

10

EIGENSCHAFTEN, DIE EINE SASE-LÖSUNG BIETEN SOLLTE

Whitepaper



Das Konzept des Secure Access Service Edge (SASE) hat sich als zentrale Technologie etabliert, die moderne Unternehmensnetzwerke sicherer und effizienter macht.

SASE verbindet Netzwerk- und Sicherheitsfunktionen in einer integrierten Architektur, die speziell darauf ausgelegt ist, die Herausforderungen dezentraler IT-Umgebungen zu bewältigen.

In diesem Beitrag beleuchten wir die 10 grundlegenden Eigenschaften einer SASE-Lösung, die für den Betrieb moderner Netzwerke unverzichtbar sind.

Integrierte Architektur: Netzwerk und Sicherheit immer zusammen denken

Eine der wichtigsten Eigenschaften von SASE ist die integrierte Architektur, die Netzwerk- und Sicherheitsfunktionen in einer einheitlichen Plattform vereint. Traditionell wurden Netzwerkmanagement und Sicherheitslösungen separat betrachtet, was zu einer fragmentierten IT-Infrastruktur führen konnte. SASE überwindet diese Trennung, indem es Netzwerkkonnektivität und Sicherheitsrichtlinien in einer einzigen, Cloud-basierten Lösung kombiniert.

Diese integrierte Architektur ermöglicht es Unternehmen, ihre Netzwerkeffizienz zu steigern und gleichzeitig die Sicherheit zu verbessern. Durch die enge Verzahnung von Netzwerk- und Sicherheitsfunktionen können Bedrohungen schneller erkannt und abgewehrt werden, während der Netzwerkverkehr optimiert wird.

Globales, Cloud-basiertes Backbone-Netzwerk mit Points-of-Presence (PoPs)

2

Das Rückgrat einer SASE-Lösung ist ein globales, Cloud-basiertes Backbone-Netzwerk, das über sogenannte Points of Presence (PoPs) auf der ganzen Welt zugänglich ist. Diese PoPs dienen als Einstiegspunkte für Standorte, Remote-Benutzer und Geräte in das SASE-Netzwerk. Sie bieten eine direkte, sichere Anbindung an den SASE-Service und gewährleisten eine hohe Verfügbarkeit und geringe Latenzzeiten.

Ein weiteres wichtiges Merkmal dieser PoPs ist die Integration von SD-WAN-Funktionen. SD-WAN optimiert den Datenverkehr und ermöglicht es, verschiedene Verbindungstypen effizient zu nutzen. Durch die Kombination mit einem globalen Backbone-Netzwerk können Unternehmen die Leistung und Ausfallsicherheit ihrer Netzwerke erheblich verbessern.

Einheitliches Management mittels CMA und Plattform-API

3

Die Verwaltung einer SASE-Lösung erfolgt über eine zentrale Management-Anwendung (CMA) und eine Plattform-API, die ein einheitliches Management der Netzwerk- und Sicherheitsfunktionen ermöglichen. Dies umfasst die Konfiguration von Sicherheitsrichtlinien, die Überwachung des Datenverkehrs und die Verwaltung von Benutzerzugriffen.

Die Plattform-API ermöglicht zudem die nahtlose Integration von SASE in bestehende IT-Ökosysteme, was die Flexibilität und Anpassungsfähigkeit der Lösung erhöht. Damit wird die Komplexität entscheidend reduziert und die Verwaltung vereinfacht.

Built-in Self Healing: Automatische Fehlererkennung und -mitigation

4

Moderne Netzwerke müssen in der Lage sein, sich selbst zu reparieren, um Ausfallzeiten zu minimieren und die Netzwerkverfügbarkeit zu maximieren. Eine SASE-Lösung bietet integrierte „Self-Healing“-Funktionen, die automatisch Fehler im Netzwerk erkennen und beheben können. Diese automatische Fehlererkennung und -mitigation basiert auf fortschrittlichen Algorithmen und Machine-Learning-Technologien, die in Echtzeit Netzwerkdaten analysieren und Anomalien identifizieren.

Sobald ein Problem erkannt wird, leitet das System automatisch Maßnahmen ein, um das Problem zu beheben, bevor es zu einem größeren Ausfall kommt. Dies erhöht die Zuverlässigkeit des Netzwerks und reduziert den Bedarf an manuellen Eingriffen.

Identitäts-Fokus: Zero-Trust-Netzwerkzugriff (ZTNA)

5

In einer SASE-Lösung steht die Identität des Benutzers im Mittelpunkt der Sicherheitsstrategie. Der Zero-Trust-Ansatz (ZTNA) geht davon aus, dass kein Benutzer, Gerät oder Dienst standardmäßig vertrauenswürdig ist – ein zentraler Aspekt insbesondere angesichts einer steigenden Zahl von Benutzern, die remote zugreifen und dabei unterschiedliche Geräte nutzen. So wird jede Zugriffsanfrage individuell überprüft, basierend auf der Identität des Benutzers, dem Gerätestatus und anderen Kontextinformationen.

Auf Basis dieses Ansatzes ermöglicht SASE, den Zugriff auf Ressourcen granular zu steuern und dabei sicherzustellen, dass nur autorisierte Benutzer auf die für sie freigegebenen Daten und Anwendungen zugreifen können.

Next-Generation-Security



SASE integriert Next-Generation-Security-Technologien, die den Schutz für alle Benutzer, Geräte und Anwendungen gewährleisten, unabhängig davon, wo sie sich befinden.

Zu den wichtigsten Edge-Sicherheitsfunktionen gehören:

Firewall-as-a-Service (FWaaS): Eine cloudbasierte Firewall, die den gesamten Netzwerkverkehr überwacht und unerwünschte Aktivitäten blockiert.

Cloud Access Security Broker (CASB): Ein Sicherheitsdienst, der den Zugriff auf Cloud-Dienste überwacht und schützt.

Secure Web Gateway (SWG): Ein Filter, der den Webverkehr auf Bedrohungen untersucht und den Zugang zu gefährlichen Websites blockiert.

Data Protection und Threat Prevention in Echtzeit



Die Sicherheit von Daten während der Übertragung ist ein zentraler Bestandteil jeder SASE-Lösung. SASE bietet umfassende Data-Protection-Funktionen, einschließlich der Verschlüsselung des Datenverkehrs mittels IPsec und TLS. Zusätzlich sorgt Network Access Control (NAC) dafür, dass nur autorisierte Geräte Zugriff auf das Netzwerk erhalten.

Echtzeit-Bedrohungsprävention ist eine weitere Schlüsselkomponente von SASE. Durch den Einsatz von Technologien wie Sandboxing, Intrusion Detection and Prevention Systems (IDS/IPS) und Erweiterter Erkennung und Reaktion (XDR) kann SASE Bedrohungen proaktiv erkennen und abwehren, bevor sie Schaden anrichten können. Diese Funktionen arbeiten Hand in Hand, um die Sicherheitslage des Unternehmensnetzwerks kontinuierlich zu überwachen und zu verbessern.

8

Dynamisches, intelligentes Traffic-Management

Ein weiteres zentrales Merkmal einer SASE-Lösung ist das dynamische Traffic-Management, das den Datenverkehr intelligent steuert, um die Netzwerkleistung zu optimieren. Es basiert auf Algorithmen, die den Netzwerkverkehr in Echtzeit analysieren und optimieren.

Anhand aktueller Netzwerkbedingungen wie Latenz, Bandbreite und Auslastung erfolgt eine dynamische Anpassung, um jederzeit die Anforderungen geschäftskritischer Anwendungen zu erfüllen.

9

Lokale Datenverarbeitung und optimiertes Routing

Um die Netzwerkleistung weiter zu steigern, ermöglicht SASE die lokale Datenverarbeitung, wann immer dies möglich ist. Indem Daten nahe ihrer Quelle verarbeitet werden, reduziert sich die Latenzzeit und die Effizienz des Netzwerks wird erhöht. Dies ist besonders wichtig für latenzempfindliche Anwendungen wie Video- und Sprachdienste.

Darüber hinaus optimiert SASE das Routing, indem es den Datenverkehr automatisch über die besten verfügbaren Pfade leitet. Dies gewährleistet nicht nur eine schnelle und zuverlässige Datenübertragung, sondern verbessert auch die Sicherheit, indem potenziell unsichere Netzwerke vermieden werden.

Multi-Cloud-Konnektivität

10

In einer Welt, in der viele Unternehmen eine Multi-Cloud-Strategie verfolgen, ist die Fähigkeit einer SASE-Lösung, nahtlose Konnektivität zwischen verschiedenen Cloud-Anbietern zu gewährleisten, von entscheidender Bedeutung. SASE ermöglicht die Integration von Public-Cloud-Diensten wie AWS, Microsoft Azure und Google Cloud über sichere, redundante IPsec-Tunnel. Diese Multi-Cloud-Konnektivität optimiert das Routing des Cloud-Datenverkehrs und reduziert die Abhängigkeit von teuren Direct-Connect-Diensten. Zudem stellt sie sicher, dass der gesamte Datenverkehr durch die Sicherheitsfunktionen der SASE-Lösung geschützt ist, unabhängig davon, welche Cloud-Plattform genutzt wird.

Fazit

Eine SASE-Lösung bietet eine Vielzahl von Eigenschaften und Funktionen für einen optimalen, sicheren Betrieb moderner Unternehmensnetzwerke. Durch die Kombination von Netzwerk- und Sicherheitsfunktionen in einer integrierten, Cloud-basierten Architektur ermöglicht SASE eine effiziente und zukunftssichere IT-Infrastruktur, die sich leicht managen lässt und einen Teil des herkömmlichen Aufwands mittels automatisierter und intelligenter Funktionen vermeidet

Ihr Ansprechpartner



Nils Kammann
Lead Security Consultant
T +49 040 4134980
contact@xantaro.net

Die Xantaro Gruppe

Xantaro ist einer der führenden Solution Provider für High-Performance-Netzwerke und Sicherheitslösungen. Xantaro unterstützt Unternehmen aller Branchen, Carrier und Service-Provider, Rechenzentren sowie Hosting- und Cloud-Dienstleister herstellerübergreifend mit rund 80 zertifizierten Netzwerk-Experten und 60 Kundenberatern.

Xantaro Deutschland GmbH | Jungfernstieg 7 | 20354 Hamburg
T +49 040 4134980 | contact@xantaro.net | www.xantaro.net

© Xantaro 2024