Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE) kombiniert Netzwerk- und Sicherheitsfunktionen in der Cloud, um einen sicheren Zugriff auf Anwendungen zu ermöglichen, egal wo die Benutzer arbeiten. Das Ziel ist, Funktionen, die traditionell in siloartigen On-Premise Punktlösungen geliefert wurden, in einem einzigen, integrierten Cloud-Service zu konsolidieren.

Ausgangslage

Die steigende Nutzung von Cloud-Speicher und -Anwendungen führt vermehrt zu direktem Internetzugang bei Benutzern und Applikationen. Dies erhöht die Bedrohung, da traditionelle Sicherheitssysteme damit umgangen werden.

Lösung

Durch einen in der Cloud zur Verfügung gestellten WAN- und Security-Stack können Benutzer sowie der Zugriff auf Anwendungen und Daten standortunabhängig geschützt werden. Der Funktionsumfang umfasst dabei die beiden grundlegenden Punkte:

1. **Networking: Sicherer Zugriff auf das Internet und Anwendungen.**
   - Überwachung und intelligente Steuerung des Datenverkehrs durch SD-WAN.
   - Umleitung von DNS- und Web-Verkehr zum SASE Stack.
   - Zugriff auf interne Applikationen mit oder ohne VPN.
2. **Security: Schutz des Datenverkehrs von jedem Benutzer zu jeder Applikation.**
   - Erste Verteidigungslinie durch Sicherheit auf DNS-Ebene.
   - Kontrolle von Web- und Nicht-Web-Anwendungen.
   - Sicherer Zugriff auf cloudbasierte Anwendungen.

Wichtigste Erkenntnisse

1. SASE verbindet Benutzer nahtlos mit den Anwendungen und Daten, auf die sie zugreifen müssen – in jeder Umgebung, von jedem Ort aus.
2. Kontrolle des Zugriffs und Anwendung der entsprechenden Sicherheitsregeln unabhängig vom Arbeitsort der Benutzer.
3. Zusammenführen von Netzwerk- und Sicherheitsfunktionen zur sicheren Bereitstellung von Konnektivität als Service.

Darum Security by Netcloud

Durch Expertise im Cloud-, Netzwerk- und Security-Umfeld vereint Netcloud alle nötigen Disziplinen, um Secure Access Service Edge erfolgreich einzuführen. Wir bieten die gesamte Lösung aus einer Hand an und decken von Beratung bis Betrieb alle Phasen ab.

Weitere Infos:

Cisco SASE-Übersicht

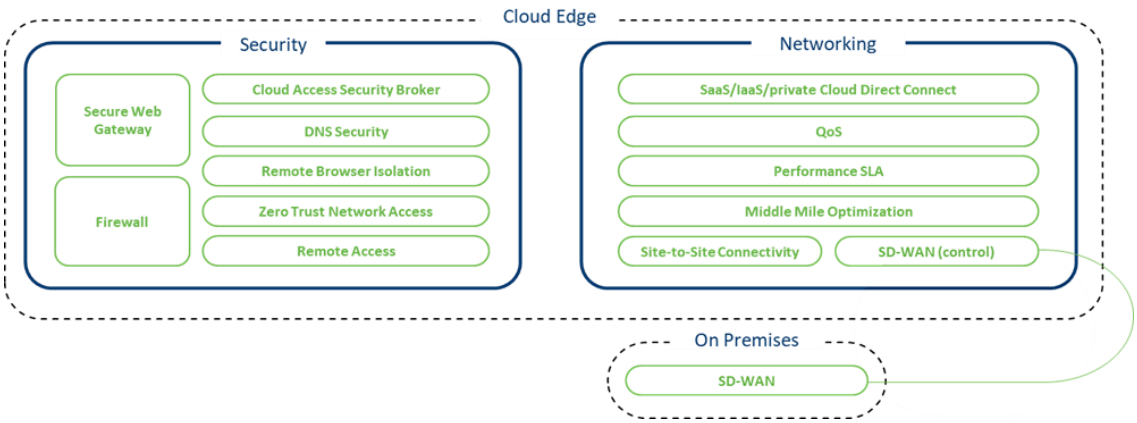

Abbildung 1: Basic SASE Service Framework gemäss Gartner

Secure Web Gateway	- Inhaltsfilterung nach Kategorie und Blockieren von bestimmten Benutzeraktivitäten in ausgewählten Anwendungen (z. B. Hochladen von Dateien auf Dropbox). - Ausführung von risikobehafteten Websites und Web-Applikationen in einem Remote-Browser in der Cloud. - Echtzeitprüfung eingehender Dateien auf Malware und andere Bedrohungen.
Firewall	- Zentrale Verwaltung von IP-, Port-, Protokoll- und Anwendungsregeln (Layer 3, 4 und 7) - Blockieren von risikoreichen, nicht-webbasierten Anwendungen / Protokollen.
Cloud Access Security Broker	- Überwachung und Kontrolle von Benutzeraktivitäten in SaaS-Anwendungen. - Anwenden von Scans/Richtlinien auf den Datenverkehr zu einer SaaS-Applikation (Verhinderung von Datenexfiltration).
DNS-Security	- Blockieren von bösartigen / unerwünschten Domains bei der DNS-Auflösung.
Zero Trust Network Access	- Überprüfung der Benutzeridentitäten, Geräteeinsicht erhalten & Vertrauenswürdigkeit feststellen. - Durchsetzung von Richtlinien für jeden Zugriffsversuch.
SD-WAN	- Cloudbasierte WAN-Architektur, die Anwender mit Anwendungen in Multicloud-Umgebungen verbindet. - Optimierung für SaaS-Anwendungen durch intelligente Pfadauswahl, hoher Servicequalität und Effizienzsteigerung auf der mittleren Meile.