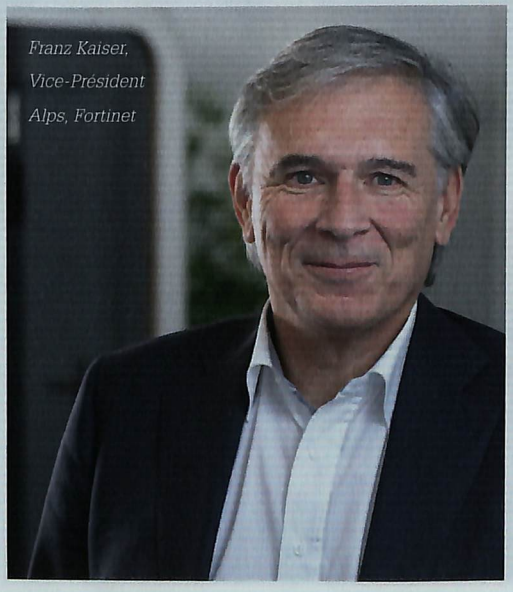
Surmonter les déficits de sécurité du SD-WAN

Le manque d'outils de sécurité natifs dans la plupart des solutions SD-WAN oblige les entreprises à élaborer leur propre stratégie en aval. Voici quatre aspects que les entreprises doivent prendre en compte en amont de la mise en œuvre de leur solution SD-WAN.



Franz Kaiser, Vice-Président Alps, Fortinet

1. En matière de SaaS, les entreprises doivent vérifier toutes les connexions et applications, évaluer les privilèges accordés et inspecter leur trafic. La connectivité pouvant évoluer à tout moment, la sécurité doit également s'adapter en temps réel pour prendre en charge les évolutions et les changements sur le réseau. Une solution de SD-WAN doit donc impérativement intégrer un panel de fonctions de sécurité professionnelle, parmi lesquelles un pare-feu nouvelle génération, un anti-malware, un système IPS et un filtrage web.
2. L'accès à des applications et ressources métiers hébergées en environnement multi-cloud et la migration de workflows essentiels vers ce multi-cloud viennent exacerber les défis de sécurité du SD-WAN, car les environnements cloud ne parlent pas tous le même langage. Les connexions doivent être en mesure de traduire, efficacement et en temps réel, les politiques, les protocoles et les fonctions de sécurité entre les différentes plateformes. Ces environnements modernes sont particulièrement vulnérables aux menaces zero-day, ce qui incite au déploiement d'une solution de sandbox dans le cadre de la stratégie de SD-WAN.
3. Il est de plus en plus urgent de chiffrer les données acheminées sur un réseau public, notamment au niveau des différents data centers, des services et applications SaaS, de l'Internet et entre les sites distants. Afin d'établir et de contrôler ces liens, les solutions SD-WAN doivent être compatibles avec SSL et s'adapter aux stratégies de réseau VPN en topologie mesh.
4. Le fait de rajouter a posteriori des solutions de sécurité autonomes à un environnement SD-WAN existant impose de devoir jongler entre différentes interfaces d'administration, ce qui, in fine, grève la visibilité et le contrôle. Les entreprises sont donc invitées à déployer une stratégie intégrée de monitoring de la conformité et de la sécurité pour s'assurer que toutes les connexions répondent aux exigences de base.

FORTINET®

Fortinet

Riedmühlestrasse 8
8305 Dietlikon
Suisse

Téléphone:
+41 44 833 68 48