Pourquoi le modèle « Zero-Trust » va bouleverser les stratégies VPN

Le modèle « Zero Trust » a été formalisé par le cabinet d'analyste Forrester. Il est né d'un constat : en matière de Système d'Information, la distinction entre les zones « externes » et « internes » a tendance à disparaitre. Des applications internes côtoient celles en mode SaaS hébergées à l'extérieur (et les plus critiques ne sont pas toujours celles que l'on croit !), tandis que l'infrastructure passe allégrement de serveurs virtualisés dans le datacenter à des instances ou du stockage dans un Cloud public.

Et puis les utilisateurs changent eux aussi : non seulement ils sont désormais souvent mobiles (n'oublions pas qu'en France la Loi autorise désormais, par défaut, le télétravail), mais ils ne sont plus uniquement que des humains : le nombre d'APIs explose et les machines parlent désormais tout autant aux machines que ne le font les collaborateurs (sinon plus !).

Il devient difficile dans ces conditions de déterminer qui est « de confiance » et qui ne l'est pas. Qu'est-ce qui est réellement interne, lorsqu'un serveur web public peut être hébergé en interne dans une DMZ et une application métier critique fonctionner sur une instance de Cloud public connectée à une base de données dans le datacenter ?

Dans de telles conditions, harmoniser les ACL, les autorisations d'accès aux divers Clouds et les annuaires Active Directoy devient forcément complexe. Et garder une visibilité parfaite sur les droits des utilisateurs à travers tous ces modèles, un défi !

Le VPN fortement remis en question

Il n'est donc pas étonnant que le concept de VPN, (comme ceux mis en avant sur le site Opportunites Digitales) créé à une époque où les topologies réseau étaient fort différentes, ne parvienne plus vraiment à suivre. De nombreuses organisations se rendent désormais compte qu'il est de plus en plus difficile d'adapter et de maintenir leurs configurations VPN, et ce n'est pas un hasard !

En outre, elles réalisent que la stratégie d'un contrôle d'accès à l'entrée suivi d'une quasi-liberté en interne (même au sein de VLANs bien segmentés) ne répond plus vraiment aux besoins actuels. Et l'avènement de la 5G, en multipliant les opportunités de connexions distantes et en remplaçant peut-être même à terme les connexions WiFi d'entreprise, ne va certainement pas simplifier les choses.

La micro-segmentation à la rescousse du modèle Zero Trust

C'est là qu'intervient le modèle Zero Trust : si le périmètre disparait, alors la notion de confiance accordée par défaut (au sein d'un réseau, d'une branche, du VLAN) doit elle aussi disparaitre. Elle est remplacée par un modèle plus agile dans lequel chaque ressource, où qu'elle soit, n'accepte plus que des utilisateurs authentifiés - d'où qu'ils viennent.

Évidemment, cela pose de sérieux défis d'architecture systèmes réseau. Va-t-on vraiment devoir placer une terminaison VPN devant chaque application ? Va-t-on devoir revenir aux clients VPN

multiples sur le poste de travail ? Et comment centraliser les différents droits et autorisations d'un utilisateur mobile ?

C'est là que le concept de micro-segmentation vient en aide. La micro-segmentation traite chaque connexion vers chaque application comme un environnement distinct, avec ses propres exigences de sécurité. Et surtout, cela est totalement transparent pour l'utilisateur.

Sans lancer de client VPN, avec un simple client local actif automatiquement dès le démarrage de la session, il est possible d'accéder de manière transparente aux différentes ressources de l'entreprise, où qu'elles se trouvent, où que soit l'utilisateur et avec toujours le même niveau de sécurité, que l'on soit au bureau connecté via Ethernet ou en déplacement sur une connexion 4G.

Sous le capot, le client de micro-segmentation identifie chaque application et lui applique une politique de sécurité spécifique définie par l'entreprise. Il va ainsi pouvoir chiffrer de manière sélective, appliquer des politiques prédéfinies ou exiger une authentification supplémentaire en fonction du profil de risque. Et cela fonctionne sur n'importe quelle connexion TCP ou UDP, que ce soit pour des flux applicatifs natifs (SAP, par exemple) ou des protocoles réseau (SSH, RDP, etc.)

Il devient alors possible de gérer de manière très précise les accès distants à tout type d'application où qu'elle soit hébergée, et quelle que soit l'origine de la connexion. Il n'existe plus de distinction entre les choix d'hébergement ou les modes de connexion (réseau d'entreprise ou 4G) : tout le monde est logé à la même enseigne et doit être correctement authentifié avant d'accéder à une ressource.

L'approche micro-segmentation, nativement adaptée au modèle Zero Trust

Par définition, la micro-segmentation considère en effet chaque paire utilisateur-ressource comme totalement indépendante, à la fois de l'origine de la connexion, mais aussi des autres connexions applicatives qui pourraient être actives sur le même terminal.

Au même titre que le modèle Zero Trust, la micro-segmentation considère donc que le plus petit élément significatif est la paire utilisateur-application, peu importe le terminal, la nature de la connexion et l'emplacement de chaque extrémité.

C'est pourquoi les organisations qui feront le choix de migrer progressivement vers un modèle Zero Trust devraient commencer dès à présent à implémenter de la micro-segmentation pour une partie de leurs utilisateurs, et commencer ainsi à accumuler une expérience qui leur sera précieuse pour l'avenir, lorsque le Zero Trust sera devenu incontournable.