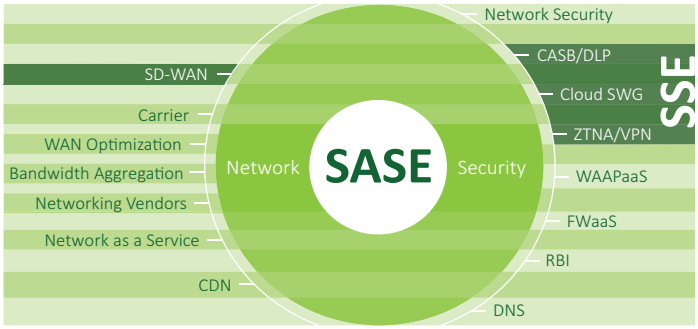
Was ist eigentlich Security Service Edge (SSE)?

Im Jahr 2021 führte Gartner einen neuen Magic Quadrant für die Sicherheitskategorie Security Service Edge (SSE) ein. Doch was ist eigentlich der Unterschied zwischen Security Service Edge (SSE) und Secure Access Service Edge (SASE)?

SASE (Secure Access Service Edge) ist ein Architekturmodell, welches Security- und Network-Funktionalitäten verbindet. Endpunkte können auf SASE-Plattformen sowohl abgesichert als auch miteinander verbunden werden. Dadurch ermöglichen SASE-Lösungen die standortunabhängige Arbeit (Home- und Remote-Benutzer) mit optimiertem und sicherem Netzwerkzugriff auf jede Anwendung. Auf der Sicherheitsseite umfasst SASE Dienste wie Secure Web Gateway (SWG), Cloud Access Security Broker mit Data Loss Prevention (CASB/DLP), Firewall as a Service (FWaaS), Zero Trust Network Access (ZTNA) etc. SSE bietet im Vergleich zu SASE lediglich einen begrenzten Umfang an konvergierter Netzwerksicherheit an. SSE konvergiert die SWG, CASB/DLP und ZTNA-Sicherheitslösungen in einem einzigen Cloud-nativen Service.



Quelle: CATO Networks

Warum SASE entstanden ist

Secure Access Service Edge (SASE) entstand aus der Erkenntnis, dass die separate Behandlung von Netzwerk- und Security-Anforderungen nicht zum Ziel führt. Traditionelle Netzwerk- und Netzwerksicherheitsarchitekturen, die das Unternehmensrechenzentrum als Mittelpunkt für den Zugriff positionieren, sind in der neuen Cloud-Welt gemäss Gartner zunehmend ineffektiv – selbst mit der Einführung einiger cloudbasierter Dienste wie cloudbasierte SWG, Content Delivery Network, Web Application Firewall usw.

Warum SSE entstanden ist

Durch die Digitalisierung und flexible Veränderung des Arbeitsplatzes müssen neue Herausforderungen gelöst werden. Die Einführung einer Security-Service-Edge-Architektur ermöglicht das ortsunabhängige Arbeiten und den Zugriff auf alle Cloud-Instanzen mit der bestmöglichen Sicherheit. Die Einführung einer SASE-Infrastruktur kann die Firmen überfordern, darum kann es sinnvoll sein, zuerst die SSE-Sicherheitskomponenten und die Netzwerkkomponenten in einem zweiten Schritt zu implementieren. Wichtig ist es, die Komplexität der Cloud-Instanzen zu verringern und die Datensicherheit zu erhöhen, sodass die Mitarbeiter von überall aus dem Internet auf Cloud-Dienste zugreifen können.

Den Einstieg in SSE in Phasen durchführen

Schritt 1: Das SSE-Framework adressiert CASB-, SWG- und ZTNA-Lösungen. Bereits bestehende Technologien sollten zunächst nach den Kategorien der Anwender, Geräte, Daten und Applikationen strukturiert werden, bevor sie auf eine integrierte Lösung migriert werden. Auch der Betrieb auf verteilten Systemen ist möglich, was allerdings entsprechend sorgfältig vorbereitet und auf aufeinander aufbauenden Modulen beruhen muss. Die Schritte 2 und 3 sind über folgenden QR-Code abrufbar:

Inseya und Cato SASE Cloud – die Partner für Onboard und Betrieb

Der Weg in die Cloud ist eine lange Reise. Die nötigen Bausteine zum Erfolg tangieren die Vernetzung, Sicherheitsinfrastruktur, Identitätsservices und datenführende Systeme. Die ausgewiesenen Security-Consultants von Inseya begleiten von Beginn weg, damit Security ein Teil des Designs ist und die Investitionen geschützt sind. Mit Cato SASE Cloud können Unternehmen jeden Benutzer sicher und optimal mit jeder Anwendung überall auf der Welt verbinden. Die Cloud-native Architektur ermöglicht die schnelle Bereitstellung neuer Funktionen und die Aufrechterhaltung einer optimalen Sicherheitslage.

INSEYA simply secure CATO NETWORKS

Inseya AG
Stauffacherstrasse 72, CH-3014 Bern
✆ +41 (0)31 914 18 18
info@inseya.ch, www.inseya.ch