Transformation sécurisée : Prisma Access remplace les accès distants par VPN

Les accès distants par VPN font partie du paysage des réseaux d'entreprise depuis des années. Tant et si bien que beaucoup considèrent « VPN » et « accès à distance » comme des synonymes. Toutefois, l'adoption rapide des applications cloud transforme radicalement les besoins des entreprises en matière de sécurité et de réseau. Dans ces deux domaines, les équipes veulent dorénavant sécuriser les accès à toutes les applications, et pas seulement celles hébergées dans le data center.

Ces nouvelles exigences soulèvent par conséquent deux questions essentielles : les VPN sont-ils encore d'actualité ? Faut-il remettre à plat la question même des accès à distance et opter pour une architecture plus efficace ?

Les limites des accès à distance

Les accès à distance ont pour vocation première d'agir comme une passerelle permettant aux utilisateurs situés hors du périmètre du pare-feu d'accéder aux ressources hébergées à l'intérieur du data center.

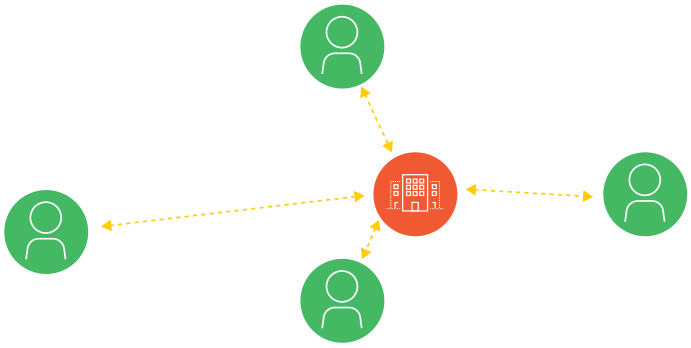

Figure 1 – Architecture traditionnelle d'un VPN

Architecturalement parlant, un VPN s'appuie sur une structure « hub-and-spoke », ou architecture en étoile, qui consiste à connecter les utilisateurs via des tunnels d'une longueur proportionnelle à la distance les séparant du data center. Certes, les problèmes de performances et de latence s'accentuent avec la distance. Mais il s'agit là de l'architecture optimale pour les applications hébergées en data center, car l'objectif est ici d'atteindre le « hub » (centre).

Toutefois, ce modèle montre un certain nombre de lacunes dès lors que l'environnement contient une variété d'applications cloud. Avec un VPN, le trafic passe toujours par le data center avant d'accéder à l'application hébergée dans le cloud. Concrètement, le trafic transite de la passerelle VPN vers le siège de l'entreprise, puis traverse le pare-feu du périmètre en direction d'Internet. La réponse de l'application emprunte ensuite le chemin inverse pour remonter jusqu'à l'utilisateur. Comme on le voit, le trafic doit donc effectuer tout un détour avant d'atteindre l'application cloud via Internet. D'un point de vue sécurité, une telle approche est justifiée lorsqu'une inspection du trafic s'opère au niveau du périmètre Internet du siège. Elle n'a cependant aucun sens en termes d'optimisation du réseau.

L'utilisation d'un VPN pour accéder aux applications cloud peut avoir un impact négatif sur l'expérience des utilisateurs, ce qui pousse ces derniers à éviter autant que possible

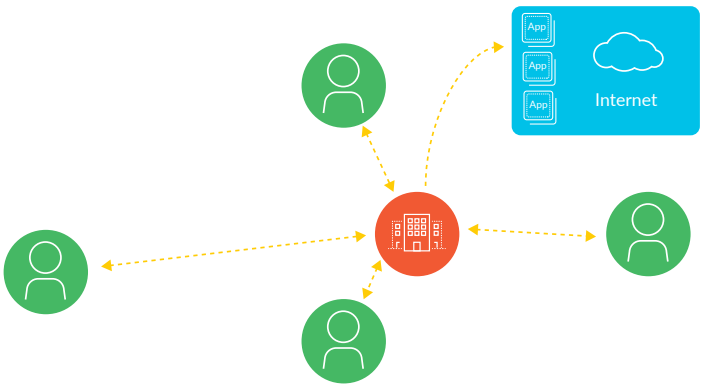

Figure 2 – Trafic VPN traditionnel vers le cloud

ce type d'accès. Par conséquent, ils ont tendance à se connecter lorsqu'ils doivent accéder au data center interne, puis se déconnectent aussitôt qu'ils n'en ont plus besoin. Or, cela génère de multiples problématiques de mise en application des politiques de sécurité. En effet, lorsqu'un utilisateur est déconnecté, l'entreprise perd toute visibilité sur son usage des applications, tout contrôle sur ses accès aux applications non approuvées, et toute capacité à assurer sa sécurité.

Ajouter une passerelle VPN ne résout en rien cette situation, car cette dernière ne représente ni plus ni moins qu'un point de terminaison du tunnel. Elle n'effectue aucune inspection du trafic. Et même déployées en grand nombre, ces passerelles ne seraient pas plus en mesure d'inspecter le trafic sans des mesures de sécurité supplémentaires.

Mauvais compromis

Pour pallier les problèmes réseau liés aux accès distants par VPN, les équipes IT doivent souvent faire des compromis qui peuvent avoir des conséquences sur la sécurité de l'entreprise.

- **Tunnel activé par l'utilisateur** – Un modèle VPN courant consiste à laisser aux utilisateurs le soin d'activer le tunnel d'accès au data center selon leurs besoins. Ils se connectent alors brièvement le temps d'accomplir leurs tâches, puis se déconnectent. Cependant, une fois déconnectés, ils accèdent directement à Internet sans que le trafic ne soit inspecté.
- **VPN avec « split tunneling »** – Un autre modèle VPN courant, mais non sécurisé, consiste à mettre en place un tunnel partagé. Dans ce cas de figure, le trafic en direction du siège passe par le tunnel VPN et tout le reste se connecte directement à Internet. Bien que cela réduise la latence, aucune inspection du trafic Internet et cloud n'est effectuée.
- **Proxy web** Pour gérer les scénarios d'utilisation hors connexion VPN, de nombreuses entreprises se sont tournées vers des dispositifs de sécurité réseau alternatifs comme les proxys web. Or, par définition, un proxy web n'inspecte pas tout le trafic réseau. Pire, l'inspection réalisée par le proxy sera complètement différente de celle qui s'opère au niveau du siège, avec pour conséquence des résultats divergents selon la situation géographique des utilisateurs.

Face à l'explosion du nombre de collaborateurs mobiles et d'applications cloud, les entreprises ne peuvent que constater que les accès VPN ne sont ni sécurisés ni optimisés pour le cloud. La mixité actuelle des parcs applicatifs impose d'adopter une nouvelle approche.

Une architecture moderne pour les collaborateurs mobiles

Les utilisateurs mobiles ont besoin d'accéder à Internet, au data center, mais aussi aux applications situées dans des clouds privés, publics et hybrides. Autrement dit, il leur faut une architecture capable d'optimiser les accès à toutes les applications, peu importe leur emplacement ou celui des utilisateurs. Avec Prisma™ Access, votre entreprise dispose d'une infrastructure cloud de sécurité pour connecter ses utilisateurs à une passerelle cloud avoisinante. Ils bénéficient ainsi d'un accès sécurisé à toutes les applications, en plus d'une visibilité et d'une inspection complètes du trafic sur tous les ports et protocoles.

Appareils mobiles gérés

L'application GlobalProtect™ est installée sur tous les appareils utilisateurs gérés (smartphone, tablette, ordinateur portable, etc.). Elle se connecte automatiquement à Prisma Access dès qu'un accès Internet est disponible. Aucune action n'est requise de la part de l'utilisateur.

Par ailleurs, Prisma Access s'appuie sur la couche de connectivité pour relier les applications de divers emplacements. Les utilisateurs accèdent ainsi à toutes leurs applications, hébergées dans le cloud ou le data center. Concrètement, la couche de connectivité se fonde sur les politiques des technologies App-ID™ et User-ID™ pour établir des accès sécurisés à un cloud public, une plateforme SaaS (Software-as-a-Service) et des applications de data center.

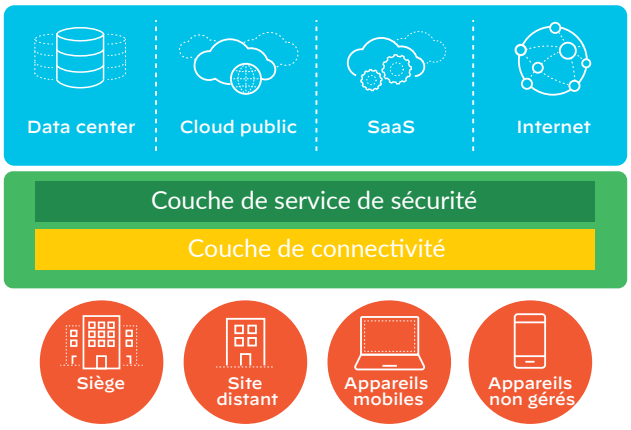

Figure 3 – Protection de tous les utilisateurs, quel que soit leur emplacement

Prisma Access intervient également sur la couche de service de sécurité pour assurer la protection de l'infrastructure Contre les cybermenaces (exploits, malwares connus et inconnus, trafic CnC, attaques par détournement d'identifiants, etc.) via la Palo Alto Networks Security Operating Platform®.

Appareils BYOD / non gérés

Prisma Access peut être intégré à une solution de gestion des appareils mobiles (MDM) pour contrôler les environnements BYOD (Bring Your Own Device). Cette intégration permet d'exploiter des fonctions comme les connexions VPN par application. Ainsi, les utilisateurs équipés d'appareils non gérés (par ex. des contractuels et salariés utilisant un équipement personnel) peuvent accéder au data center via un VPN sans client. Cette approche recourt à un proxy SAML pour une protection in-line des accès aux applications SaaS à partir d'équipements non gérés.

Une solution d'avenir

Vous êtes en pleine réévaluation de votre VPN ? Optez pour une architecture conçue pour sécuriser les accès à toutes les applications et vous protéger contre les cyberattaques. Avec Prisma Access, votre entreprise lève les freins des VPN classiques pour assurer un accès sécurisé à l'éventail complet d'applications dont vos utilisateurs ont besoin.

Pour en savoir plus, rendez-vous sur paloaltonetworks.com/prisma/access.

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101 HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr