Lösungsprofil

Die drei wichtigsten Vorteile von SASE

Warum Secure Access Service Edge (SASE)?

Moderne digitale Geschäftsmodelle ermöglichen eine ganz neue Art der Kunden- und Mitarbeiterbindung, indem sie weltweit den durchgängigen Zugriff auf Anwendungen und Services ermöglichen, unabhängig davon, von wo aus Mitarbeiter und Kunden eine Verbindung herstellen oder welche Geräte sie verwenden.

In einer digitalen Welt, in der User und Anwendungen räumlich verteilt sind, kommt man mit herkömmlicher Netzwerksicherheit nicht mehr weiter. Gartner hat deshalb Networking und Sicherheit überdacht und ein Modell entwickelt, das den Anforderungen digitaler Unternehmen gerecht wird. Dieses Modell trägt den Namen Secure Access Service Edge (SASE).

> Eine SASE-Architektur spielt eine entscheidende Rolle. Idealerweise ist das Angebot cloudnativ, basiert auf Microservices und kann bei Bedarf skaliert werden. Um die Latenz zu minimieren, sollten Pakete in den Speicher kopiert, verarbeitet und übertragen/blockiert werden, und nicht von VM (virtuelle Maschine) zu VM oder von Cloud zu Cloud weitergeleitet werden. Der Software-Stack sollte keine spezifische Hardware-Abhängigkeit aufweisen und bei Bedarf instanziiert werden, um die risikooptimierten und richtlinienbasierten Funktionen für die Endgeräteidentität bereitzustellen.“ **— Gartner**[1]

#1 Geringere IT-Kosten und Komplexität

Angesichts der Verteilung der Daten auf Cloud-Anwendungen und SaaS-Services und den geografisch mehr oder weniger weit verstreuten Zugriffen der User, stößt das herkömmliche netzwerkbasierte Sicherheitsmodell an seine Grenzen. Um dies zu kompensieren, mussten Organisationen die Sicherheitslücken durch die Bereitstellung zusätzlicher Services schließen, dabei aber, trotz eines Mangels an Fachkräften, erheblich höhere Bereitstellungs-, Verwaltungs- und Betriebskosten in Kauf nehmen. Allerdings ist dieses Netzwerksicherheitsmodell — trotz wachsender Kosten und Komplexität — immer noch nicht skalierbar, nicht agil und in einer digitalen Welt einfach nicht effektiv.

Anstatt zu versuchen, ein zeitgemäßes Problem mit einem alten Konzept zu lösen, stellt Zero Trust SASE das Sicherheitsmodell einfach auf den Kopf. Während Legacy-Ansätze darauf basierten, Perimeter rund um die Anwendungen zu errichten, konzentriert sich SASE auf Entitäten, zum Beispiel User, die auf die Anwendungen zugreifen, und rückt die Sicherheit so nahe wie möglich an diese Entitäten heran. Als Cloud-Service erlaubt oder verweigert SASE — dynamisch und gemäß den definierten Geschäftsregeln einer Organisation — Verbindungen zu Services und Anwendungen. Das alles wird über einen einzigen Service abgewickelt, der mehrere, bis dahin getrennte Funktionen, wie SWG, ZTNA usw. zusammenführt.

WORAUF ES ANKOMMT

Die wichtigste Komponente eines erstklassigen SASE-Angebots ist die Architektur, auf der es basiert. Gartner hat genaue Angaben zur Art der Architektur gemacht, die erforderlich ist, um die Vorteile von SASE voll auszuschöpfen. Am wichtigsten ist, dass sie von Grund auf so aufgebaut sein muss, dass sie die Anforderungen hinsichtlich der Skalierbarkeit an einen vollständig in der Cloud bereitgestellten Sicherheitsservice erfüllt.

Es muss sich um ein verteiltes Angebot handeln, das mehrinstanzenfähig ist und eine bedarfsabhängige globale und dynamische Skalierung ermöglicht. Das Angebot muss sich von herkömmlichen, auf Richtlinien und Policy-Layers basierenden Netzwerkkonzepten lösen und stattdessen auf Unternehmensrichtlinien aufbauen. Und schließlich muss diese Architektur eine tatsächlich integrierte Plattform mit einheitlichem Cloud-Management unterstützen.

WAS ES ZU VERMEIDEN GILT

Gartner warnt ausdrücklich vor herkömmlichen Netzwerksicherheitsansätzen, die VM-basierte Angebote nutzen, die in Infrastrukturen von Cloud-Anbietern ausgeführt werden. Die Skalierung solcher VM-basierter Lösungsansätze ist in einer IaaS-Umgebung problematisch und bietet aufgrund des unausweichlichen Hairpinnings zwischen den Cloud-Anbietern und den Usern der Anwendungen keine konsistente User Experience.

Dieses Modell basiert auf einer Single-Tenancy-Architektur, die in einem SASE-Modell auf dem Userzugriff basierende, netzwerkorientierte Zugriffsrichtlinien zu verwenden versucht. Das führt zu erheblich komplexeren Bereitstellungen, die sich nicht in ein SASE-Modell übertragen lassen. Darüber hinaus basieren diese Ansätze häufig auf mehreren Produkten, die nicht wirklich integriert sind, sondern durch eine Overlay-Oberfläche unabhängiger Services, die häufig durch Übernahmen hinzugekommen sind, zusammengefügt werden.

> „Secure Access Service Edge ist ein neu entwickeltes Angebot, das die Leistungsfähigkeit von WAN mit umfassenden Netzwerksicherheitsfunktionen (wie SWG, CASB, FWaaS und ZTNA) kombiniert, um die dynamischen, sicheren Zugriffsanforderungen digitaler Unternehmen zu gewährleisten.“ — **Gartner**[1]

#2 Gewährleistet hervorragende Anwendererfahrungen

Es gibt einen guten Grund, warum der Schwerpunkt von SASE auf der User Experience liegt. Solange sich die User im Netzwerk befanden, die Anwendungen im Rechenzentrum liefen und Server und Infrastruktur im Besitz der IT-Abteilung waren und dort verwaltet wurden, war die User Experience leicht zu steuern und vorherzusagen. Nun sind die Anwendungen über mehrere Clouds verteilt, aber der Zugriff auf diese Anwendungen stützt sich weiterhin auf das alte Modell eines VPN, das aus Sicherheitsgründen eine Verbindung zu einem Netzwerk herstellt. Dieses Modell bringt den User zur Sicherheit und nicht die Sicherheit zum User, obwohl das für eine positive User Experience unerlässlich ist. Um eine optimale Bandbreite und geringe Latenz sicherzustellen, fordert Zero Trust SASE die Durchsetzung der Sicherheit in der Nähe der User, die intelligente Verwaltung der Userverbindungen an den Internetknoten und die Optimierung der direkten Verbindungen (Peering) zu Cloud-Anwendungen und -Services.

WORAUF ES ANKOMMT

Der Schlüssel zu einer erstklassigen User Experience liegt in der Bereitstellung optimaler Bandbreite mit geringster Latenz. Die einzige Möglichkeit, dieses Ziel zu erreichen, besteht darin, die Anzahl der Hops auf dem Weg zur Anwendung zu reduzieren und sicherzustellen, dass die richtige Bandbreite durch Bandbreitenkontrollen zugewiesen wird.

Idealerweise liegt der Sicherheits-Stack so nah wie möglich am Standort des Users, an Internetknoten in einer geografisch weit verteilten Bereitstellung. Der Zugriff auf Anwendungen über diese Vermittlungspunkte erfordert die Fähigkeit, den Datenverkehr durch direktes Peering intelligent zum nächstgelegenen geografischen Standort der Anwendung leiten zu können.

WAS ES ZU VERMEIDEN GILT

Angebote, die auf VMs basieren, die bei Cloud-Anbietern oder in IaaS ausgeführt werden, führen zu Traffic-Hairpinning. Solche Angebote werden von Gartner ausdrücklich nicht als SASE-Lösung definiert und sollten vermieden werden.

Dies liegt in erster Linie daran, dass VM-basierte Architekturen Verbindungen nicht auf User-, sondern auf Anwendungsebene skalieren und steuern. Damit lässt sich jedoch keine gute User Experience garantieren. Außerdem lassen sich diese Angebote nicht dynamisch skalieren und erfordern eine Nutzungsplanung, bei der spätere Änderungen nicht ohne geplante Ausfallzeiten möglich sind.

> SASE-Funktionen zur Richtlinienentscheidung und -durchsetzung müssen überall dort vorhanden sein, wo sich die Endgeräteidentitäten befinden... SASE-Angebote, die nur die Internet-Backbone-Kapazität von IaaS nutzen, aber keine lokalen POPs/Edge-Funktionen bereitstellen, riskieren Latenz, Performanceprobleme und daraus resultierend Unzufriedenheit auf Userseite.“ **— Gartner**[1]

#3 Vermindertes Risiko

Bei der Sicherheit dreht sich alles darum, Risiken zu erkennen und zu vermeiden. Zero Trust SASE als Cloud-Service wurde entwickelt, um den besonderen Risiken der neuen Gegebenheit geografisch weit verteilter User und Anwendungen begegnen zu können. Die Definition von Sicherheit als in die Struktur des Modells integrierte Funktion statt als Funktion, die von der Konnektivität der Services getrennt ist, stellt sicher, dass alle Verbindungen überprüft und abgesichert werden, unabhängig davon, wo User eine Verbindung herstellen, auf welche Anwendungen sie zugreifen oder ob eventuell eine Verschlüsselung zum Einsatz kommt.

WORAUF ES ANKOMMT

Um Risiken zu minimieren, muss das Konzept der netzwerkbasierten Konnektivität aufgegeben und stattdessen eine Verbindung zwischen Usern und Anwendungen auf Grundlage eines echten ZTNA-Modells (Zero Trust Network Access) hergestellt werden. ZTNA stellt sicher, dass nur Usern, die berechtigt sind, auf eine Anwendung zuzugreifen, dieser Zugriff gestattet wird. Dabei wird diese Berechtigung durch Unternehmensrichtlinien und nicht durch komplexe mehrschichtige Richtliniendefinitionen festgelegt.

Eine SASE-Plattform vermindert Risiken auch dadurch, dass sie die Angriffsfläche beseitigt. Sie verbirgt das Unternehmensnetzwerk und die Quellidentitäten vor dem Internet und verhindert damit, dass Sie zum Ziel von Angriffen, wie beispielsweise DDoS, werden.

Das SASE-Modell wird über eine Proxy-basierte Architektur bereitgestellt, die die gesamte Kommunikation zwischen Usern und Anwendungen abwickelt. Diese Architektur gewährleistet, dass der gesamte Traffic entschlüsselt und überprüft werden kann, und bietet umfassende Transparenz. Schlussendlich sorgt die SASE-Architektur für den Austausch des vollständigen Datenkontexts zwischen Entitäten und Anwendungen, um sicherzustellen, dass alle Verbindungen den Compliance- und Data-Governance-Anforderungen entsprechen.

WAS ES ZU VERMEIDEN GILT

Herkömmliche Ansätze zur Perimeter-Sicherheit verwendeten ein Firewall-basiertes Modell, das Paketströme untersuchte und das Risiko auf der Grundlage der Überprüfung dieser Pakete bestimmte. Dieses Modell hat sich zwar im Rahmen der perimeterbasierten Sicherheit bewährt, ist jedoch den neuen Herausforderungen einer SASE-basierten Bereitstellung nicht gewachsen.

Das größte Problem einer als Dienst ausgeführten Firewall-Architektur ist, dass Bedrohungen erst nachträglich erkannt und es diesen ermöglicht wird, ihr Ziel zu erreichen, bevor sie entdeckt werden. Das hat einen einfachen Grund: Sie sind nicht in der Lage, die Daten vor dem Senden zurückzuhalten, um ihre Folgen zu ermitteln. Diese Einschränkung erschwert die Sitzungsentschlüsselung und den Datenschutz außerordentlich, da dies Funktionen sind, bei denen der Stream — ähnlich wie bei einem Proxy — zurückgehalten und neu zusammengesetzt werden muss.

Bei einem Firewall-Service ist für die Entschlüsselung, Überprüfung und Wiederherstellung von Funktionen ein separater Prozess erforderlich, der vom Dienst entkoppelt ist. Dieser Prozess kompliziert die Richtlinien, erzeugt Latenzen und führt und zu einer schlechten Leistung — im Rahmen der Implementierung ist häufig nur ein eingeschränkter Funktionsumfang möglich. Darüber hinaus erfordert SASE eine Single-Pass-Architektur, um den gesamten Inhalt auf einmal verarbeiten zu können. Stream-basierte Firewall-Angebote setzen die Source-IP-Adresse des Host-Netzwerks auch potenziellen Gegnern aus — im Prinzip machen sie auf ihre eigenen Angriffsflächen aufmerksam und laden praktisch zu gezielten Angriffen ein.

Der Zscaler SASE-Ansatz

Die KI-gestützte Cloud-Sicherheitsplattform von Zscaler ist ein SASE-Service, der von Grund auf für Leistung und Skalierbarkeit konzipiert ist. Da es sich um eine global aufgestellte Plattform handelt, sind User immer nur einen Katzensprung von ihren Anwendungen entfernt. Durch das Peering mit Hunderten Partnern an wichtigen Internetknoten auf der ganzen Welt bietet Zscaler Ihren Usern, Workloads, Geschäftspartnern und Standorten optimale Performance und Zuverlässigkeit.

Zscaler Zero Trust SASE baut auf der bewährtesten SSE-Plattform der Branche auf und bietet eine neue Herangehensweise an SD-WAN. Heute vertrauen mehr als 30 % der Forbes Global 2000-Unternehmen darauf, dass Zscaler sie sicher ins digitale Zeitalter führt.

Aufgrund seiner langen Marktpräsenz konnte Zscaler unter Beweis stellen, dass seine Architektur skalierbar ist und derzeit über 360 Milliarden Transaktionen pro Tag und über 500 Billionen tägliche Signale für KI-/ML-Cloud-Effekte verarbeitet.

Die Zero-Trust-SASE-Architektur von Zscaler wird in 150 Rechenzentren weltweit bereitgestellt, um zu gewährleisten, dass User sichere, schnelle und lokale Verbindungen erhalten, egal wo sie sich befinden.

Weitere Informationen zum SASE-Ansatz von Zscaler finden Sie unter
zscaler.de/capabilities/secure-access-service-edge

[1] Gartner, The Future of Network Security Is in the Cloud; Lawrence Orans, Joe Skorupa, Neil MacDonald

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, zuverlässiger und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an beliebigen Standorten vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de