citrix

Whitepaper

Secure Access Service Edge (SASE) Architekturen verstehen

Überdenken Sie Netzwerk- und Sicherheitsarchitekturen, um moderne Anforderungen zu erfüllen

Eine weiterentwickelte Art zu arbeiten

Die Art, wie Menschen arbeiten, hat sich weiterentwickelt. Unternehmen müssen diese veränderten Arbeitsweisen berücksichtigen, um zukünftige Investitionen in Infrastrukturen und Architekturen zu planen oder Zeitpläne zu erstellen, beispielsweise für die Bereitstellung neuer digitaler Services. Es ist wichtig, mit diesen Entwicklungen Schritt zu halten, um nachweisbare Kennzahlen für den Unternehmenserfolg positiv beeinflussen zu können, wie z. B. die Betriebsperformance, Finanzierungskosten, Mitarbeitermotivation und Kundenzufriedenheit.

- **Gestiegene Nutzung von Cloud-Anwendungen und -Services:** Gartner schätzt, dass die Ausgaben für SaaS-Anwendungen zwischen 2020 und 2022 weltweit um 34 % steigen werden[1]. Diese SaaS-Anwendungen werden sowohl für geschäftliche als auch private Zwecke genutzt. In beiden Fällen erwarten Nutzer einen erstklassigen Benutzerkomfort von diesen Anwendungen. Sie möchten einen schnellen Zugriff auf jede Anwendung, egal wo sie sich gerade befinden.
- **Mehr Remote-Mitarbeiter:** COVID-19 hat Arbeitgeber und Mitarbeiter gezwungen, Remote-Arbeit auszuprobieren. Laut einer Umfrage im Juni 2020 möchten 72 % der Mitarbeiter mindestens zwei Tage pro Woche per Remote-Zugriff arbeiten, selbst wenn COVID-19 keine Gefahr mehr darstellt[2]. Remote-Mitarbeiter haben auch erwähnt, dass es schwieriger geworden ist, mit anderen zusammenzuarbeiten, was einer der Hauptgründe für den Produktivitätsverlust ist. Daher ist es nicht überraschend, dass 53 % aller Arbeitgeber in eine bessere mobile Experience für geschäftliche Anwendungen und Daten investieren möchten[3].
- **Sicherheitsbedrohungen haben immer schwerwiegendere Auswirkungen:** 3,86 Millionen USD – das sind die durchschnittlichen Gesamtkosten eines Datenverstoßes[4]. Die meisten Datenverstöße werden vorsätzlich geplant und machen sich menschliche Fehler oder Schwachstellen im System zunutze. Für Unternehmen ist es daher wichtig, ihre Sicherheitssysteme und -architekturen weiterzuentwickeln, um schädliche Angriffe unterbinden zu können. Dadurch verhindern sie nicht nur finanzielle Schäden, sondern bewahren auch das Vertrauen von Kunden und Mitarbeitern.

IT-Teams benötigen eine Netzwerk- und Sicherheitsarchitektur, die allen Nutzern – einschließlich Remote-Mitarbeitern – einen schnellen, zuverlässigen und sicheren Zugriff auf Anwendungen ermöglicht. Leider stammen die Hub-and-Spoke-Architekturen, die heutzutage in Gebrauch sind, aus einer Zeit, als Anwendungen sich im Rechenzentrum befanden und Mitarbeiter in Büros über private WANs auf diese zugegriffen haben. Diese zugrundeliegenden Architekturen müssen sich ändern, um neue technologische Trends zu unterstützen, die den Unternehmenserfolg nachweislich fördern können.

„53 % aller Arbeitgeber möchten in eine bessere mobile Experience für geschäftliche Anwendungen und Daten investieren“

Architekturen für Cloud- und mobile Lösungen

Herausforderungen bei herkömmlichen Architekturen

Nachstehend einige der spezifischen Herausforderungen, die sich durch Architekturen, die für Cloud- und mobile Lösungen optimiert sind, meistern lassen.

- **Schlechte Employee Experience bei Anwendungen:**
  - *Herausforderungen in Bezug auf die Architektur:* Hub-and-Spoke-Architekturen machen es aus Sicherheitsgründen erforderlich, dass Traffic durch das Rechenzentrum geleitet wird. Diese zusätzliche Traffic-Weiterleitung steigert die Anforderungen an das WAN. Noch schlimmer ist jedoch, dass dies auch eine vermeidbare Latenz erzeugt und die Employee Experience verschlechtert.
  - *Herausforderungen in Bezug auf Anwendungen:* Remote-Mitarbeiter nutzen Cloud-Anwendungen, um zusammenzuarbeiten und zu kommunizieren, dazu gehören verschlüsselte Anwendungen für den Dateiaustausch wie Microsoft SharePoint und Videokonferenzanwendungen wie Microsoft Teams. Dies stellt eine hohe Belastung für die zugrundeliegende Infrastruktur dar, also Appliances im Rechenzentrum und WAN-Verbindungen. Diese Hardware-Appliances haben eine eingeschränkte Rechenkapazität. Wenn die Belastung durch verschlüsselte Cloud-Anwendungen die Performance verschlechtert, schadet dies der Employee Experience.
- **Uneinheitliche Sicherheit für Remote-Mitarbeiter:** Mitarbeiter erwarten, dass die Anwendungsperformance so gut ist wie im Büro, selbst wenn sie von zuhause aus arbeiten. Um dies zu erreichen, beenden Mitarbeiter häufig die Verbindung zu VPN-Clients, wenn sie auf Web- und SaaS-Anwendungen zugreifen. Dadurch sind sie ungeschützt und anfällig für Bedrohungen. Mitarbeiter, die über BYO-Geräte auf Unternehmensdaten zugreifen, setzen das Unternehmen einem ähnlichen Risiko aus. 61 % aller CISOs und CIOs geben an, dass das Risiko durch private Endgeräte und Software gestiegen ist, da mehr Menschen per Remote-Zugriff arbeiten[5]. Deswegen benötigen Unternehmen einen Weg, um alle Nutzer und Endgeräte einheitlich abzusichern, ohne die Performance zu beeinträchtigen – egal wo diese sich befinden.
- **Komplexer Betrieb:** Herkömmliche Architekturen bestehen häufig aus dezentralen, aufeinanderfolgenden Servicelösungen. Dadurch ist es schwierig, Änderungen an der Architektur vorzunehmen, ohne einen weiteren Teil der Konfiguration zu stören. Wenn die Architektur anhand des Traffic-Aufkommens skaliert werden soll, muss zudem häufig die Kapazität physischer Appliances erweitert werden. Dies ist zeitaufwendig und hindert das IT-Team daran, sich auf die Bereitstellung neuer digitaler Services zu konzentrieren.

Wichtige Funktionen für eine moderne Unternehmensarchitektur

- **Direkter Internetzugang:** Mitarbeiter müssen auf direktem Wege auf alle Anwendungen zugreifen können. Diese Verbindung muss jedoch abgesichert sein.
- **Sicherheit, die dem Benutzer folgt:** Auf einem Rechenzentrum basierende Sicherheitsmodelle erlauben keinen direkten Internetzugang. Daher wird eine Sicherheitsarchitektur benötigt, die zwischen dem Mitarbeiter und der Anwendung positioniert ist, egal wo sich der Mitarbeiter befindet. Dies kann nur durch Sicherheitsservices erreicht werden, die über die Cloud bereitgestellt werden. Es wird davon ausgegangen, dass 76 % aller Unternehmen ihre Sicherheitsfunktionen in die Cloud übertragen[6].
- **WAN-Services für eine hohe Anwendungsperformance:** Ein direkter Internetzugang verkürzt den Übertragungsweg zwischen dem Mitarbeiter und der Anwendung. Dies mindert jedoch nicht Schwankungen bei der Anwendungsperformance, die aufgrund von schlechten privaten oder geschäftlichen Internetverbindungen entstehen. Daher benötigen Unternehmen umfassende Funktionen wie ein softwaredefiniertes WAN (SD-WAN) sowie WAN-Optimierung, um eine konstante Anwendungsperformance über einen direkten Internetzugang sicherzustellen.
- **Single-Pass-Architektur:** Um die Latenz zu beseitigen, die durch aufeinanderfolgende Inspektionsfunktionen in einer typischen Sicherheitsumgebung erzeugt wird, müssen Unternehmen eine Single-Pass-Architektur einsetzen. Single-Pass-Architekturen öffnen und inspizieren den Traffic nur einmal und lassen ihn gleichzeitig von mehreren Policy Engines untersuchen. Zum Beispiel würde ein verschlüsseltes Paket in einer Single-Pass-Architektur nur ein einziges Mal geöffnet werden, um es von einer Malware- und einer Datenverlust-Engine inspizieren zu lassen.
- **Zentrales Management:** Die Integration der Steuerebene in die Netzwerk- und Sicherheitsumgebung muss den gesamten Lebenszyklus vereinfachen: Provisioning,

richtlinienbasiertes Management, Visibilität und Fehlerbehebung. IT-Administratoren müssen beispielsweise über ein zentrales Dashboard verfügen, das einen umfassenden Überblick über die gesamte Netzwerk- und Sicherheitsumgebung der Unternehmensarchitektur bietet, wie z. B. Niederlassungen, Points of Presence, Tunnel und die Netzwerknutzung. Dadurch werden tote Winkel beseitigt und Konfigurationen der gesamten Architektur vereinfacht, wodurch die Wahrscheinlichkeit durch menschliche Fehler verringert wird.

„76 % aller Unternehmen planen, ihre Sicherheitsfunktionen in die Cloud zu übertragen“

Secure Access Service Edge

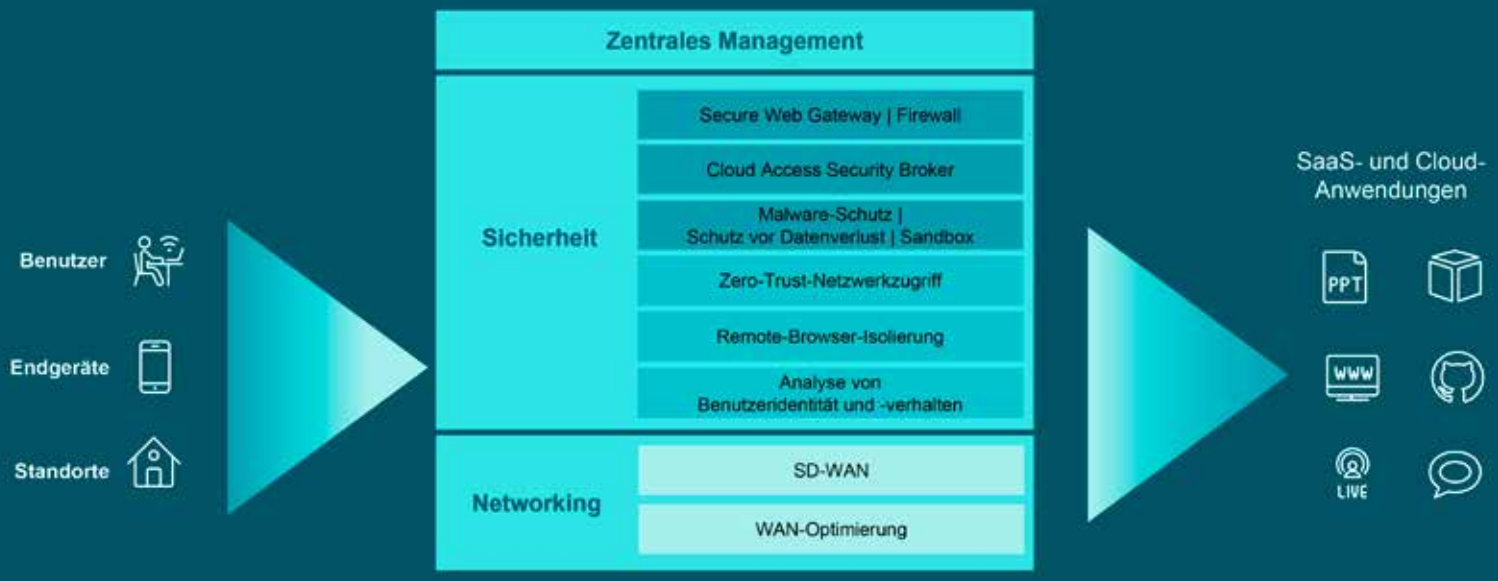
Secure Access Services Edge (SASE) wurde entwickelt, um herkömmliche Hub-and-Spoke-Architekturen durch einen sicheren direkten Internetzugang zu ersetzen. Die Konsolidierung von über die Cloud bereitgestellten Sicherheitsfunktionen, Zero-Trust-Zugriff und umfassenden WAN-Funktionen sorgt für eine hohe Sicherheit und eine stets erstklassige Employee Experience. Dabei spielt es keine Rolle, wo sich der Mitarbeiter befindet oder wo die Anwendung gehostet wird.

SASE-Services werden unter Berücksichtigung der Identität des Nutzers und dem Kontext in Echtzeit eingesetzt. Beispielsweise würde ein Manager in der Finanzabteilung einen anderen Zugriff erhalten als ein Auftragnehmer, der für die Marketingabteilung arbeitet. Zu den wichtigsten Services einer SASE-Architektur gehören:

- **Secure Web Gateways (SWG)** sind für Unternehmen konzipierte Sicherheitslösungen, die Anwender vor Bedrohungen aus dem Netz schützen. Sie bieten folgende Funktionen:
  - *URL Filtering* – Gewährt oder blockiert den Zugriff auf Websites, indem die angeforderten URLs mithilfe einer Datenbank gefiltert werden, die von der Organisation festgelegt wird.
  - *Malware-Schutz* – Prüft verschlüsselte und unverschlüsselte Web-Inhalte, um Bedrohungen zu identifizieren und zu blockieren.
  - *Anwendungskontrolle* – Bietet einen Überblick darüber, auf welche Anwendungen zugegriffen wird, sowie eine granulare Kontrolle, um Sicherheit und Compliance zu gewährleisten.

SWGs werden üblicherweise als Inline-Cloud-Service implementiert und über global verteilte

SASE vereint Networking und umfangreiche, über die Cloud bereitgestellte Sicherheitsfunktionen mit einem zentralen Management



Points of Presence (PoPs) in mandantenfähigen Sicherheitsumgebungen orchestriert. Traffic von Unternehmensnutzern – sowohl Remote-Mitarbeitern als auch Mitarbeitern im Büro – wird zur SWG-Cloud weitergeleitet, wo er inspiziert und abgesichert wird.

- **Cloud Access Security Broker (CASB)** unterstützen Sie bei der Überwachung, Absicherung und dem Management des Zugriffs auf genehmigte und ungenehmigte SaaS-Anwendungen. CASB-Funktionen basieren auf vier Grundpfeilern:
  - *Visibilität* – Konsolidierter Überblick über alle Anwendungen, einschließlich ungenehmigter Anwendungen (Schatten-IT), die von Anwendern im Unternehmen genutzt werden
  - *Datensicherheit* – Schutz vor unautorisiertem Zugriff und Diebstahl von vertraulichen Daten
  - *Schutz vor Bedrohungen* – Nutzung von Inline-Proxy-Architekturen, nativen oder integrierten Bedrohungs-Feeds und Verhaltensanalysen, um den Schaden durch Malware und infizierte Benutzerkonten zu senken
  - *Compliance* – Visibilität und Berichterstellung, sodass Sie nachweisen können, dass Branchenrichtlinien und Vorschriften zum Datenspeicherort eingehalten wurden
- **Zero-Trust-Zugriff auf das Netzwerk (Zero-trust Network Access; ZTNA)** hat das Ziel, Benutzern und genehmigten Anwendungen nur einen für ihre Zwecke angemessenen Zugriff statt umfassende Zugriffsrechte zu bieten. Anders als bei einer traditionellen VPN-Lösung, bei der ein Nutzer mit einer bestimmten IP-Adresse auf das gesamte Unternehmensnetzwerk zugreifen kann, bietet ein ZTNA einen präzisen, anpassbaren Zugriff, der die Identität des Nutzers und den Kontext berücksichtigt. Hier sind einige der Haupteigenschaften von ZTNA-Lösungen:
  - *Identitätserkennung* – Der Zugriff wird anhand der Benutzeridentität vergeben. ZTNA-Lösungen lassen sich üblicherweise in die Lösungen verschiedener Identity Provider wie Microsoft Azure Active Directory integrieren, um Identitätsinformationen zu erhalten.
  - *Kontexterkennung* – ZTNA-Lösungen berücksichtigen in Echtzeit Parameter wie die Identität des Nutzers, seinen Standort, das Endgerät, über das ein Zugriff angefordert wird, die Tageszeit, die Vertraulichkeit der angeforderten Anwendung sowie eine Risikoberechnung basierend auf den Informationen von Sicherheits- und Monitoring-Services. Das Zugriffsniveau ist anpassbar. Wenn sich die Parameter ändern, kann der Zugriff gewährt/eingeschränkt/verweigert werden.
  - *Zugriff auf Anwendungsebene* – Autorisierte Anwender erhalten einen Zugriff auf eine bestimmte Anwendung, nicht auf das zugrundeliegende Netzwerk. Dadurch wird das Risiko eingeschränkt, dass sich Malware im gesamten Unternehmensnetzwerk ausbreitet.
  - *Anwendungen sind über das Internet nicht zu sehen* – Datentransfer zwischen einem Benutzer und einer Anwendung wird über einen „Broker“ innerhalb der ZTNA-Architektur durchgeführt, ohne dass die Anwendung gegenüber dem Internet ihre IP offenlegen muss. Somit ist die Anwendung für Angreifer, die einen DDoS-Angriff oder Ähnliches planen, nicht einsehbar.

ZTNA-Lösungen minimieren die Angriffsfläche des Unternehmens und schützen sowohl Benutzer als auch Anwendungen. Da sich Benutzer nicht mehr bei einem VPN einloggen müssen und ihr Traffic nicht mehr durch die VPN-Infrastruktur geleitet wird, verbessert sich die Performance. Zu guter Letzt vereinfachen ZTNA-Lösungen die Sicherheitsarchitektur, indem die VPN-Architektur im Rechenzentrum durch einen über die Cloud bereitgestellten Service ersetzt wird. Dies verbessert die betriebliche Agilität und Effizienz.

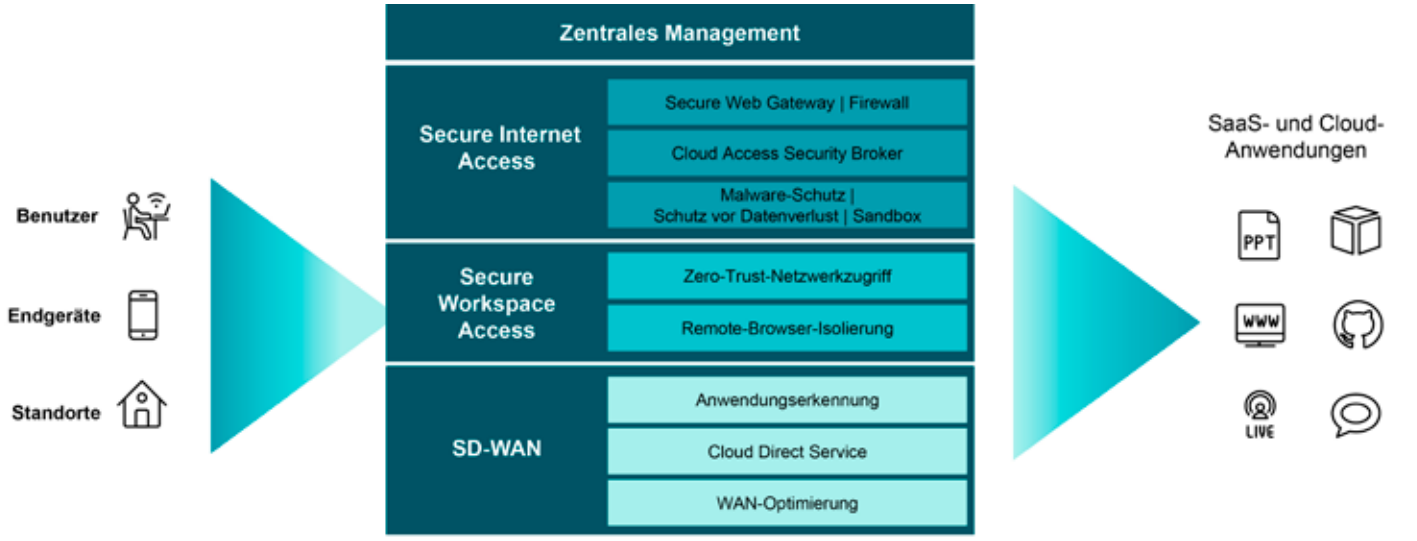
- **Firewall-as-a-Service** – Firewalls überwachen den Zugriff und filtern Inhalte zwischen dem Netzwerk und dem Internet heraus. Dies geschieht über bidirektionale Kontrollfunktionen (Ein- und Ausgang), sodass nur vertrauter, sicherer Datenverkehr passieren kann. Firewalls bieten häufig Funktionen wie Intrusion Detection/Intrusion Prevention Systeme, Malware-Schutz, Protokollierung und Berichterstellung. Zudem bieten die meisten modernen Firewalls auch Sandboxing, Standortbestimmung und eine signaturlose Bedrohungserkennung (basierend auf Anomalien). Nachfolgend werden einige dieser Funktionen erklärt:
  - *Malware-Schutz* – Prüft verschlüsselte und unverschlüsselte Web-Inhalte, um Bedrohungen zu identifizieren und zu blockieren.
  - *Intrusion Prevention/Intrusion Detection Systeme (IPS/IDS)* – IPS/IDS inspizieren Traffic und vergleichen ihn mit bekannten Signaturen, um schädliche Dateien zu identifizieren. IDS ist ein Tool für das Monitoring und die Protokollierung, das Sie benachrichtigt, wenn Malware erkannt wird. IPS geht einen Schritt weiter und blockiert potenziell schädlichen Datenverkehr automatisch.
  - *Signaturlose/anomaliebasierte Bedrohungserkennung* – Bei der anomaliebasierten Erkennung wird das Dateiverhalten bzw. ein potenzielles Verhalten mit gängigen Standardwerten verglichen (indem der Code in der Datei inspiziert wird). Beispielsweise sollte eine neu heruntergeladene Datei, die

versucht, Sicherheitskontrollen zu deaktivieren, wahrscheinlich in Quarantäne gesetzt werden.
- *Netzwerk-Sandbox* – Verdächtige Dateien werden in die Sandbox geleitet und dort in einer isolierten Umgebung ausgeführt. Wenn sich die Dateien als schädlich herausstellen sollten, werden Informationen zu den Dateien an die Firewall gesendet, welche diese dann blockiert.
- *Standortbestimmung* – IP-Adressbereiche werden der entsprechenden Region zugeteilt und der Benutzerzugriff wird anhand dieser Information gewährt/eingeschränkt/verweigert.

Firewalls werden eingesetzt, um Niederlassungen, Rechenzentren und Cloud-Instanzen des Unternehmens vor Bedrohungen zu schützen. Sie werden häufig in andere Sicherheits- und SecOps-Lösungen (für die Analyse) integriert, um eine zuverlässigere, umfangreiche „Plattform“ für das Bedrohungsmanagement zu erschaffen.

- **SD-WAN:** Softwaredefinierte WAN-Lösungen ermöglichen eine widerstandsfähige Verbindung mit geringer Latenz zwischen den verteilten Unternehmensstandorten zur Cloud und den Anwendungen im Rechenzentrum. Gleichzeitig wird die Komplexität verringert, die beim Management moderner Netzwerke mit traditionellen, routerbasierten Netzwerklösungen entsteht. SD-WAN-Funktionalität umfasst umfangreichere WAN-Edge-Funktionen wie:
  - *Pfadauswahl* – Identifikation und dynamische Steuerung von Traffic anhand von eigens festgelegten Richtlinien sowie des WAN-Zustands (Paketverluste, Verbindungsstörungen, Latenz usw.). Die Pfadauswahl stellt sicher, dass Anwender von einer einheitlichen Anwendungsperformance profitieren, auch wenn sich die Netzwerkperformance ändert.
  - *Routing* – Ermöglicht den Austausch von Routern in Niederlassungen (BGP, OSPF, Support für mehrere Topologien).
  - *Native Sicherheit* – Erstklassige Sicherheitsfunktionen, einschließlich IPS/IDS, signaturbasiertem und heuristischem Malwareschutz sowie Webfiltern. SD-WAN-Lösungen vereinfachen häufig die Einrichtung von VPN-Tunneln zwischen Zweigstellen und Cloud-Instanzen (IaaS/PaaS).
  - *Zero-Touch-Provisioning* – Durch diese Funktion kann das Provisioning und die Erstkonfiguration von SD-WAN Appliances per Remote-Zugriff von einem zentralen IT-Team vorgenommen werden. Dadurch können SD-WAN Appliances an eine Zweigstelle geliefert und einfach mit einer oder mehreren WAN-Leitungen verbunden werden, ohne dass komplexe Konfigurationen vor Ort vorgenommen werden müssen. Die SD-WAN Appliances laden Konfigurationen von der Steuerebene herunter und beginnen automatisch die Einrichtung von Tunneln zu anderen Niederlassungen und Cloud-Standorten, bei denen das SD-WAN aktiviert ist.

Der konsolidierte SASE-Ansatz von Citrix



Der SASE-Ansatz von Citrix konsolidiert Funktionen für einen sicheren und zuverlässigen Zugriff auf Anwendungen zu jeder Zeit, an jedem Ort und über jedes Endgerät

Dank der oben genannten Sicherheitsfunktionen, die mit SD-WAN konsolidiert werden, kann ein Unternehmen sein Netzwerk und seine Sicherheitsarchitekturen transformieren, um die Anforderungen der Cloud, der mobilen Nutzung und einer immer größer werdenden, diversen Belegschaft zu erfüllen.

Der konsolidierte SASE-Ansatz von Citrix

Citrix bietet eine vollständig konsolidierte SASE-Lösung, die umfassende, über die Cloud bereitgestellte Sicherheitsfunktionen in SD-WANs und Zero-Trust-Zugriffsfunktionen integriert. So können Sie Mitarbeitern einen erstklassigen Benutzerkomfort für jede Anwendung bieten, egal wo sie sich befinden oder welches Endgerät sie nutzen.

- **Über die Cloud bereitgestellte, umfangreiche Sicherheit:** Citrix Secure Internet Access (SIA) bietet umfangreiche, über die Cloud bereitgestellte Sicherheitsservices. Dazu gehören unter anderem ein Secure Web Gateway, eine Firewall der nächsten Generation, ein Cloud Access Security Broker, Malware-Informationen aus über zehn Threat Engines, Schutz vor Datenverlust, Sandboxing und KI-gestützte Analysefunktionen. SIA verfügt über mehr als 100 Knotenpunkte (Points of Presence, PoP) auf der ganzen Welt. Jeder dieser PoPs stellt jederzeit alle Services bereit. Mitarbeiter sind somit vollständig durch die umfassenden Sicherheitsfunktionen von SIA abgesichert, egal wo sie sich befinden.

Citrix Secure Internet Access bietet umfangreiche über die Cloud bereitgestellte Sicherheitsservices

- **Zero-Trust-Zugriff mit Identitätserkennung:** Citrix Secure Workspace Access bietet einen Zero-Trust-Zugriff mit Identitätserkennung auf alle vom Unternehmen genehmigten Anwendungen in einem digitalen Arbeitsplatz, um die Employee Experience auf jedem Endgerät zu optimieren. Die integrierte Remote-Browser-Isolierung schützt Endgeräte und das Unternehmensnetzwerk vor browserbasierten Angriffen. Website-Daten werden nicht direkt an das Endgerät des Anwenders gesendet. Dadurch ist die Nutzung sicher.
- **Hohe Anwendungsperformance mit SD-WAN:** Citrix SD-WAN ist eine WAN-Edge-Lösung der nächsten Generation, die eine sichere, flexible, automatisierte Verbindung herstellt, um die Performance von SaaS-, Cloud- und virtuellen

Anwendungen zu verbessern. Funktionen wie die Priorisierung von Traffic auf Paketebene mit Failovern zwischen WAN-Verbindungen in Sekundenbruchteilen und zweiseitigem QoS stellen eine hohe Anwendungsperformance sicher, unabhängig von der Netzwerkverfügbarkeit.

- **Umfassende Analyse und einfache Suche:** Die detaillierte Protokollierung aller (mobiler) Nutzer und ihrer Aktivitäten, einschließlich vollständiger URL-Informationen (nicht nur der Domain-Name) im HTTPS-Traffic ermöglicht eine einzigartige und umfassende Visibilität. KI-gestützte Engines für die Berichterstellung sammeln kritische Informationen für Berichte und Benachrichtigungen. Zusätzlich zu den integrierten Berichten können Protokolle in Echtzeit an SIEM-Lösungen exportiert werden.
- **Zentrales Management:** Citrix ermöglicht eine umfassende Integration, Automatisierung und Administration von SD-WANs und SIA über eine zentrale Oberfläche. So können Sie Ihren Betrieb auf einfache Weise vollständig managen – von der Einrichtung bis hin zum laufenden Betrieb und der Fehlerbehebung.
  - Automatisierte, „doppelt widerstandsfähige“ Verbindungen zwischen Citrix SD-WAN Standorten und Citrix SIA
  - Zentraler Einblick in die vollständige Architektur aller SD-WAN Standorte, SIA PoPs und Verbindungstunnel
  - Granulare Kontrolle, Traffic-Weiterleitung und Zuteilung der Bandbreite für SIA, Cloud Provider und andere WAN-Verbindungen, je nach geschäftlichen Anforderungen
  - Beseitigung toter Winkel durch die Integration von Berichten in der gesamten Netzwerk- und Sicherheitsarchitektur

Vorteile der Implementierung einer SASE-Architektur

SASE-Architekturen wurden mit dem Ziel entwickelt, mobilen und Remote-Nutzern einen schnellen, zuverlässigen und sicheren Zugriff auf Cloud-Anwendungen zu bieten, während gleichzeitig die IT-Agilität verbessert wird. Wenn Unternehmen darauf achten, dass bestimmte Funktionen verfügbar sind, z. B. das zentrale Management aller Netzwerk- und Sicherheitsfunktionen, die Single-Pass-Architektur und die leistungsstarken SD-WAN Funktionen, können sie mit einer SASE-Lösung von den folgenden Vorteilen profitieren:

- **Verbesserte Performance, Zusammenarbeit und Produktivität** – Der direkte Internetzugang beseitigt Latenz, da Traffic nicht mehr durch das Rechenzentrum geleitet werden muss. Jedoch müssen SASE-Lösungen Optimierungen für SD-WAN und WAN anbieten, damit auch bei wechselhaften Internetverbindungen eine konstante Performance sichergestellt ist. Eine Single-Pass-Architektur stellt sicher, dass Traffic-Inspektionen und das Anwenden von Richtlinien keine zusätzliche Latenz erzeugen.
- **Verbesserte Sicherheit, unabhängig vom Standort des Mitarbeiters** – Für genehmigte Anwendungen ist ein Zero-Trust-Zugriff mit Identitätserkennung aktiviert. Dies verringert die Angriffsfläche und beugt einer Verbreitung von Malware innerhalb des Unternehmensnetzwerks vor. Für ungenehmigte sowie Web-Anwendungen gibt es umfangreiche, über die Cloud bereitgestellte Sicherheitsfunktionen, die für ein einheitliches, hohes Sicherheitsniveau sorgen, egal wo sich der Mitarbeiter befindet.
- **Vereinfachter Betrieb mit gesteigerter IT-Agilität** – SASE-Architekturen konsolidieren Netzwerk- und Sicherheitslösungen verschiedener Anbieter. Lösungen von einem einzigen Anbieter bieten bessere Integrationsmöglichkeiten sowie ein zentrales Management. Dies vereinfacht die Implementierung, Konfiguration, Berichterstellung und Support-Services. Da SASE-Architekturen eine Migration der Sicherheitsfunktionen in die Cloud erfordern, ist insgesamt weniger Hardware erforderlich, was wiederum die Elastizität und Skalierbarkeit der Architektur verbessert.

Erste Schritte

Wie bei jeder revolutionären Technologie werden einige Unternehmen SASE-Architekturen früher einführen als andere. Der Austausch traditioneller Hub-and-Spoke-Architekturen oder älterer VPN-Technologien, die Migration von Anwendungen in die Cloud, einheitliche Sicherheit für Remote-Mitarbeiter oder der Wunsch nach einer höheren Mitarbeitermotivation sind nur einige der Gesprächsthemen, über die Sie auf SASE zu sprechen kommen können.

Die Möglichkeit, Netzwerk- und Sicherheitsarchitekturen neu zu gestalten, wird Early Adoptern deutliche Vorteile bieten. Sie können den Unternehmenserfolg nachweislich verbessern, z. B. durch eine bessere betriebliche Performance, eine Senkung der Kosten oder die Verbesserung der Mitarbeitermotivation und der Kundenzufriedenheit. Um diese Transformation einzuleiten, müssen Unternehmen sich für den richtigen Technologiepartner entscheiden.

Citrix vereint alle SASE-Services, einschließlich Netzwerk- und Sicherheitsfunktionen, mit umfangreichen Integrationsmöglichkeiten, Automatisierung und einer zentralen Administrationsoberfläche. 400.000 Organisationen

vertrauen Citrix bereits dabei, eine bessere Art zu arbeiten zu ermöglichen. Wir können auch Sie dabei unterstützen, Ihr Netzwerk und Ihre Sicherheitsumgebung zu transformieren.

Weitere Informationen finden Sie unter *www.citrix.de/secure-internet*.

Fußnoten

1 Basierend auf den eigenen Berechnungen von Citrix. Pressemitteilung von Gartner vom 23. Juli 2020, Gartner prognostiziert für 2020 einen Anstieg des weltweiten Public Cloud-Umsatzes um 6,3 %. https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

2 Umfrage zur Remote-Arbeit von PwC, Juni 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

3 Umfrage zur Remote-Arbeit von PwC, Juni 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

4 Bericht zu den Kosten eines Datenverstoßes 2020, IBM, https://www.ibm.com/security/data-breach

5 Workforce Pulse Survey von PwC, https://www.pwc.com/us/en/library/covid-19/workforce-pulse-survey.html

6 Global Digital Trust Insights 2021 von PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/global-digital-trust-insights/cyber-defense-technology.html

Enterprise Sales
Nordamerika | 800-424-8749
Weltweit | +1 408 790 8000

Standorte
Unternehmenszentrale | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, USA
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, USA