Quatre obstacles à la sécurité du réseau SD-WAN à surmonter

Le plus grand défi du SD-WAN est que les solutions de sécurité traditionnelles ne sont pas suffisantes

Examinons quatre obstacles à franchir sur votre parcours SD-WAN, de même que le moyen le plus efficace de sécuriser votre déploiement.

Obstacle 1 — S'appuyer sur le firewall de votre périphérique SD-WAN edge

L'utilisation exclusive de la sécurité native SD-WAN laisse d'importants angles morts.

La plupart ne disposent pas de protections avancées contre les menaces, telles que NGFW, le sand-boxing, la prévention avancée des menaces, la sécurité IPS et DNS.

Que rechercher dans une solution?

- Un firewall basé sur le cloud, sensible aux applications, aux protocoles et au contexte.
- Inspection du trafic sur et hors réseau pour tous les utilisateurs, applications, appareils et emplacements.
- La capacité de prendre des décisions d'accès en fonction du contenu de la demande, pas seulement de la destination.

Obstacle 2 — Abandonner l'idée selon laquelle les approches de sécurité traditionnelles sont à la hauteur

Prendre des raccourcis tue l'efficacité.

Le déploiement d'appliances dans chaque filiale est d'un coût prohibitif et entraîne des compromis en matière de sécurité ou de performance.

Le backhauling du trafic vers les hubs régionaux n'est pas non plus la solution, car il entraîne la latence et une augmentation des coûts.

Que rechercher dans une solution?

- Une protection identique pour tous les utilisateurs avec une sécurité complète fournie par le cloud.
- Le décryptage et l'inspection de tous les ports et protocoles, y compris le trafic crypté SSL.

Obstacle 3 — Ne comptez pas sur les architectures de sécurité existantes pour gérer le trafic crypté

L'inspection du trafic crypté est cruciale.

Les firewall traditionnels n'inspectent pas nativement le trafic SSL.

L'activation de l'inspection dégrade généralement les performances, ce qui conduit certaines entreprises à contourner l'inspection SSL, les exposant ainsi à des risques plus importants.

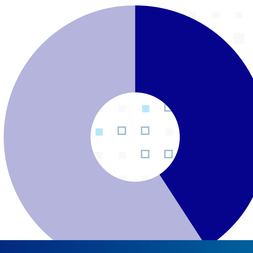
Que rechercher dans une solution?

- Une architecture basée sur un proxy qui inspecte nativement le trafic crypté SSL.
- Inspection de tout le trafic sans altérer la performance.
- Évolutivité élastique à mesure que le trafic et le nombre d'utilisateurs augmentent.

Plus de

41%

des attaques de réseau aujourd'hui utilisent le chiffrement pour échapper à la détection[1].



Obstacle 4 — Évitez le piège de plusieurs plates-formes de gestion de la sécurité

Les anciennes technologies sont éprouvantes.

La collecte et la corrélation des activités sont difficiles.

La mise en œuvre des modifications de politique nécessite généralement des interfaces de gestion individuelles ou un déploiement manuel.

Fournir une visibilité et des rapports en temps opportun est compliqué avec des appliances dispersées dans chaque filiale.

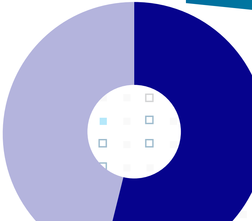
Que rechercher dans une solution?

- Un cadre flexible qui fournit des informations exploitables.
- Une plate-forme unique pour corréler et afficher les journaux.
- La capacité de définir de manière centralisée et de déployer immédiatement des politiques sur tous les sites.

54%

des organisations

ont signalé une complexité technologique accrue comme principale préoccupation concernant les méthodes actuelles de sécurisation des connexions Internet entre les sites[2].



Aimeriez-vous en savoir plus?

Lire en entier le Livre Blanc

zscaler™

[1] Ponemon Institute, « Hidden Threats in Encrypted Traffic: A Study of North America and EMEA », 2016
[2] Network World, Inc. Sondage auprès des directeurs informatiques de 100 organisations

zscaler.com