aruba
a Hewlett Packard Enterprise company

EBOOK

Edge-to-Cloud-Sicherheit: Ein neues WAN- und Security-Edge

Eine praktische Anleitung zur Einführung einer SASE-Architektur (Secure Access Service Edge)

Die digitale Transformation und das Work From Anywhere (WFA) auf WAN und Sicherheit in einer cloudzentrierten Welt

Da Organisationen noch immer mit den Herausforderungen der COVID-19-Pandemie und der neuen WFA-Routine (Work from Anywhere) kämpfen, beschleunigt sich weiterhin auch die Einführung von Diensten, die in der Cloud gehostet werden. Durch diesen Trend steigt die Dringlichkeit, konventionelle Rechenzentren sowie MPLS-zentrierte und VPN-basierte Netzwerke in einem nativen Cloud-SASE (Secure Access Service Edge) zu transformieren, das sichere Netzwerkdienste dynamischer bereitstellt und Daten im gesamten Netzwerk durchgehend schützt.

Diese drei Fragen müssen sich IT-Verantwortliche bei der Sicherung des WAN in erster Linie stellen:

- Wie kann ich sicherstellen, dass ich die richtige SD-WAN-Architektur wähle, um Geschäftsanwendungen in einer Cloud-first-Umgebung sicher zu gewährleisten?
- Wie beeinflusst eine dauerhafte WFA-Hybridumgebung IT-Entscheidungen bei der Einführung einer sicheren Architektur in ein SASE-Framework?
- Wie kann die IT-Abteilung den Sicherheitsproblemen begegnen, die durch die Verbreitung von IoT-Geräten ohne Agent entstehen?

Wir untersuchen hier, wie sich die Netzwerk- und Sicherheitsanforderungen in einer cloudzentrierten Welt ändern.

50 %
der Befragten führen 2021 gegenwärtig verschiedene Initiativen zur digitalen Transformation durch, im Vergleich zu 38 % im Jahr 2020.[1]

45 %
der Unternehmen verfügen über eine Cloud-First-Richtlinie.[2]

1, 2. Umfrage zu geplanten IT-Technologieausgaben von ESG, Dezember 2020

Zero-Trust, ZTNA und SASE in einer cloudzentrierten Welt

Bei der Entwicklung herkömmlicher Sicherheitslösungen spielte die Cloud keine Rolle. Das Konzept, den Datenverkehr in ein zentrales Rechenzentrum zurückzuführen, funktionierte, als sich alle Anwendungen auch dort befanden. Bei zunehmendem Datenverkehr von Benutzern in Zweigniederlassungen und Anwendungen, die in die Cloud verlagert werden, führt die Rückführung von Datenverkehr in einem älteren Hub-and-Spoke-Netzwerk zu einer schlechten Benutzererfahrung, mehr Sicherheitsrisiken und höheren Kosten.

Ältere Netzwerk-Sicherheitslösungen verfügen vermutlich noch nicht über das Konzept von Zero-Trust, einem IT-Sicherheitsmodell für die Identitäts- und Zugriffsverwaltung. Es basiert auf der Annahme, dass Benutzer oder Software erst nach einer Authentifizierung als vertrauenswürdig angesehen werden. Anders ausgedrückt, alles wird authentifiziert und der Zugriff dann auf die Anwendungen und Daten beschränkt, die mit der Rolle des Benutzers oder Geräts übereinstimmen. Bei Zero-Trust müssen alle Benutzer, Geräte und Anwendungsinstanzen nachweisen, dass sie das sind, was sie zu sein vorgeben, und dass sie berechtigt sind, auf die gewünschten Ressourcen zuzugreifen. Dabei spielt es keine Rolle, ob sie sich vor oder hinter dem Netzwerkperimeter befinden.

Zero Trust Network Access (ZTNA) besteht aus einer Reihe von Technologien in einem Zero-Trust-Framework. Der Zugriff wird hier streng bedarfsorientiert nach genau abgestimmten Richtlinien und mit minimalen Berechtigungen gewährt. ZTNA ermöglicht es Benutzern, eine nahtlose und sichere Verbindung mit privaten Anwendungen herzustellen, ohne diese im Netzwerk bereitzustellen oder Apps im Internet offenzulegen.

Schließlich gibt es noch SASE – ein neuer Begriff, der von Gartner geprägt wurde. SASE definiert eine Edge-Architektur, die umfassende WAN-Funktionen mit umfassenden Netzwerk-Sicherheitsfunktionen der Cloud kombiniert: Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), ZTNA und vieles mehr.

Herausforderungen bei WAN und Netzwerksicherheit

In der cloudzentrierten Welt von heute sind WAN- und Netzwerk-Sicherheitsanforderungen enger miteinander verbunden als je zuvor. Um das vollständige Potenzial der digitalen Transformation auszuschöpfen, müssen Unternehmen WAN- und Sicherheitsarchitektur transformieren sowie Geschäftsanwendungen unterstützen, die an jedem beliebigen Ort und über jedes Transportnetzwerk gehostet werden können und auf die von überall aus zugegriffen werden kann.

Das sind die vorrangigen Sicherheits- und WAN-Herausforderungen, mit denen Unternehmens-IT und Netzwerkteams konfrontiert sind:

- Wie lassen sich die geschäftlichen und betrieblichen Vorteile der Cloud nutzen und gleichzeitig ein hohes Maß an Sicherheit bei einem minimalen Gesamtrisiko aufrechterhalten werden?
- Wie kann eine einheitliche Benutzererfahrung von hoher Qualität bei allen in der Cloud gehosteten Geschäftsanwendungen im gesamten WAN sichergestellt werden?
- Wie können einheitliche Richtlinien für den Netzwerkzugriff eingeführt und umgesetzt werden, wenn Mitarbeiter in einer hybriden Umgebung (Büro und Zweigniederlassung) oder an einem beliebigen Ort (WFA) arbeiten?
- Wie lassen sich Sicherheit und WAN-Konnektivität so vieler unterschiedlicher Endgeräte, Benutzer und Anwendungen aufrechterhalten?
- Kann die Wahl der richtigen SD-WAN-Plattform die Integration der WAN- und Netzwerksicherheit verbessern?
- Kann ein einziger Anbieter alle benötigten Sicherheitsdienste liefern?

Integration von SD-WAN-Anwendungs- und Sicherheitsrichtlinien

Im schnelllebigen globalen Markt von heute müssen Unternehmen agil sein, um schnell neue Zweigniederlassungen einrichten und Richtlinien sowie Sicherheitsregeln dynamisch anpassen zu können. Auch die Weitergabe von Richtlinien ist bei der Automatisierung von Zweigniederlassungen entscheidend, ebenso wie die nötige Schlüsselfunktion, die nur eine fortschrittliche SD-WAN-Lösung liefern kann – wie die Edge-Plattform EdgeConnect SD-WAN von Aruba.

Eine fortschrittliche SD-WAN-Lösung kann den Einsatz mehrerer Appliances für Unternehmen überflüssig machen, da wichtige WAN-Edge-Funktionen für Zweigniederlassungen vereinheitlicht werden:

- SD-WAN
- Routing
- Zonenbasierte Firewall und Segmentierung
- Unified Threat Management (UTM)
- Transparenz und Steuerung von Netzwerk und Anwendungen
- WAN-Optimierung

Eine Konsolidierung dieser Funktionen vereinfacht oder „verschlankt“ das WAN-Edge von Zweigniederlassungen. Die zentrale Verwaltung steigert außerdem die Effizienz der IT erheblich und ermöglicht eine einheitliche Umsetzung von Quality of Service(QoS)- und Sicherheitsrichtlinien.

Die zentrale SD-WAN-Orchestrierung von Aruba EdgeConnect vereinheitlicht die Konfiguration und laufende Verwaltung. Darüber hinaus wird sichergestellt, dass QoS und Sicherheit einheitlich bei Anwendungen oder Anwendungsklassen umgesetzt werden, unabhängig davon, wo oder wie auf sie zugegriffen wird. Die Performance und Sicherheit von Anwendungen kann mithilfe von Top-Down-Geschäftsrichtlinien gewährleistet werden, anstatt durch die Beschränkungen von Bottom-Up-Technologien.

Wie SD-WAN für einheitlichere Sicherheit sorgt

Eine SASE-Architektur, die Cloud-Sicherheit mit einer fortschrittlichen SD-WAN-Lösung kombiniert, vermeidet Kosten und Komplexitäten, die bei der Verwaltung mehrerer Next-Generation-Firewalls an einem Standort entstehen. Das Modell erfordert zur Abwehr eingehender Bedrohungen dennoch eine zustandsbehaftete zonenbasierte Firewall für die Standorte der Zweigniederlassungen.

Die EdgeConnect-Plattform umfasst:

- Intelligenz und die Fähigkeit zur Erkennung von Anwendungen mit Zugriffsgenehmigung für einen direkten Zugriff auf Ressourcen in der Cloud
- Automatisierte Integration und Orchestrierung von Cloud-Sicherheitsanbietern aus Zweigniederlassungen zum nächsten Point of Presence (PoP)

Entscheidende Vorteile:

- Geringere Latenz
- Optimierte Anwendungsleistung
- Unterstützung höchster Qualität bei vertrauenswürdigen SaaS-Anwendungen

Die Integration von Aruba Threat Defense in die Aruba EdgeConnect SD-WAN-Edge-Plattform erweitert die fortschrittlichen IDS/IPS-Funktionen (Intrusion Detection and Prevention) für das SD-WAN. Die physischen und virtuellen Appliances von EdgeConnect nutzen die Infrastruktur zur Gefahrenabwehr sowie Bedrohungsdaten von Aruba und ermöglichen es Unternehmen, eine laterale Ost-West-Sicherheit und sichere lokale Internet-Breakouts für Zweigniederlassungen zu schaffen. Die Bereitstellung kann zentral, vor Ort oder in der Cloud erfolgen. Das Bedrohungsprotokoll sendet Netzwerk- und Sicherheitsanalysen an Aruba Central und stellt umfassende Edge-to-Cloud-UTM-Funktionen bereit.

Zero-Trust: Sicherung des Edge nach Rolle, Kontext und Anwendung

Durch die steigende Zahl von Mobilgeräten, Remotemitarbeitern, Cloudanwendungen und Internet of Things(IoT)-fähigen Geräten müssen Unternehmen, Business Intent ausgerichtete Netzwerk- und Sicherheitsrichtlinien anpassen.

Die Integration der identitätsbasierten Zugriffssteuerung von Aruba ClearPass Policy Manager in die Aruba EdgeConnect SD-WAN-Plattform steigert die Anwendungsintelligenz durch ergänzende Daten zu Nutzeridentitäten, Geräten, Rollen sowie Sicherheitslagen und schafft das Fundament für ein sicheres WAN-Edge.

Diese neue Kontextebene ermöglicht eine detaillierte Segmentierung der Gerätetypen anhand der Rolle in der Organisation ohne die Komplexität, die die Verwaltung Tausender von VLANs mit sich bringt. Beispielsweise kann eine detaillierte Segmentierungsrichtlinie definiert werden, die verhindert, dass Sicherheitskameras auf die Verarbeitung von Kreditkartentransaktionen oder auf HLK-Anlagen zugreifen können. Es könnte auch verhindert werden, dass Sicherheitskameras mit der Überwachungskopfstation oder einem Aufzeichnungsgerät kommunizieren können, andere Kameras jedoch schon. Dadurch kann die IT-Abteilung die Einhaltung der Anwendungssicherheit und von Sicherheitsaudits besser verwalten. Zudem werden Gefahrenprotokolle generiert, die in eine Security Information and Event Management(SIEM)-Anwendung Dritter exportiert werden können.

57 %

der Befragten geben an, dass in ihrer Organisation Zero Trust bereitgestellt wird oder werden soll.[3]

49 %

der Befragten geben an, dass in ihrer Organisation eine SASE-Architektur bereitgestellt wird oder werden soll.[4]

71 %

der Befragten würden sich bei der Bereitstellung von SD-WAN und cloudbasierter Sicherheit für eine SASE-Architektur für den besten Anbieter entscheiden[5]

3, 4, 5. Ponemon Institute, The State of SD-WAN, SASE and Zero Trust Security Architectures, April 2021

ClearPass: Sicherung des IoT mit fortschrittlichem SD-WAN

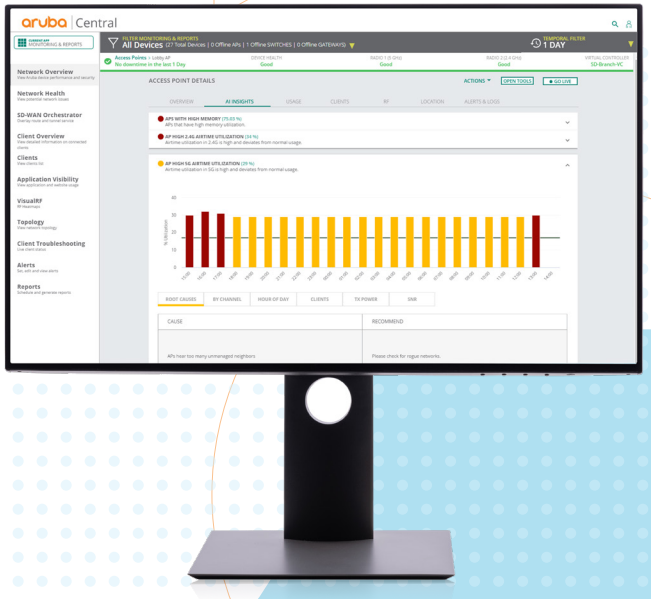
Smartphones, Laptops oder Tablets können mit ZTNA-Softwareagenten gesichert werden. Sicherheits-Softwareagenten können jedoch nicht auf IoT-Geräten installiert werden, da diese keine Agenten besitzen. Dadurch entsteht ein Sicherheitsproblem, das SASE nicht unmittelbar behebt.

Eine Aruba EdgeConnect SD-WAN-Plattform kann das Risiko durch Sicherheitsverstöße bei der Bereitstellung von IoT-Geräten reduzieren. Die EdgeConnect-Plattform identifiziert und klassifiziert den Anwendungsdatenverkehr des ersten Pakets, fängt ihn am Netzwerk-Edge ab und weist ihn dem entsprechenden Segment zu. Durch diese grobe Segmentierung wird er von anderem Datenverkehr im Netzwerk isoliert.

ClearPass-Integration mit EdgeConnect ergänzt die Anwendungsintelligenz durch rollenbasierte Richtlinien zur Benutzer- sowie Geräteidentität und ermöglicht eine detaillierte Segmentierung. Der zusätzliche identitätsbasierte Kontext ermöglicht eine einheitliche Durchsetzung von Sicherheitsrichtlinien im gesamten Netzwerk, vom Edge bis hin zur Cloud.

Aruba Zero Trust mit dynamischer Segmentierung hilft Unternehmen dabei, Bedrohungen nach Endgerät, Rolle und Anwendung zu identifizieren und gleichzeitig Compliance-Standards der Branche einzuhalten, z. B. PCI, HIPAA und SOX.

Die Kombination aus fortschrittlichem SD-WAN und Cloudsicherheit mit richtlinienbasiertem ZTNA stellt sicher, dass das WAN, Benutzer, Endgeräte und Anwendungen des Unternehmens stets sicher sind.



Best-of-Breed-WAN und -Sicherheit – ohne Wenn und Aber

Da zentral orchestrierte und in der Cloud gehostete Best-of-Breed-Sicherheitsdienste Sicherheits- und Kostenproblemen begegnen, erfreuen sie sich zunehmender Beliebtheit. Zentral verwaltete Cloudsicherheitsdienste schützen alle Benutzer. Sie werden durch einheitliche Richtlinien und die Durchsetzung der Richtlinien an Hunderten oder sogar Tausenden von Standorten unterstützt – ohne die Komplexität, die die Bereitstellung und Verwaltung physischer Sicherheitsappliances mit sich bringt.

Fortschrittliche SD-WAN-Lösungen wie die Edge-Plattform EdgeConnect SD-WAN von Aruba ermöglichen Unternehmen intelligente Breakouts für Clouddatenverkehr von Zweigniederlassungen über das Internet. Sie unterstützen außerdem Mikrosegmentierungsfunktionen und eine detaillierte Durchsetzung von Richtlinien, sodass Unternehmen das WAN sichern, Compliance-Verpflichtungen einhalten und Verstöße abwehren können.

Die automatisierte Orchestrierung eines branchenführenden Cloud-sicherheitsdienstes mit der anwendungsorientierten Aruba EdgeConnect SD-WAN-Edge-Plattform bietet eine leistungsstarke SASE-Lösung ohne Einschränkung der Netzwerkfunktionalität oder der Sicherheitsfunktionen.

SASE schützt Unternehmen vor Bedrohungen und liefert optimale Anwendungsperformance sowie Benutzererfahrung bei überschaubaren Kosten.

Vorteile dieser Verbindung aus SD-WAN und Cloudsicherheit:

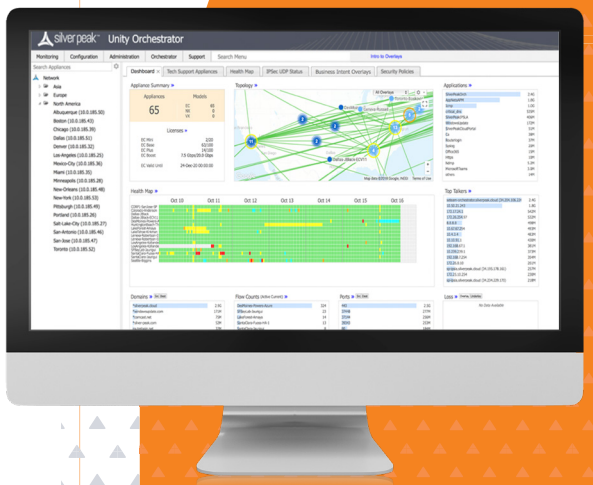
- Höhere Unternehmensagilität und vereinfachte IT-Richtlinien mit einer SASE-Architektur, die alle Vorteile der Cloud bietet
- Vereinfachte und rationalisierte Integration von cloudnativen Sicherheitsfunktionen mit optimierten SD-WAN-Funktionen
- Wahlfreiheit bei der Best-of-Breed-Netzwerksicherheit und Best-of-Breed-SD-WAN-Funktionen
- Keine Bindung an einen Anbieter
- Verzicht auf teure und komplexe Next-Generation-Firewalls für jede Zweigniederlassung
- Flexibilität zur Einführung künftiger Sicherheitsinnovationen

Cloudbasierte Sicherheitsautomatisierung mit SD-WAN

Unternehmen suchen nach einfacheren Wegen, Anwendungen im WAN sowie in die Sicherheitsinfrastruktur zu integrieren und zu verwalten. Am einfachsten lassen sich cloudbasierte Sicherheitsdienste an Zweigniederlassungen unter anderem durch Automatisierung mit Aruba Edge Connect SD-WAN orchestrieren.

EdgeConnect verwendet Application Programmable Interfaces (APIs) und eine Dienstorchestrierung Dritter für die Integration in führende Cloudsicherheitsanbieter wie ZScaler, Check Point, NetSkope und Palo Alto Prisma Access. Aruba Orchestrator validiert die zur Anmeldung verwendeten Cloudsicherheitsdaten und automatisiert oder orchestriert das Herstellen der Verbindung der Zweigniederlassungen in der SD-WAN-Fabric mit den nächsten primären und optionalen sekundären PoPs, die der Durchsetzung der Cloudsicherheit dienen.

Die Konfiguration von Sicherheitsrichtlinien ist ein einfacher Drag-and-Drop-Vorgang in der intuitiven Benutzeroberfläche von Aruba Orchestrator. Organisationen können eine Reihe von Sicherheitsrichtlinien festlegen, die sich in einem einzigen Vorgang auf alle Zweigniederlassungen anwenden lassen.



Flexibilität und Wahlfreiheit

Das sich die Bedrohungslandschaft ständig weiterentwickelt, müssen Unternehmen agil bleiben und in der Lage sein, schnell und kosteneffektiv neue Sicherheitslösungen einzuführen. Sie sollten Plattformen in Erwägung ziehen, die ihnen die Wahl lassen, Best-of-Breed-Netzwerklösungen und -Sicherheitslösungen zu integrieren. So können sie vermeiden, dass sie an proprietäre Lösungen eines einzigen Anbieters gebunden sind oder sich mit Basisfunktionen und -fähigkeiten zufriedengeben müssen.

Die unternehmensorientierte Aruba Edge Connect SD-WAN-Plattform ist eine tragende Säule einer Best-of-Breed-SASE-Architektur. Sie ermöglicht die Integration einer Best-in-Class-SD-WAN-Plattform in eine Vielzahl von Best-in-Class-Cloud-Sicherheitsdienste. Aruba EdgeConnect unterstützt grundlegende Sicherheitsfunktionen, die in der Zweigniederlassung erforderlich sind, und ergänzt die Cloudsicherheit, sodass im gesamten Unternehmen ein sicheres Edge für einen nahtlosen Zugriffsdienst verfügbar ist.

Weitere Informationen finden Sie unter www.arubanetworks.com/sdwan

eBook_Aruba-Edge-to-Cloud-Security_DC_062321 a00114994enw

aruba
a Hewlett Packard Enterprise company