Unternehmenstransformation mit SASE vorantreiben

Secure Access Service Edge (SASE) verspricht weniger Komplexität und Aufwand bei der sicheren Anbindung von mobilen Nutzenden und Filialen ans Unternehmensnetzwerk. Rolf Bamert vom IT-Security-Distributor BOLL schildert die Vorteile und stellt eine konkrete Lösung vor.

Was ist SASE?
Der von Gartner 2019 beschriebene Ansatz vereint WAN- und Security-Funktionalität in einem cloudbasierten Betriebsmodell. Die Abkürzung steht für Secure Access Service Edge – einem sicheren Zugangspunkt zu Unternehmensressourcen oder Cloud-Diensten –, wobei am Zugangspunkt kein physisches Gateway, sondern eine virtuelle Security-Instanz bereitgestellt wird.

Wieso braucht es SASE?
Traditionell kommen bei der Anbindung von Filialen, Heimarbeitsplätzen und mobilen Benutzenden, bei der Zusammenarbeit mit externen Partnern, beim Zugriff auf Applikationen in einer Private Cloud sowie bei der Nutzung von SaaS-Lösungen und Public-Cloud-Diensten unterschiedliche Technologien von verschiedenen Herstellern zum Einsatz – ein Albtraum punkto Administration und Komplexität.

Was ist dabei das Problem?
Die Sicherheitslösungen sind oft nicht integriert, müssen separat administriert werden und bilden im Ganzen eine hochkomplexe Landschaft mit hohem Verwaltungs- und Wartungsaufwand. Wenn hingegen alles als Cloud-Lösung aus einer Hand bereitsteht, entfällt ein Grossteil des Aufwands, und die Kosten sinken.

Wie funktioniert die Kommunikation mit den Zugangspunkten?
Mobile Nutzende oder Filialnetzwerke kommunizieren verschlüsselt mit dem nächstgelegenen Zugangspunkt. Dabei können bereits vorhandene IPSec-

Rolf Bamert ist Sales Engineer beim IT-Security-Distributor BOLL

Gateways, wie Router oder Perimeter-Firewalls, genutzt werden. Mobile Nutzende verwenden einen Software-Client. Im Fall der SASE-Lösung Prisma Access von Palo Alto Networks ist dies der GlobalProtect-Client.

Wie unterscheidet sich Prisma Access von anderen SASE-Lösungen?
Prisma Access stellt virtuelle Instanzen der Palo Alto Networks Next-Generation Firewall in der Cloud bereit mit Funktionen wie SSL Decryption, DNS-/Web-Security, Threat Prevention und Sandboxing. Dabei wird sämtlicher Datenverkehr nach dem Prinzip Zero Trust Network Access (ZTNA) anhand von Benutzer, Applikation, Gerät und Kontext inline überprüft. Nichts läuft an der Firewall vorbei, der gesamte Datenverkehr (nicht nur webbasierter) wird kontrolliert.

Wie garantiert Palo Alto Networks die globale Verfügbarkeit des Dienstes?
Die Firewall-Instanzen werden in den Rechenzentren von Google und AWS provisioniert. Der Kunde erhält damit Zugriff auf hochverfügbare High-Speed/Low-Latency-Backbones und profitiert dabei von weltweit verfügbaren Zugangspunkten. Palo Alto Networks kann auf diese Weise SLAs auch im Hinblick auf End-to-End-Latenz bei SaaS-Anwendungen wie Microsoft 365 oder Salesforce anbieten. Der Service verwendet für jeden Kunden eigene Instanzen, die vollautomatisch skalieren.

Wie ist Prisma Access lizenziert?
Palo Alto Networks bietet ein abgestuftes Lizenzmodell an und unterscheidet dabei zwischen verschiedenen Einsatzszenarien (mobile User, Filialanbindung oder beides), lokal oder global tätigen Kunden sowie vier Editionen mit unterschiedlichem Funktionsumfang. So ist die ZTNA-Edition ausschliesslich für den Zugriff durch mobile Nutzer auf Web und SaaS sowie auf das Unternehmensnetzwerk vorgesehen, während die Business- und Business-Premium-Editions den klassischen Secure Internet Access ohne Zugriff aufs Firmennetz abdecken. Die Enterprise-Edition bietet die komplette Funktionalität für alle Szenarien.

→ **www.boll.ch/info/Prisma-Access**

BOLL
IT Security Distribution

BOLL Engineering AG
Jurastrasse 58
CH-5430 Wettingen

Telefon +41 56 437 60 60
info@boll.ch
www.boll.ch