Soutenir la transformation de l'entreprise avec le SASE

Le modèle Secure Access Service Edge (SASE) promet moins de complexité et d'efforts pour connecter en toute sécurité les utilisateurs mobiles et les succursales au réseau de l'entreprise. Rolf Bamert, du distributeur de sécurité informatique BOLL, décrit les avantages et présente une solution unique.

Rolf Bamert, Sales Engineer chez le distributeur de sécurité informatique BOLL

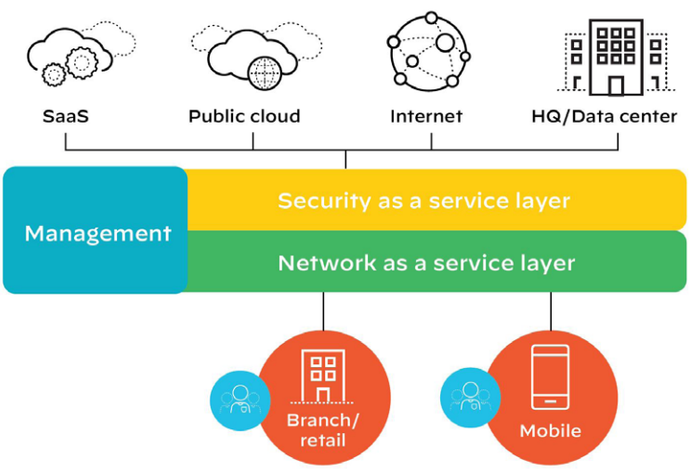
Qu'est-ce que le SASE ?
L'approche décrite par Gartner en 2019 combine les fonctionnalités WAN et de sécurité dans un modèle d'exploitation basé sur le cloud. L'abréviation signifie Secure Access Service Edge – un point d'accès sécurisé aux ressources de l'entreprise ou aux services cloud – avec une instance de sécurité virtuelle plutôt qu'une gateway physique déployée au point d'accès.

Pourquoi le SASE est-il nécessaire ?
Traditionnellement, différentes technologies de différents fabricants sont utilisées lors de la connexion des succursales, des postes de travail à domicile et des utilisateurs mobiles, lors de la collaboration avec des partenaires externes, lors de l'accès aux applications dans un cloud privé, lors de l'utilisation de solutions SaaS et de services de cloud public – un cauchemar en termes d'administration et de complexité.

Quel est le problème ?
Souvent, les solutions de sécurité ne sont pas intégrées, doivent être gérées séparément et, dans leur ensemble, forment un paysage très complexe avec des coûts d'administration et de maintenance élevés. En revanche, si tout est disponible à partir d'une seule source en tant que solution cloud, une grande partie de l'effort est éliminée et les coûts sont réduits.

Comment fonctionne la communication avec les points d'accès ?
Les utilisateurs mobiles ou les réseaux de succursales communiquent de manière cryptée avec le point d'accès le plus proche. Les passerelles IPSec existantes telles que les routeurs ou les firewalls de périmètre peuvent être utilisées. Les utilisateurs mobiles utilisent un client logiciel. Dans le cas de la solution SASE Prisma Access de Palo Alto Networks, il s'agit du client GlobalProtect.

En quoi Prisma Access se distingue-t-il des autres solutions SASE ?
Prisma Access fournit des instances virtuelles du firewall Palo Alto Networks dans le cloud, avec des fonctions telles que SSL Decryption, DNS/Web Security, Threat Prevention et Sandboxing. Tout le trafic de données est vérifié en ligne avec le principe Zero Trust basé sur l'utilisateur, l'application, l'appareil et le contexte. Rien ne contourne le firewall, tout le trafic de données (pas seulement web) est contrôlé.



Source: PAN_Prisma_Access_Grafik

Comment Palo Alto Networks garantit-il la disponibilité globale du service ?
Les instances de firewalls sont provisionnées dans les centres de données Google et AWS. Le client a ainsi accès à des backbones High-Speed/Low-Latency et bénéficie de points d'accès disponibles dans le monde entier. De cette manière, Palo Alto Networks peut également proposer des SLA en ce qui concerne la latence end-to-end pour les applications SaaS telles que Microsoft 365 ou Salesforce. Le service utilise pour chaque client ses propres instances.

Quels sont les différents modes de licensing pour Prisma Access ?
Palo Alto Networks propose un modèle de licence à plusieurs niveaux, en distinguant différents scénarios d'applications (utilisateur mobile, connexion à une succursale ou les deux), des clients actifs localement ou globalement. L'édition ZTNA est destinée exclusivement à l'accès des utilisateurs mobiles au web et au SaaS ainsi qu'au réseau de l'entreprise, tandis que les éditions Business et Business Premium couvrent l'accès internet sécurisé classique sans accès au réseau de l'entreprise. L'Edition Entreprise offre la fonctionnalité complète pour tous les scénarios.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch