HPE aruba networking

Business-Whitepaper

SASE-Architektur mit einem sicheren, geschäftsorientierten SD-WAN

HPE GreenLake

Inhaltsverzeichnis

3 Kurzübersicht

4 Warum SD-WAN für die Sicherheit von entscheidender Bedeutung ist

6 Vorstellung von EdgeConnect SD-WAN von HPE Aruba Networking

7 So ermöglicht EdgeConnect SD-WAN ein sicheres SD-WAN

7 Anwendungsorientierte Sicherheit auf Datenebene

12 Unified SASE mit HPE Aruba Networking

13 Integration mit mehreren SASE-Partnern

14 Sicherheit auf Management- und Systemebene

15 Sicherheitszertifizierung und Compliance

16 Fazit

Erfahren Sie, wie die sichere HPE Aruba Networking EdgeConnect SD-WAN-Plattform erstklassigen Schutz bietet, und beschleunigen Sie Ihren Wandel zu SASE

Kurzübersicht

Softwaregesteuerte Wide Area Networks (SD-WAN) ermöglichen es den geografisch verteilten Unternehmen von heute, das Transformationsversprechen des Cloud Computings zu verwirklichen, Kapital- und Betriebskosten zu senken, Mitarbeitenden und Kunden die bestmögliche Qualität zu bieten und sich schnell an veränderte Geschäftsanforderungen anzupassen.

Doch durch digitale Transformation, Cloud Computing und hybride Arbeitsmodelle entstehen auch völlig neue Sicherheitsherausforderungen. Dazu gehören:

- Benutzer verbinden sich von überall und von jedem Gerät aus
- Ständig wachsende Cybersicherheitsrisiken
- Mehr vertrauliche Daten werden in der Cloud gehostet
- Die Verbreitung von IoT-Geräten vergrößert die Angriffsfläche
- Einhaltung von Vorschriften und Industriestandards

Ein wesentlicher Vorteil eines SD-WAN ist die Möglichkeit, kostengünstige Breitbandservices aktiv zu nutzen. Da es sich bei Breitbandservices jedoch um „öffentliche“ und nicht um „private“ Dienste handelt, sind fortschrittliche Sicherheitsfunktionen erforderlich, um die Vertraulichkeit und Integrität des Anwendungsverkehrs zu gewährleisten, der über solche Verbindungen läuft. Mittels einer integrierten Firewall bieten sichere SD-WANs fortschrittliche Sicherheit in Filialen. Diese umfasst IDS/IPS und DDoS-Schutz und isoliert IoT-Datenverkehr von geschäftskritischen Anwendungen. Sie segmentiert Netzwerke in verschiedene Zonen und verkleinert die Angriffsfläche, um die Einhaltung von Industriestandards zu unterstützen.

Außerdem sehen sich Unternehmen, die einen Großteil ihrer Geschäftsanwendungen in die Cloud verschieben, mit neuen Herausforderungen konfrontiert. So müssen sie beispielsweise Remote-Mitarbeitenden einen sicheren Zugriff zur Verfügung stellen, Internetbenutzer vor Bedrohungen aus dem Web schützen und sicherstellen, dass vertrauliche Unternehmensdaten, die in Cloud-Anwendungen gehostet werden, geschützt bleiben und nicht durch Datenlecks offengelegt werden.

Durch eine enge Integration in SSE-Lösungen (Security Service Edge) bildet ein modernes, sicheres SD-WAN eine robuste SASE-Architektur, die es Unternehmen ermöglicht, die Herausforderungen von hybriden Arbeitsmodellen und Cloud Computing zu bewältigen.

In diesem Dokument wird behandelt, warum SD-WAN von kritischer Bedeutung für die Sicherheit ist, und wie eine umfassende SD-WAN-Sicherheitsimplementierung die dynamischen Cloud-First-Unternehmen von heute besser schützen kann. Anschließend werden die umfassenden integrierten Sicherheitsfunktionen der HPE Aruba Networking EdgeConnect SD-WAN-Plattform besprochen, einschließlich einer Next-Generation Firewall. Ebenso erfahren Sie, wie sich die SD-WAN-Plattform eng mit SSE-Funktionen (Security Service Edge) integrieren lässt, entweder mit HPE Aruba Networking SSE, um eine einheitliche SASE-Lösung (Secure Access Service Edge) zu bilden, oder mit externen Cloud-Sicherheitsanbietern.

Netzwerksicherheit in der Cloud-Ära

„Hybride Arbeitsmodelle und die unermüdliche Umstellung auf Cloud Computing haben die SASE-Einführung beschleunigt.“

– Gartner 2022[1]

Da immer mehr Anwendungen und Workloads in die Cloud migriert werden, hat sich die Bedeutung des Rechenzentrums eines Unternehmens deutlich verringert. Durch hybride Arbeitsmodelle löst sich auch der Sicherheitsperimeter zunehmend auf, da sich die Benutzer von verschiedensten Orten und Geräten aus verbinden und auf vertrauliche Daten in der Cloud zugreifen.

Unternehmen, die versuchen, WANs mit herkömmlichen Routern zu verwalten, müssen immer wieder Kompromisse eingehen und abwägen. Manuelle Prozesse und komplexe Architekturen hindern Unternehmen daran, eine sichere Architektur aufzubauen und effektiv auf Bedrohungen wie DoS-Angriffe (Denial of Service) zu reagieren. Sicherheitsbedenken können die Nutzung von kostengünstigen Breitbandverbindungen behindern und die Umstellung auf die Cloud im Allgemeinen und auf SaaS-Anwendungen im Besonderen verlangsamen.

[1] Top Trends Impacting Infrastructure and Operations for 2023, Gartner, Dezember 2022

Diese Veränderungen haben zur Folge, dass sich auch die WAN-Architektur des Unternehmens ändern muss. Im August 2019 definierte Gartner „Secure Access Service Edge“ (SASE) als die Kombination von fortschrittlichen WAN-Edge-Netzwerkfunktionen mit Netzwerksicherheitsfunktionen wie SWG, CASB, FWaaS und ZTNA, die in der Cloud bereitgestellt werden. Eine SASE-Architektur bietet eine sicherere und flexiblere Möglichkeit, sich mit in der Cloud gehosteten Anwendungen zu verbinden, da der Anwendungsverkehr vor der Weiterleitung in die Cloud nicht in ein Rechenzentrum umgeleitet wird.

Mit einer SASE-Architektur kann das SD-WAN den Anwendungsverkehr direkt zu einem vertrauenswürdigen SaaS-Anbieter oder zunächst zu einem in der Cloud gehosteten Sicherheitsservice leiten, wo vor der Weiterleitung an den SaaS-Anbieter erweiterte Sicherheitsprüfungen im Einklang mit den Sicherheitsrichtlinien des Unternehmens durchgeführt werden können.

Herkömmliche Konnektivitätsoptionen für private Leitungen (z. B. Multi-Protocol Label Switching, MPLS) und Routing-Praktiken – insbesondere Backhauling – sind für Cloud-basierte Anwendungen eindeutig ungeeignet. Zu den wichtigsten Defiziten gehören die negativen Auswirkungen auf die Leistung (insbesondere bei Internet- oder Cloud-Datenverkehr), die hohen Kosten solcher Netzwerkservices und -architekturen sowie die Tatsache, dass sie die Wartung einer Vielzahl von Sicherheitsgeräten in den Filialen erfordern.

Die Verbreitung von IoT-Geräten (Internet of Things – Internet der Dinge) ist zu einem weiteren wichtigen Problem für Unternehmen geworden, das die Angriffsfläche erheblich vergrößert. Aufgrund ihres einfachen Designs können diese Geräte in der Regel keinen Sicherheitsagenten beherbergen und sind daher nicht leicht zu schützen. Aus diesem Grund benötigen Unternehmen für IoT-Geräte eine andere Sicherheitslösung, um Unternehmensnetzwerke vor potenziellen Bedrohungen zu schützen, die in das Netzwerk eindringen könnten. Daher muss SASE durch ein Zero-Trust-Sicherheits-Framework ergänzt werden, das auf der Identitätsgrundlage den Datenverkehr dynamisch segmentiert, sodass Anwender und IoT-Geräte nur Netzwerkziele erreichen können, die ihrer Rolle im Unternehmen entsprechen.

Warum SD-WAN für die Sicherheit von entscheidender Bedeutung ist

Starke Sicherheit ist eine Voraussetzung und ein integraler Bestandteil vieler Vorteile eines geschäftsorientierten SD-WAN. So ist beispielsweise die Nutzung von Breitbandinternet als kostengünstige Konnektivitätsoption ein zentraler Bestandteil des SD-WAN-Wertversprechens. Die Tatsache, dass Breitband „öffentlich“ und nicht „privat“ ist, führt jedoch zu der Notwendigkeit, die Vertraulichkeit und Integrität des Anwendungsverkehrs, der über solche Verbindungen läuft, zu gewährleisten. Nicht zu vergessen ist auch, dass SD-WAN-Geräte bei der Inline-Implementierung „in der Schusslinie“ stehen – zumindest im Vergleich zum Szenario, in dem ein herkömmlicher WAN-Optimierer in einer Out-of-Path-Konfiguration implementiert wird.

Backhauling und lokaler Internet-Breakout

Beim Backhauling wird der Anwendungsverkehr einer Filiale, der für das Internet bestimmt ist (oder von dort zurückkehrt), über eine WAN-Verbindung zwischen der Filiale und dem Hauptsitz des Unternehmens weitergeleitet. Auf diese Weise kann der Anwendungsverkehr von den Sicherheitskontrollen und -maßnahmen profitieren, die am Standort der Zentrale eingerichtet wurden, bevor er ins Internet geleitet wird. Das Backhauling des Anwendungsverkehrs führt jedoch aufgrund der zusätzlichen Latenzzeit zu einer schlechten Leistung. Die Alternative, die als lokaler Internet-Breakout bezeichnet wird, besteht darin, dass ausgewählter Anwendungsverkehr von Filialen direkt zum/vom Internet geleitet wird (d. h. ohne das WAN zu durchqueren und eine Reihe von zentral bereitgestellten Sicherheitstools zu durchlaufen, bevor er schließlich die Cloud-basierte Anwendung erreicht).

Obwohl ein lokaler Internet-Breakout für die Verbesserung der Leistung und die Verringerung der für das Backhauling benötigten Bandbreite von entscheidender Bedeutung ist, setzt er die Benutzer in den Filialen und ihre lokalen Netzwerke direkt dem Internet und seinen unzähligen Bedrohungen aus. Sie brauchen also eine Möglichkeit, ausgehende Ziele zu begrenzen, unerwünschten/unaufgefordert eingehenden Datenverkehr zu blockieren und erlaubten/erwarteten Datenverkehr nach Bedrohungen zu filtern.

Allerdings sind nicht alle Webanwendungen gleich, und ein Teil des Webverkehrs kann das Unternehmen für Viren, Trojaner, DDoS-Angriffe und andere Schwachstellen anfällig machen. Daher muss auch der direkte Internet-Zugang sicher sein. Eine Sicherheitsrichtlinie für den Webverkehr könnte zum Beispiel wie folgt definiert werden:

- Sende bekannten, vertrauenswürdigen Unternehmens-SaaS-Datenverkehr, z. B. Sprach- und Videodatenverkehr (Unified Communications-as-a-Service, UCaaS) direkt an das Internet.
- Sende sämtlichen sonstigen Webverkehr an eine SSE-Lösung (Security Service Edge).
- Sende den im Rechenzentrum des Unternehmens gehosteten Anwendungsverkehr direkt an die Zentrale.

Um eine solche Richtlinie umzusetzen, muss der Webverkehr präzise an das gewünschte Ziel geleitet werden. Dies erfordert die Identifizierung der Anwendung im ersten Paket, da eine einmal aufgebaute Anwendungssitzung nicht an ein anderes Ziel umgeleitet werden kann, ohne den Datenfluss zu unterbrechen, was zu einer Unterbrechung der Anwendung führt. Und da sich die von SaaS-Anwendungen genutzten IP-Adressbereiche fast ständig ändern, müssen die Adresstabellen automatisch und täglich aktualisiert werden.

Intelligente und sichere Steuerung des Datenverkehrs

Obwohl es sich nicht um eine Sicherheitsfunktion im eigentlichen Sinne handelt, spielt die EdgeConnect First-packet iQ™-Klassifizierung eine wichtige Rolle für die Gesamteffizienz der HPE Aruba Networking SD-WAN-Plattform. Durch die Identifizierung von Anwendungen beim ersten Paket einer Sitzung wird eine anwendungsorientierte Steuerung des Datenverkehrs ermöglicht, die nicht nur eine effiziente Nutzung der WAN-Ressourcen gewährleistet, sondern auch die automatische Durchsetzung von Sicherheitsrichtlinien unterstützt.

So kann beispielsweise mit First-packet iQ vertrauenswürdiger SaaS- und Webverkehr direkt an das Internet gesendet werden (ohne Leistungseinbußen und Kosten für Backhauling), während sonstiger Datenverkehr an eine SSE-Lösung (Security Service Edge) oder an Sicherheitsservices des Unternehmens gesendet wird. Die zuvor beschriebenen automatisierten SaaS-IP-Adressaktualisierungen stellen sicher, dass der Anwendungsverkehr gemäß den definierten Sicherheitsrichtlinien korrekt geleitet wird.



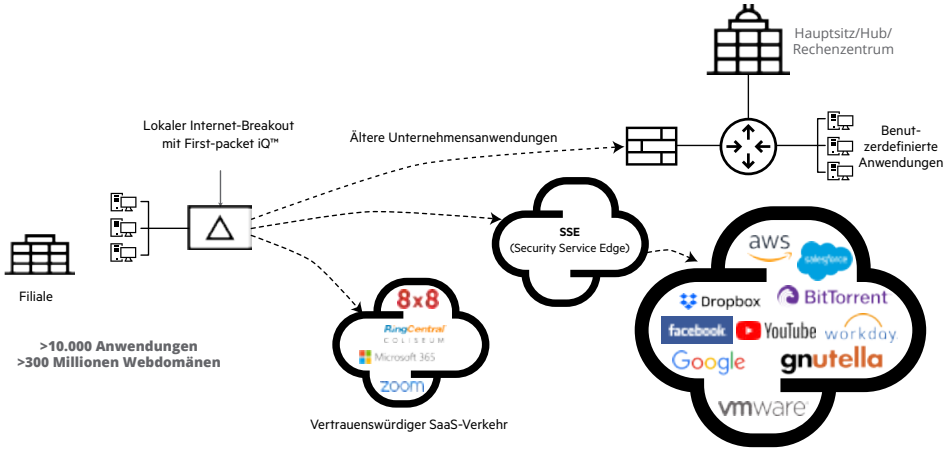


Abbildung 1. Der Anwendungsverkehr wird bereits beim ersten Paket identifiziert, um den Datenverkehr an das richtige Ziel zu leiten und die Durchsetzung von Sicherheitsrichtlinien zu ermöglichen.

Vorstellung von HPE Aruba Networking EdgeConnect SD-WAN

Die EdgeConnect SD-WAN-Plattform bietet Unternehmen die Flexibilität, eine beliebige Kombination von Transporttechnologien – einschließlich öffentlicher Breitbandservices – zu verwenden, um Benutzer mit Anwendungen zu verbinden, ohne die Anwendungsleistung oder Sicherheit zu beeinträchtigen. Zu den vier Hauptkomponenten der Plattform gehören:

- **EdgeConnect SD-WAN**, physische oder virtuelle Zero-Touch-Appliances, die in den Filialen, an zentralen Standorten und in Cloud-Rechenzentren eines Unternehmens bereitgestellt werden
- **HPE Aruba Networking EdgeConnect SD-WAN Orchestrator**, ein zentralisiertes Managementsystem, das eine einfachere Konfiguration und Orchestrierung des gesamten WAN ermöglicht und eine vollständige Beobachtbarkeit von Legacy- und Cloud-Anwendungen bietet. QoS- und Sicherheitsrichtlinien werden zentral definiert und automatisch auf allen Appliances im SD-WAN bereitgestellt. Dadurch wird die betriebliche Effizienz erhöht und menschliche Fehler, die die Sicherheit von Filialen gefährden können, werden minimiert

- **WAN-Optimierung**, ein Leistungspaket, mit dem IT-Teams bei Bedarf marktführende WAN-Optimierungsfunktionen nutzen können, indem sie ganz einfach ein Kontrollkästchen in der Orchestrator-Oberfläche aktivieren
- **Erweiterte Sicherheit**, eine optionale Sicherheitslizenz, die Funktionen zur Angriffserkennung und -verhinderung (IDS/IPS) in EdgeConnect SD-WAN-Appliances ermöglicht

EdgeConnect SD-WAN wurde mit einem umfangreichen Funktionspaket entwickelt, um alle Herausforderungen und Anforderungen an die Sicherheit am WAN-Edge in Filialen zu bewältigen, die mit SD-WAN-Implementierungen einhergehen.

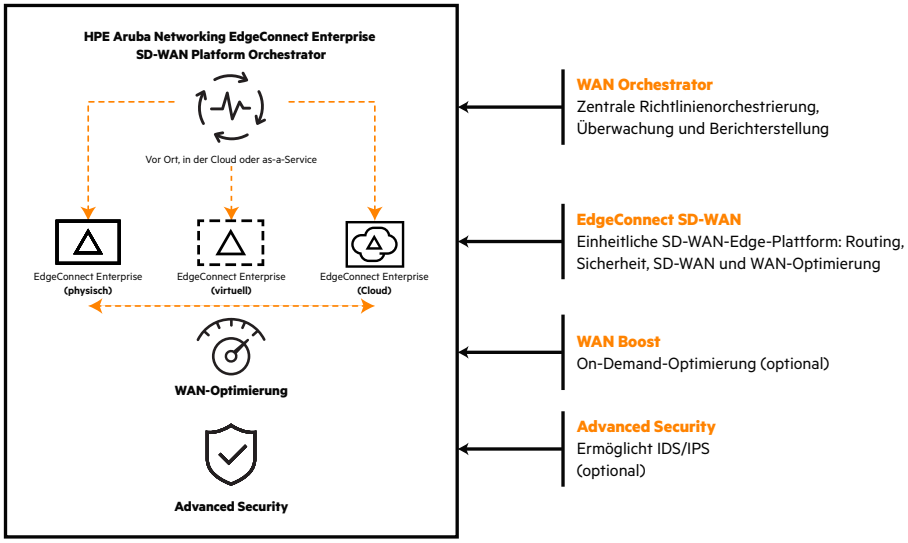


Abbildung 2. HPE Aruba Networking EdgeConnect SD-WAN-Plattform

So ermöglicht EdgeConnect SD-WAN ein sicheres SD-WAN

HPE Aruba Networking EdgeConnect SD-WAN geht weit über die Grundlagen der Gewährleistung der Vertraulichkeit des Anwendungsverkehrs in öffentlichen Netzwerken hinaus. Umfassende Sicherheitsfunktionen decken vier wesentliche Bereiche ab: die Datenebene, die Managementebene, Integration mit Security Service Edge (SSE) und Compliance. Das Ergebnis ist der umfassende Schutz, den Unternehmen benötigen, um die Vorteile eines modernen SD-WAN voll ausschöpfen zu können – verbesserte Anwendungsleistung, niedrigere WAN-Gesamtkosten und höhere geschäftliche Flexibilität –, ohne sich größeren Sicherheitsrisiken auszusetzen.

Anwendungsorientierte Sicherheit auf Datenebene

Verschiedene Anwendungen verdienen – oder erfordern vielleicht sogar – eine unterschiedliche Behandlung, wenn es darum geht, wie sie aus der Sicherheitsperspektive gehandhabt werden (ganz zu schweigen von anderen „Perspektiven" wie QoS, Leistungsoptimierung und Tunnel-Bonding-Richtlinie). So muss eine Geschäftsanwendung, die sensible Transaktionen verarbeitet, unabhängig von der Art des verwendeten Transports möglicherweise verschlüsselt werden, um die Compliance-Anforderungen zu erfüllen, während SaaS-Anwendungen sich auf ihre eigenen Funktionen (z. B. TLS) verlassen können. Deshalb ist es wichtig, über ein anwendungsorientiertes SD-WAN zu verfügen, bei dem Richtlinien und Konfigurationseinstellungen für jede einzelne Anwendung implementiert werden können.

Zu den relevanten Sicherheitsfunktionen, die mit HPE Aruba Networking EdgeConnect SD-WAN verfügbar sind, gehören:

Next-Generation Firewall: EdgeConnect SD-WAN umfasst eine Next-Generation Firewall, die in einer einzigen Entität fortschrittliche Sicherheitsfunktionen wie Deep Packet Inspection, Intrusion Prevention sowie Application und User Identity Awareness bietet. IT-Verantwortliche können Malware auf der Grundlage von Anwendung, Identität und Kontext am Eindringen in das Netzwerk hindern, unabhängig vom verwendeten Port/Protokoll. Darüber hinaus profitieren IT-Verantwortliche von einem besseren Einblick in die Netzwerkaktivitäten und potenziellen Risiken.

Angriffserkennung und -verhinderung (IDS/IPS): EdgeConnect SD-WAN integriert ein regelbasiertes Angriffserkennungs- und -verhinderungssystem (IDS/IPS). Das signaturbasierte System überwacht den Netzwerkverkehr, um Muster zu finden, die einer bestimmten Angriffssignatur entsprechen. Durch die Integration in die EdgeConnect Next-Generation Firewall ermöglicht das System die Auswahl der zu prüfenden Anwendungen auf der Grundlage von Firewall-Zonen und bietet Aktionen wie das Verwerfen oder Zulassen von Datenverkehr, wenn ein Eindringling erkannt wird.

Das System kann entweder im strikten Modus oder im Performance-Modus arbeiten. Im strikten Modus durchläuft der Datenverkehr den Sensor, sodass er sofort blockiert wird, wenn ein Eindringen erfolgt. Im Performance-Modus wird eine Kopie des Datenverkehrs zur Analyse gesendet, was die Netzwerkleistung nicht beeinträchtigt und mehr Effizienz verleiht. Mit diesem Modus wird ein Eindringen nach seiner Erkennung blockiert. Je nach Sicherheitsanforderungen können Unternehmen zwischen dem strikten und dem Performance-Modus wählen.

Die Bedrohungsprotokollierung liefert Netzwerk- und Sicherheitsanalysen zurück an HPE Aruba Networking Central oder ein SIEM eines Drittanbieters wie Splunk, um Bedrohungen in Echtzeit zu überwachen. Die EdgeConnect Security App für Splunk bietet eine Dashboard-Ansicht aller Benachrichtigungen über Sicherheitsereignisse, die von EdgeConnect Geräten innerhalb des SD-WAN eines Unternehmens exportiert werden. IT-Manager können EdgeConnect einfach so konfigurieren, dass alle Benachrichtigungen über Sicherheitsereignisse an Splunk weitergeleitet werden, wodurch die Protokollierung, Visualisierung und Analyse von Sicherheitsereignissen neben anderen Telemetrie- oder Netzwerkereignissen zentralisiert wird. Von Splunk aus können Benutzer die gesammelten Benachrichtigungen über Sicherheitsereignisse, die über die gesamte SD-WAN-Fabric generiert wurden, sowie allgemeine Trends und Top-Talker filtern, sortieren, navigieren und anzeigen, um Netzwerkereignisse zu identifizieren, die eine weitere Untersuchung erfordern.

Abbildung 3. Splunk Sicherheits-Dashboard

DDoS-Abwehr: Angesichts der zunehmenden Häufigkeit von DDoS-Angriffen (Distributed Denial of Service) ist es unerlässlich, dass Unternehmen kosteneffiziente Schutzmaßnahmen für alle möglicherweise betroffenen Standorte einrichten. Mit EdgeConnect, das in Filialen eingesetzt wird, erhalten Sie genau das. Im Falle eines DDoS-Angriffs begrenzt EdgeConnect die Anzahl der böswilligen Anfragen durch Maßnahmen wie Rapid Aging, Drop Excess und Block Source.

Die Aktionen basieren auf voreingestellten oder konfigurierbaren DoS-Schwellenwerten, die für Verkehrsparameter wie Flussrate, gleichzeitige Flüsse und embryonale Flüsse festgelegt werden. Darüber hinaus kann die Lösung im Falle eines DDoS-Angriffs den Datenverkehr dynamisch über nicht betroffene Netzwerkverbindungen leiten, ohne die Anwendungsleistung zu beeinträchtigen oder die SD-WAN-Verwaltbarkeit zu beeinflussen. EdgeConnect schützt nicht nur sich selbst, sondern auch alle Benutzer und Systeme sowohl im lokalen Netzwerk als auch über die verbleibenden, operativen WAN-Verbindungen.

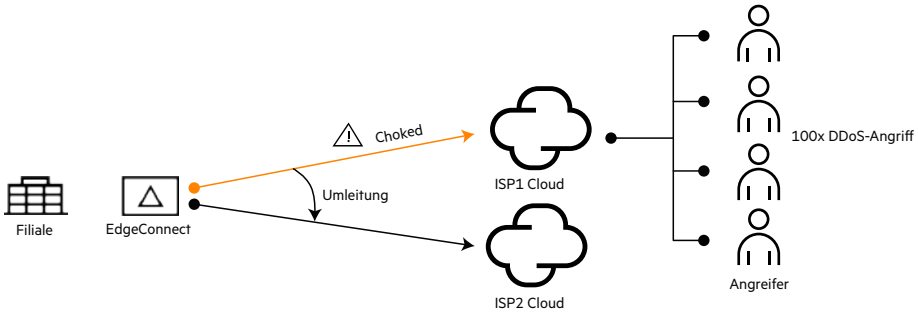


Abbildung 4. HPE Aruba Networking EdgeConnect SD-WAN schützt das SD-WAN vor DDoS-Angriffen und leitet den Datenverkehr über einen alternativen Transportservice, damit die Anwendungen weiterlaufen können und die Business Continuity gewährleistet ist.

Schutz von Daten während der Übertragung: Jeder HPE Aruba Networking EdgeConnect Datenpfad wird durch IPsec-Tunnel geschützt, die mithilfe von AES-256-Bit-Verschlüsselung die Vertraulichkeit von Anwendungen und Daten gewährleisten. EdgeConnect verwendet ein „IKE-loses" IPsec-UDP-Protokoll, d. h. es verwendet eine standardbasierte IPsec-UDP-Verschlüsselung, benötigt aber keine Internet Key Exchange Pre-Shared Keys. Die Verschlüsselungsschlüssel werden nie wiederholt und sind in jeder Richtung eindeutig. HPE Aruba Networking SD-WAN Orchestrator verwaltet die Verschlüsselungsschlüssel und Rotationen automatisch, was die Zeit für die Einrichtung des Tunnels verkürzt, ohne dass es zu einem Serviceverlust kommt. Dieses Protokoll vermeidet Probleme, die beim Einsatz von NAT (Network Address Translation) mit IKE auftreten, wie z. B. Ausfälle, wenn Filialen mehrere Geräte mit unterschiedlichen VPN-Anforderungen haben. Da IKE-less-Tunnel andere Ports als IPsec verwenden, ist es unwahrscheinlich, dass sie durch vorgeschaltete Firewalls eingeschränkt oder blockiert werden. Diese erweiterten Funktionen zum Schutz von Daten während der Übertragung erhöhen die Flexibilität, Sicherheit und Robustheit der sicheren Kommunikation zwischen Remote-Endpunkten.

Schutz von Daten bei Inaktivität: Alle Datenblöcke, die aufgrund der optionalen Datendeduplizierungsfunktion der WAN-Optimierung in HPE Aruba Networking EdgeConnect Appliances verbleiben, werden durch AES-128-Bit-Verschlüsselung geschützt.

Zero-Trust-Segmentierung: EdgeConnect SD-WAN bildet sichere End-to-End-Zonen für beliebige Kombinationen von Benutzern, Geräten, Anwendungsgruppen und virtuellen Overlays und überträgt Konfigurationsaktualisierungen im Einklang mit der geschäftlichen Absicht an verschiedene Standorte. In Verbindung mit HPE Aruba Networking ClearPass Policy Manager erzwingt EdgeConnect SD-WAN eine Zero-Trust-Architektur, die das Netzwerk dynamisch segmentiert und Zugriff auf der Grundlage des Prinzips der geringsten Rechte anwendet. Es gewährleistet, dass Anwender und IoT-Geräte nur mit Zielen kommunizieren, die ihrer jeweiligen Rolle in Bezug auf Identität, Zugriffsrechte und Sicherheitsstatus entsprechen.

Darüber hinaus können Unternehmen mit EdgeConnect SD-WAN mehrere anwendungsspezifische virtuelle WAN-Overlays (auch Business Intent Overlays genannt) erstellen. Jedes virtuelle Overlay spezifiziert Prioritäts- und Servicequalitätsanforderungen für Anwendungsgruppen auf der Grundlage der geschäftlichen Anforderungen. Mithilfe dieser Spezifikationen automatisiert EdgeConnect die Steuerung des Datenverkehrs End-to-End über alle zugrunde liegenden WAN-Transportservices.

Jedes virtuelle Overlay wird einer LAN-seitigen Zone bzw. Zonen zugeordnet. Eine Zone kann aus VLANs, physischen und logischen Schnittstellen und Sub-Schnittstellen bestehen. Jeder Zone können Sicherheitsrichtlinien zugewiesen werden, die die Konnektivität mit anderen Zonen einschränken. So könnte eine Richtlinie beispielsweise nur ausgehenden Datenverkehr zulassen, eingehenden Datenverkehr nur von zugelassenen Anwendungen und Services erlauben oder den gesamten Datenverkehr aus weniger sicheren Zonen blockieren.

Mit Zero-Trust-Segmentierung:

- Benutzer und IoT-Geräte greifen je nach Rolle und Kontext auf der Grundlage des Prinzips der geringsten Rechte auf Ressourcen zu
- Der Datenverkehr innerhalb jeder Zone ist vom Datenverkehr in anderen Segmenten isoliert, was unbefugte Zugriffe reduziert und das Ausmaß von Zwischenfällen einschränkt
- Die Mikrosegmentierung wird vom LAN über das WAN bis hin zu Rechenzentren und Cloud-Plattformen ausgedehnt
- Anwendungen mit hoher Priorität genießen eine schnellere und zuverlässigere Leistung über das WAN, wodurch die Anwendungsverfügbarkeit erhöht wird und die Erfahrung und Produktivität der Endbenutzer verbessert werden

Einfache Erstellung von Richtlinien: IT-Administratoren können mithilfe einer intuitiven grafischen Benutzeroberfläche in wenigen Minuten Netzwerksegmente erstellen. Diese Segmente können LANs mit anderen LANs (LAN-WAN-LAN) und mit Rechenzentren (LAN-WAN-Rechenzentrum) verbinden. Die virtuellen WAN-Overlays werden auf der Grundlage von geschäftlichen Anforderungen und Absichten definiert, nicht von Infrastrukturdetails wie IP-Adressen. Die zonenbasierten Sicherheitsrichtlinien werden in einer Konfigurationsmatrix angezeigt, die sie leicht verständlich macht.

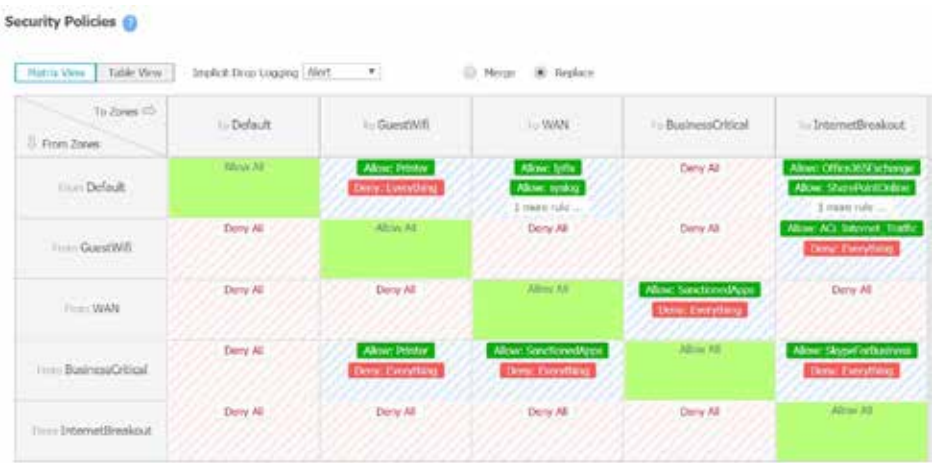
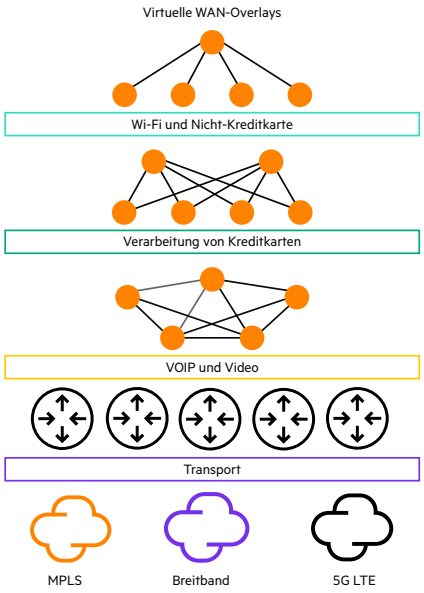


Abbildung 5. Eine Konfigurationsmatrix für Sicherheitsrichtlinien vereinfacht die Erstellung und Verwaltung von Segmentierungsregeln erheblich.

Zentrale Orchestrierung und automatisierte Durchsetzung: Sobald virtuelle WAN-Overlays und zonenbasierte Firewall-Richtlinien definiert sind, stellt HPE Aruba Networking SD-WAN Orchestrator sie auf allen EdgeConnect SD-WAN-Appliances bereit, wo sie automatisch durchgesetzt werden. Dies ersetzt die zeitraubende manuelle Konfiguration von Routern und Firewalls bei jeder Änderung einer Richtlinie.

Zu den Vorteilen gehören:

- Konsistente Durchsetzung von Sicherheitsrichtlinien über LANs und WANs hinweg
- Weniger Konfigurationsfehler
- Verbesserte Einhaltung von Vorschriften und Industriestandards
- Höhere Produktivität für Sicherheits- und Betriebspersonal



Zugriffsrichtlinie	Topologie	Verbindung	QoS
Gast-VLAN	Hub and Spoke	Internet	Min. Kosten
Daten-VLAN	Dual Hub and Spoke	MPLS–Internet	Max. Verfügbarkeit
Sprach-VLAN	Full Mesh	MPLS – Internet – LTE	Max. Qualität

Abbildung 6. HPE Aruba Networking EdgeConnect SD-WAN erweitert die Mikrosegmentierung über das WAN, damit Unternehmen Compliance-Standards einhalten können.

Unified SASE mit HPE Aruba Networking

Die einheitliche SASE-Lösung von HPE Aruba Networking bietet eine Konnektivitäts-Fabric, die aus dem preisgekrönten HPE Aruba Networking SSE und dem branchenführenden HPE Aruba Networking EdgeConnect SD-WAN eine einzige Lösung bildet, die den wachsenden Bedarf an integrierten Netzwerk- und Sicherheitslösungen deckt. Darüber hinaus ist HPE Aruba Networking SSE eng mit HPE Aruba Networking EdgeConnect SD-Branch und HPE Aruba Networking EdgeConnect MicroBranch integriert.

Mit dieser Lösung wird die Umstellung der Unternehmen auf SASE beschleunigt. Die einheitliche SASE-Lösung lässt sich dank einer zentralen, eng integrierten Plattform mühelos bereitstellen und bietet vereinfachtes Management.

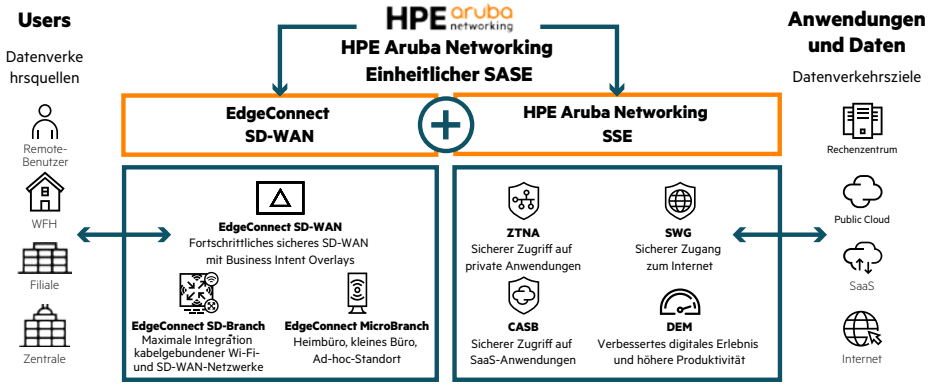


Abbildung 7. Bereitstellung des branchenführenden HPE Aruba Networking EdgeConnect SD-WAN mit der Cloud-nativen HPE Aruba Networking SSE-Plattform zur Bildung einer einheitlichen SASE-Lösung

SSE ist eine einheitliche Plattform, bei der sich ZTNA, SWG und CASB eine gemeinsame Codebasis teilen. Sämtliche Richtlinien werden über eine zentrale Benutzeroberfläche verwaltet, wodurch die Kontrolle für IT-Admins erheblich vereinfacht wird. Benutzern und autorisierten Dritten wird der Zugriff auf Ressourcen per ZTNA mit und ohne Agenten ermöglicht. Benutzer werden mit SWG vor Bedrohungen aus dem Web geschützt, und vertrauliche Daten in SaaS-Anwendungen werden mit CASB sicher überwacht, um die Exfiltration der Daten zu verhindern. Zudem vereinheitlicht die Lösung den Zugriff weltweit mittels eines Cloud-Backbones aus Amazon Web Services (AWS), Microsoft Azure, Google und Oracle.

Funktionen von HPE Aruba Networking SSE:

- **ZTNA (Zero-Trust-Netzwerkzugriff)** basiert auf dem Grundsatz „niemals vertrauen, immer verifizieren", sodass Geräten, die sich mit dem Netzwerk verbinden, nicht standardmäßig vertraut wird. Im Gegensatz zu einem VPN, das verbundenen Benutzern den Zugriff auf das Unternehmensnetzwerk gewährt, begrenzt ZTNA den Benutzerzugriff auf spezifische Anwendungen oder Mikrosegmente, die für den Benutzer freigegeben wurden, wodurch das Prinzip der geringsten Rechte durchgesetzt wird. Mit ZTNA können Remote-Mitarbeitende überall eine Verbindung herstellen.

  Auch Drittbenutzer können mit agentenlosem ZTNA einfach in das Netzwerk aufgenommen werden. Es muss kein ZTNA-Agent auf Laptops installiert werden. Stattdessen melden sich Drittbenutzer mit ihren eigenen Anmeldedaten bei einem ZTNA-Webportal an.

- **SWG (Secure Web Gateway)** schaltet sich zwischen Benutzer und Websites und bietet Schutz vor schädlichen Bedrohungen.

  Es führt eine Reihe von Sicherheitsüberprüfungen durch, darunter URL-Filterung, Erkennung von schädlichem Code und Web-Zugriffskontrolle, und stellt Richtlinien bereit, die den Zugriff einschränken können, beispielsweise auf nicht jugendfreie Websites, Glücksspielseiten oder gefährliche Websites.

- **CASB (Cloud Access Security Broker)** gewährleistet, dass in der Cloud gehostete vertrauliche Daten geschützt bleiben. Er identifiziert und erkennt vertrauliche Daten in Cloud-Anwendungen und setzt Sicherheitsrichtlinien wie beispielsweise Authentifizierung und Single Sign-On (SSO) durch. Er überwacht Benutzeraktivitäten in Cloud-Services, identifiziert potenzielle Sicherheitsrisiken und Richtlinienverstöße, um Datenverluste zu vermeiden, und kontrolliert Block-Uploads- und -Downloads von SaaS-Anwendungen wie Box, SharePoint, Facebook und Salesforce. Er verhindert, dass Benutzer sich bei Cloud-Anwendungen, die nicht von den IT- und Sicherheitsrichtlinien eines Unternehmens genehmigt sind, registrieren und diese nutzen, wodurch es Unternehmen ermöglicht wird, Schatten-IT zu reduzieren.
- **DEM (Digital Experience Monitoring)** gewährleistet die Produktivität von Benutzern, indem es Metriken Hop für Hop misst und die Anwendungs-, Geräte- und Netzwerkleistung überwacht. Die IT-Abteilung kann so ganz einfach Konnektivitätsprobleme identifizieren und die Mean Time to Resolution verkürzen.

Integration mit mehreren SASE-Partnern

HPE Aruba Networking EdgeConnect SD-WAN kann nahtlos mit einer Reihe von Cloud-Sicherheitsservices von Drittanbietern verbunden werden. Dies kommt Unternehmen zugute, die es vorziehen, SASE mit den Sicherheitsservices ihrer Wahl einzuführen oder nahtlos in ein vorhandenes Sicherheitsökosystem zu integrieren.

HPE Aruba Networking unterhält Technologiepartnerschaften mit führenden SSE-Anbietern (Security Service Edge), die Lösungsbereiche wie Secure Web Gateways (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) und Remote Browser Isolation (RBI) von Sicherheitsunternehmen wie Zscaler, Netskope, Check Point, McAfee, Palo Alto Networks und Symantec abdecken.

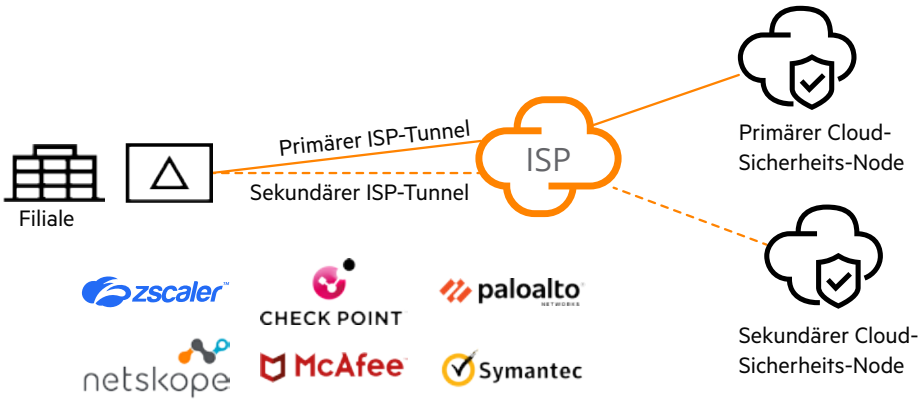


Abbildung 8. Automatisierung der Service-Orchestrierung mit mehreren Cloud-Sicherheitsanbietern

Automatisierte Integration und Orchestrierung: HPE Aruba Networking EdgeConnect automatisiert die Orchestrierung mit externen Cloud-Sicherheitsanbietern (SSE) sowie die Konfiguration von IPsec-Tunneln zwischen EdgeConnect und SSE-Anbietern. Mit dieser Fähigkeit identifiziert die First-packet iQ™-Anwendungsklassifizierungsfunktion zunächst Anwendungen und Webdomänen auf der Grundlage des ersten Pakets. Der Datenverkehr wird dann auf der Grundlage der vom Unternehmen definierten Sicherheitsrichtlinien auf intelligente Weise zu SSE-Services gelenkt. Administratoren können auch die Vorteile einer einfachen Drag-and-Drop-Oberfläche nutzen, die es ihnen erleichtert, Richtlinien für den Datenverkehr von bestimmten Anwendungen zuzuweisen und den Datenverkehr an bestimmte Sicherheitstools weiterzuleiten. So wird beispielsweise der über das Internet eingehende Datenverkehr automatisch durch Cloud-basierte Sicherheitsdienste für Layer-7-Zugangskontrolle, Bedrohungsfilterung und Analysen geleitet.

Sicherheit auf Management- und Systemebene

Obwohl die Sicherheit der System- und Managementebene weniger im Vordergrund steht als die der Datenebene, ist sie nicht weniger wichtig. Zu den relevanten Funktionen von HPE Aruba Networking EdgeConnect in diesem Bereich gehören:

Sicheres Zero-Touch-Provisioning: Ein wesentlicher Bestandteil des Wertversprechens von HPE Aruba Networking EdgeConnect SD-WAN ist ein Plug-and-Play-Bereitstellungsmodell, das eine schnelle Installation ermöglicht, ohne dass eine verteilte IT-Präsenz erforderlich ist. Die Sicherheit dieses Prozesses besteht in einem zweistufigen Authentifizierungs- und Autorisierungsverfahren. Bevor sie ihre Einstellungen und Richtlinien empfängt und zu einem aktiven Bestandteil des SD-WAN wird, muss jede neu verbundene EdgeConnect Appliance zunächst über das Cloud-Portal von HPE Aruba Networking authentifiziert und anschließend mithilfe von HPE Aruba Networking SD-WAN Orchestrator von einem IT-Administrator „genehmigt" werden.

Darüber hinaus kann SD-WAN Orchestrator auch dazu verwendet werden, den Zugriff auf eine bestimmte Appliance nachträglich zu sperren (z. B. wenn sie gestohlen oder anderweitig kompromittiert wurde). Dies führt dazu, dass jeglicher Datenverkehr im laufenden Betrieb verworfen wird und die angegebene Appliance nicht in der Lage ist, Konfigurationsinformationen herunterzuladen oder dem SD-WAN beizutreten.

Verschlüsselte Management-Kommunikation: Alle Kommunikationssitzungen zwischen EdgeConnect Appliances, SD-WAN Orchestrator, dem HPE Aruba Networking Cloud-Portal und den Webbrowsern der Administratoren sind mit TLS 1.2 geschützt. Außerdem sind alle schwachen Protokolle (z. B. SSLv2, SSLv3, TLS 1.0, TLS 1.1), schwachen Hashes (z. B. MD5) und schwachen Verschlüsselungsalgorithmen (z. B. DES, RC4) standardmäßig deaktiviert.

Systemhärtung: EdgeConnect ist eine robuste Appliance, die ab Werk mit dem Modus „gehärtet" ausgeliefert wird. Dieser Ansatz gewährleistet sofortige Sicherheit für Geräte, die zum ersten Mal angeschlossen werden.

Weitere Schutzmaßnahmen auf der Managementebene sind:

Zuverlässige Benutzerauthentifizierung und -autorisierung

- Unterstützung für lokale, RADIUS, TACACS+ und Oauth zur Authentifizierung und Autorisierung mit Identity-Management-Systemen wie Active Directory und Okta.
- Detaillierte rollenbasierte Zugriffskontrolle mit Benutzern mit Lesezugriff und mehreren Administratorrollen
- Whitelisting für Orchestrator, das den administrativen Zugriff auf eine bestimmte Gruppe von IP-Adressen oder Subnetzen einschränkt

Umfassende Protokollierung sowohl für SD-WAN Orchestrator als auch für EdgeConnect

- Ereignisprotokolle/Alarme – für Systemfehler in Bezug auf Arbeitsspeicher, CPU, Netzwerkschnittstellen, Routing und Konnektivität der Managementebene
- Warnungen beim Überschreiten von Schwellenwerten – konfigurierbare, ansteigende und abfallende Schwellenwerte, um unmittelbare/nahende Bedingungen zu signalisieren, die Anlass zur Besorgnis geben, z. B. eine hohe Arbeitsspeicher- oder Bandbreitennutzung
- Audit-Protokolle – zur Nachverfolgung aller Zugriffe auf eine Aktivität, die über eine der verfügbaren Managementschnittstellen (CLI, WebUI oder REST-APIs) durchgeführt wurden
- Firewall-Protokolle – von der EdgeConnect Next-Generation Firewall überprüfte Verkehrsströme erzeugen Verweigerungs-, Annahme- und Verwerfungsereignisse sowie die Gründe für diese Ereignisse. Die Firewall-Protokolle können dann an ein SIEM-Tool eines Drittanbieters (z. B. Splunk) weitergeleitet werden.
- Netflow-/Datenverkehrsprotokolle – zur Erfassung vollständiger (nicht abgetasteter) Datenströme, damit diese an ein Drittanbieter-Tool (z. B. Netflow collector) weitergeleitet werden können

Die Protokolldaten sind nicht nur für das Netzwerkmanagement und die Reaktion auf Zwischenfälle wichtig, sondern können auch für die Einhaltung von Standards wie HIPAA von Nutzen sein.

Sicherheitszertifizierung und Compliance

Da sich Benutzer von überall aus über von Natur aus unsichere Verbindungen wie Breitband-Internet und 5G verbinden und online auf vertrauliche Daten zugreifen, ist die Notwendigkeit, ein SD-WAN für Sicherheit zu zertifizieren, noch dringlicher geworden. HPE Aruba Networking EdgeConnect SD-WAN hat die ICSA Labs Secure SD-WAN-Zertifizierung erhalten, die auf einer umfassenden und robusten Reihe von SD-WAN-Funktionen und Plattformsicherheitsanforderungen basiert.

Zu den Anforderungen der ICSA Labs Secure SD-WAN-Zertifizierung gehören:

- **Erweiterte SD-WAN-Funktionen** wie Tunnel Bonding, dynamische Pfadauswahl und Zero-Touch-Provisioning
- **Native Unterstützung (oder Serviceverkettung) für erweiterte Sicherheitsfunktionen** wie Anti-Malware, Intrusion Prevention und DoS-Schutz
- **Verschlüsselung** vertraulicher Daten sowie der administrativen und operativen Kommunikation
- **Durchsetzung von Richtlinien** sowohl für WAN-spezifische Funktionen als auch für Sicherheitsrichtlinien
- **Protokollierung von Sicherheitsereignissen**

Mit der Gewissheit, ein sicheres SD-WAN zu nutzen, das von einer weltweit anerkannten, unabhängigen Drittorganisation zertifiziert wurde, können Unternehmen die Netzwerkarchitektur in Filialen vereinfachen, indem sie die Firewalls der Filialen durch EdgeConnect SD-WAN ersetzen.

Die meisten der bisher behandelten Sicherheitsmerkmale sind auf mehrere Anforderungen anwendbar, die sich auf mehrere Vorschriften erstrecken. Authentifizierungs-, Autorisierungs- und Audit-Funktionen sind zum Beispiel eine grundlegende Anforderung der NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations) – und damit praktisch jeder Vorschrift, die sich darauf beruft.

Bemerkenswert ist auch die Unterstützung von EdgeConnect SD-WAN für Mikrosegmentierung, die unter den SD-WAN-Lösungen einzigartig ist. Die Möglichkeit, verschlüsselte, anwendungsspezifische Overlays zu erstellen, kann IT-Teams dabei helfen, den Zugriff auf Systeme zu kontrollieren, die elektronische private Gesundheitsinformationen (ePHI) speichern und verarbeiten, um die Einhaltung des HIPAA zu unterstützen, Kredittransaktionen und zugehörige Systeme abzusondern, um den Umfang ihrer PCI DSS-Compliance-Bemühungen erheblich zu reduzieren und das Risiko eines unbefugten Zugriffs auf Kundendaten zu verringern. So können die DSGVO und andere Datenschutzvorschriften erfüllt werden.

Nicht zuletzt trägt EdgeConnect SD-WAN in Verbindung mit HPE Aruba Networking SSE auf vielfältige Weise dazu bei, die Einhaltung der einschlägigen Branchenvorschriften zu erleichtern: Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), DSGVO der Europäischen Union und andere.

Um beispielsweise die Einhaltung von Datenschutzvorschriften zu gewährleisten, helfen CASB und DLP bei der Durchsetzung der Datensicherung. Sie überwachen risikobehaftete Daten und verhindern, dass Benutzer vertrauliche Daten absichtlich oder versehentlich in Cloud-Anwendungen hochladen. Ebenso hilft CASB dabei, Schatten-IT zu reduzieren und nicht genehmigte Cloud-Anwendungen in Unternehmen zu identifizieren, vertrauliche Daten während der Übertragung zu erkennen und Sicherheitsrichtlinien wie Authentifizierung und Single Sign-On (SSO) durchzusetzen.

ZTNA schützt Daten vor Cyberbedrohungen, indem private Ressourcen vor dem Internet verborgen und Benutzer nicht ins Netzwerk gelassen werden. SWG bietet Schutz vor schädlichem Webverkehr wie Phishing und Ransomware und reduziert damit die Risiken für die Cybersicherheit und stärkt die Compliance.

Fazit

Um die vielen überzeugenden Vorteile eines sicheren SD-WAN voll ausschöpfen zu können, muss eine Lösung gefunden werden, die die Sicherheitsprobleme, Herausforderungen und Chancen berücksichtigt, die ein solcher Ansatz bietet. In dieser Hinsicht gehen die umfassenden Sicherheitsfunktionen der HPE Aruba Networking EdgeConnect SD-WAN-Plattform weit über das erforderliche Mindestmaß an Schutz hinaus, das durch Verschlüsselung auf Transportebene und Nachrichtenauthentifizierung gewährleistet wird.

Mit der integrierten Next-Generation Firewall mit erweiterten Sicherheitsfunktionen wie IDS/IPS und DDoS-Schutz ermöglicht es HPE Aruba Networking EdgeConnect SD-WAN Unternehmen, ältere Firewalls sowie auch Router in Filialen zu ersetzen und somit die Hardwarestellfläche sowie Kosten und Komplexität zu reduzieren.

Durch die Kombination von EdgeConnect SD-WAN und seiner robusten Sicherheit auf Daten- und Managementebene mit dem preisgekrönten HPE Aruba Networking SSE können Unternehmen eine einheitliche SASE-Lösung zusammenstellen und ihre Umstellung auf SASE dank nahtloser Bereitstellung und vereinfachtem Management beschleunigen. Für Unternehmen, die SASE vorzugsweise mit den Sicherheitsservices ihrer eigenen Wahl einführen möchten, unterstützt EdgeConnect SD-WAN die automatisierte Integration und Orchestrierung mit in der Cloud bereitgestellten Sicherheitslösungen von Drittanbietern.

Und zu guter Letzt ergänzt EdgeConnect angesichts der zunehmenden Verbreitung von IoT-Geräten SASE durch eine Zero-Trust-Architektur, die das Netzwerk auf Basis der Identität segmentiert, sodass Benutzer und IoT-Geräte nur solche Netzwerkziele erreichen können, die ihrer Rolle im Unternehmen entsprechen.

Entscheiden Sie sich für das richtige Produkt. Kontaktieren Sie unsere Presales-Experten.

Kontakt

Besuchen Sie **ArubaNetworks.com**

Hewlett Packard Enterprise

BP_ArchitectingSASE_LP_021924 a00126522dee