus que jamais avec l’explosion de l’utilisation de VPN, les attaquants ont en effet utilisé les faiblesses des VPN pour compromettre à distance de nombreux systèmes d’informations en réutilisant à l’insu des entreprises des identifiants légitimes dérobés ou en exploitant des vulnérabilités des équipements VPN. Ces pratiques ont conduit à de nombreuses infections par rançongiciel tout au long de l’année.

Le monde d’après

Il est temps de reconnaître que le mode de consommation des ressources de l’entreprise a déjà évolué depuis un certain temps : les applications auxquelles doivent accéder les collaborateurs sont de plus en plus souvent hors de l’entreprise, hébergées en mode SaaS dans le Cloud.
Pourtant, avec un VPN, les utilisateurs peuvent être dirigés d’abord dans le datacenter avant de ressortir vers leur application SaaS. D’un strict point de vue de la sécurité, cela présente bien entendu un intérêt (le trafic peut être contrôlé, protégé et journalisé), mais en termes d’optimisation des performances, ce n’est pas du tout efficace.

Les entreprises doivent aujourd’hui réfléchir très sérieusement à adapter leur modèle d’accès distant afin de prendre en compte, de manière industrialisée, ces deux forces telluriques : une cohabitation définitive entre des applications sur site et d’autres dans le Cloud, et une force de travail massivement à l’extérieur des bureaux… et probablement pour longtemps !Dans les deux

cas, l'extension du modèle VPN historique ne fonctionne pas, et il faudra se tourner vers une autre approche, plus souple et plus moderne : les réseaux définis par logiciels (SD-WAN, pour « *software-defined Wide Area Network* »).
Entièrement Cloud, cette approche résout immédiatement la question du *provisionning* et de la montée en charge, puisqu'elle supprime l'obligation de déployer des équipements sur site, dans le datacenter. La création de nouveaux réseaux ou l'augmentation des capacités des réseaux existants sont prises en charge de manière centralisée, par le fournisseur, dans un sens comme dans l'autre (ajouter ou retirer des licences utilisateurs, en bénéficiant à tout moment de la bande passante et des ressources adaptées).

Nativement Cloud

Mais l'intérêt de cette approche ne s'arrête pas là. Nativement Cloud, elle permet de segmenter précisément les communications qui, depuis le poste de l'utilisateur, doivent être dirigées vers une application SaaS ou entrer dans le *datacenter*. Et cela, en conservant un point de contrôle centralisé capable de répondre aux besoins de filtrage, de contrôle et de conformité.
L'optimisation est alors totale, puisque seuls les flux réellement destinés aux applications *on-premise* sont dirigées vers le datacenter. Fini le goulet d'étranglement.

L'autre atout majeur du SD-WAN pour connecter les utilisateurs est sa capacité d'adaptation : la configuration du réseau, basée sur des tags et des politiques, peut être adaptée rapidement aux nouveaux besoins (un retour massif au bureau, un changement massif de zone géographique, un recours exclusif aux applications SaaS…). Les flux réseau sont tagués, groupés et priorisés selon les besoins, sans nécessiter d'adaptation ou de reconfiguration du matériel.

Il devient alors possible, par exemple, de privilégier les flux de visioconférence des forces commerciales, car ces dernières ont besoin de faire des présentations aux clients.
Un projet SD-WAN permettra ainsi de déployer des règles et des politiques granulaires pour tirer à tout moment le meilleur de la connectivité existante en fonction des priorités de l'entreprise.

Enfin, contrairement à une architecture VPN où le point d'accès est généralement unique, ce qui peut réduire les performances en fonction de la localisation géographique des utilisateurs, une approche SD-WAN vraiment globale offre de nombreux points d'accès à travers le monde, et chaque utilisateur se connectera au plus proche d'entre eux, améliorant ainsi la qualité de sa connexion aux ressources de l'entreprise (l'une des sources principales d'insatisfaction des utilisateurs vis-à-vis du VPN)

Ainsi, alors que les infrastructures VPN étaient parfaitement adaptées à un monde dans lequel les utilisateurs distants étaient minoritaires et l'ensemble des ressources étaient hébergés dans le datacenter, les infrastructures SD-WAN, nativement Cloud, sont une réponse industrialisée, maîtrisable et sûre aux contraintes du monde actuel, où les applications peuvent être aussi bien dans le nuage que le datacenter et où les utilisateurs distants sont la norme plutôt que l'exception.