HPE Aruba Networking EdgeConnect SD-WAN

Angesichts der immer schnelleren Einführung Cloud-basierter Anwendungen betrachten geografisch verteilte Unternehmen SD-WAN zunehmend als kritische Technologie, um Benutzer und Anwendungen miteinander zu verbinden.

Im Zuge der Migration von Unternehmensanwendungen vom Unternehmensrechenzentrum in die Cloud erweisen sich Verbindungen über private Leitungen wie beispielsweise Multi-Protocol Label Switching (MPLS) als übermäßig unflexibel und teuer. Mit der zunehmenden Abhängigkeit vom Internet lässt sich „Cloud-Geschwindigkeit“ besser erreichen, indem man Breitband-Internetservices in den WAN-Transportmix integriert.

Die HPE Aruba Networking EdgeConnect SD-WAN-Plattform ermöglicht es Unternehmen, die Anwendungsleistung zu verbessern und Kosten und Komplexität beim Aufbau eines WAN mithilfe von Breitband zur Vernetzung von Benutzern und Anwendungen zu reduzieren.

EdgeConnect SD-WAN bildet eine sichere Netzwerkgrundlage für Zero-Trust- und SASE-Frameworks, um die Netzwerk- und Sicherheitsherausforderungen von hybriden Arbeitsmodellen und Cloud Computing zu bewältigen. Die Lösung integriert sich nahtlos in HPE Aruba Networking SSE und bildet so eine einheitliche SASE-Plattform für eine einfachere Einführung und schnellere Bereitstellung von SASE.

Darüber hinaus verfügt EdgeConnect SD-WAN über eine integrierte Next-Generation Firewall, die eine fein abgestufte Segmentierung und identitätsbasierte Zugriffskontrollfunktionen ermöglicht, sowie IDS/IPS und DDoS-Abwehr, um Filialen vor schädlichen Aktivitäten zu schützen. Als Anerkennung von einer unabhängigen Drittorganisation hat EdgeConnect SD-WAN dank seiner fortschrittlichen SD-WAN- und Sicherheitsmerkmale die **Secure SD-WAN-Zertifizierung von ICSA Labs** erhalten.

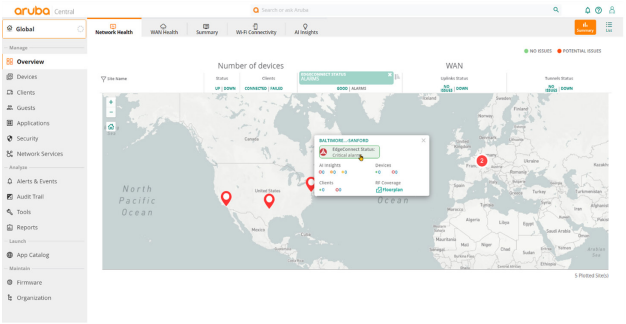


Abbildung 1. HPE Aruba Networking Central bietet die Möglichkeit, HPE Aruba Networking EdgeConnect SD-WAN Orchestrator direkt zu starten und die unternehmensweite SD-WAN-Topologie, den Zustand sowie Alarme aller HPE Aruba Networking EdgeConnect SD-WAN-Appliances im Netzwerk anzuzeigen.

EdgeConnect SD-WAN-Plattform

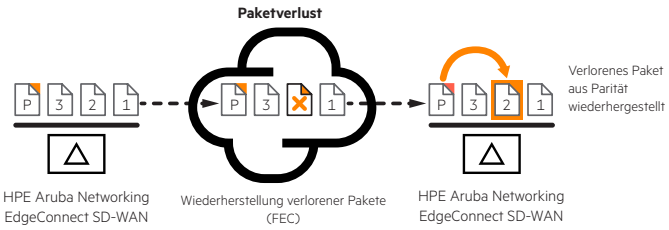
Die HPE Aruba Networking EdgeConnect SD-WAN-Plattform besteht aus drei Komponenten:

- **HPE Aruba Networking EdgeConnect SD-WAN:** Physische oder virtuelle SD-WAN-Appliances (die alle gängigen Hypervisoren und Public Clouds unterstützen), die in Filialen bereitgestellt werden, um ein sicheres virtuelles Netzwerk-Overlay zu bilden. Damit können Kunden in ihrem eigenen Tempo zu einem Breitband-WAN wechseln, ob Standort für Standort oder mittels eines hybriden WAN-Ansatzes, bei dem MPLS und Breitband-Internetkonnektivität zum Einsatz kommen.
- **HPE Aruba Networking SD-WAN Orchestrator** ist in der EdgeConnect SD-WAN-Plattform enthaltet und bietet beispiellose Einblicke in Legacy- und Cloud-Anwendungen sowie die einzigartige Möglichkeit, Richtlinien zentral auf der Grundlage der geschäftlichen Absicht zuzuweisen, um sämtlichen WAN-Datenverkehr zu schützen und zu kontrollieren. Die Richtlinienautomatisierung beschleunigt und vereinfacht die Bereitstellung mehrerer Filialen und macht anwendungsübergreifend konsistente Richtlinien möglich. Darüber hinaus können Kunden die SD-WAN Orchestrator Software direkt über HPE Aruba Networking Central starten und erhalten so die Möglichkeit, die unternehmensweite SD-WAN-Topologie, den Zustand sowie Alarme aller EdgeConnect SD-WAN-Appliances im SD-WAN zusätzlich zu anderen kabelgebundenen und Wireless-Netzwerkgeräten von HPE Aruba Networking anzuzeigen.
- **HPE Aruba Networking EdgeConnect WAN Optimization** ermöglicht es Kunden, die Leistung latenzempfindlicher Anwendungen zu steigern und die Übertragung sich wiederholender Daten aus dem WAN in einer einzigen, einheitlichen SD-WAN-Edge-Plattform zu minimieren.

Wichtigste Merkmale von EdgeConnect SD-WAN

- **Business Intent Overlays:** HPE Aruba Networking EdgeConnect SD-WAN basiert auf einem anwendungsspezifischen virtuellen WAN-Overlay-Modell. Es können mehrere Overlays definiert werden, um die zugrundeliegenden physischen Transportservices von den virtuellen Overlays zu abstrahieren, wobei jedes Overlay unterschiedliche QoS-, Transport-, Failover- und Sicherheitsrichtlinien unterstützt. Gruppen von Anwendungen werden verschiedenen Business Intent Overlays zugeordnet, um Benutzern die Anwendungen im Einklang mit den geschäftlichen Anforderungen zur Verfügung zu stellen. Ebenso können Business Intent Overlays bereitgestellt werden, um die Mikrosegmentierung von bestimmtem Anwendungsverkehr aus dem Rechenzentrum auf das gesamte WAN auszuweiten und so die Einhaltung von Sicherheitsvorgaben zu unterstützen.
- **Pfadkonditionierung:** Diese Funktion ermöglicht eine ähnliche Leistung wie bei einer privaten Leitung über das öffentliche Internet. Dies umfasst Techniken zur Bewältigung der nachteiligen Auswirkungen von Paketverlusten und ungeordneten Paketen, die häufig bei Breitband-Internet- und MPLS-Verbindungen auftreten, um die Anwendungsleistung zu verbessern.

Vorwärts-Fehlerkorrektur



Korrektur der Paketreihenfolge

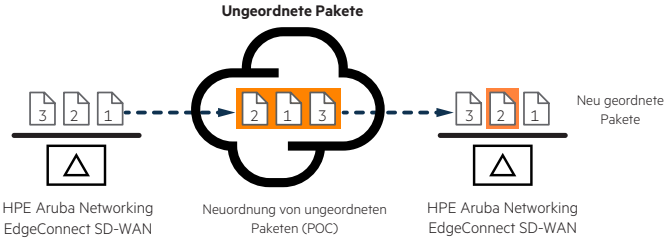


Abbildung 2. Pfadkonditionierung – fortschrittliche Funktionen für die Netzwerk- und Anwendungsleistung

- **Tunnel Bonding:** Aneinander gebundene Tunnel werden aus zwei oder mehr physischen WAN-Transportservices konfiguriert und bilden eine einzige logische Overlay-Verbindung, die die Leistung aller zugrundeliegenden Links aggregiert. Echtzeit-Datenverkehrssteuerung wird anhand der vom Unternehmen definierten, auf der geschäftlichen Absicht basierenden Richtlinien über jeden beliebigen Breitband- oder MPLS-Link bzw. jede beliebige Kombination von Links angewendet. Kommt es zu einem Ausfall oder Brownout, überträgt EdgeConnect SD-WAN den Datenverkehr weiterhin automatisch über die verbleibenden Links oder wechselt zu einer sekundären Verbindung.

  Netzwerkverkehr, der ein EdgeConnect SD-WAN durchquert, kann im Hinblick auf Verfügbarkeit, Qualität, Durchsatz und Effizienz optimiert werden. Dies wird auf Anwendungsbasis mithilfe von Business Intent Overlays erzielt. Es können mehrere Business-Intent-Richtlinien erstellt werden, wobei jede ihre eigene spezifische Bonding-Richtlinie aufweist. Im Rahmen dieser Richtliniendefinition haben Kunden die Möglichkeit, die Richtlinien zur Link-Priorisierung und Datenverkehrssteuerung anhand von mehreren Kriterien anzupassen, darunter physische Leistungsmerkmale, Link-Wirtschaftlichkeit, Link-Ausfallsicherheit sowie vom Kunden zu definierende Attribute.
- **First-packet iQ Anwendungsklassifizierung:** Die HPE Aruba Networking EdgeConnect SD-WAN First-packet iQ Anwendungsklassifizierung identifiziert Anwendungen im ersten Paket, um vertrauenswürdigen SaaS- und Web-Datenverkehr direkt an das Internet zu leiten, während unbekannter oder verdächtiger Datenverkehr zur Firewall im Rechenzentrum oder zu IDS/IPS umgeleitet wird. Die Identifizierung von Anwendungen im ersten Paket ist besonders dann wichtig, wenn Zweigstellen hinter Network Address Translation (NAT) bereitgestellt werden. Der korrekte Pfad muss auf Basis des ersten Pakets ausgewählt werden, um Sitzungsunterbrechungen zu vermeiden.

- **Sicherer Internet-Breakout:** Granulare, intelligente Datenverkehrssteuerung, die durch First-packet iQ ermöglicht wird, macht das ineffiziente Backhauling von sämtlichem HTTP-/HTTPS-Datenverkehr ins Rechenzentrum unnötig. Die Lösung eliminiert das Potenzial von Bandbreitenverschwendung und Leistungsengpässen bei vertrauenswürdigem SaaS- und Web-Datenverkehr. Vertrauenswürdiger Datenverkehr wird direkt über das Internet gesendet, während unbekannter oder verdächtiger Datenverkehr im Einklang mit den Sicherheitsrichtlinien des Unternehmens automatisch an robustere Sicherheitsservices gesendet werden kann.
- **Einheitlicher SASE (Secure Access Service Edge):** Um dem zunehmenden Bedarf an integriertem Networking und integrierter Sicherheit im Zeitalter von hybriden Arbeitsmodellen und Cloud Computing gerecht zu werden, lässt sich die HPE Aruba Networking EdgeConnect SD-WAN-Lösung nahtlos mit HPE Aruba Networking SSE kombinieren, um eine einheitliche SASE-Plattform zu bilden. Dieser kohärente Ansatz optimiert die Einführung und beschleunigt die Bereitstellung von SASE.

  Die einheitliche SASE-Lösung beinhaltet nicht nur den Funktionsumfang von SD-WAN, sondern weitet dessen Funktionen aus, um die Sicherheitsanforderungen von Remote-Benutzern und hybriden Mitarbeitenden mit Zero-Trust-Netzwerkzugriff (ZTNA) zu erfüllen. Mit ZTNA gewährleistet sie, dass der Zugriff auf Basis des Prinzips der geringsten Rechte gewährt wird, und stärkt so das allgemeine Sicherheitsniveau. Darüber hinaus ermöglicht ZTNA Benutzern und autorisierten Dritten den Zugriff auf Ressourcen mit oder ohne Agenten. Mithilfe ihres Secure Web Gateway (SWG) bietet die einheitliche SASE-Plattform Schutz vor schädlichem Web-Datenverkehr, darunter Ransomware, Malware und Phishing-Angriffe. Ebenso bietet sie einen robusten Schutz vertraulicher Daten und verhindert Datenverluste dank CASB-Funktionen (Cloud Access Security Broker). Die Lösung integriert Digital Experience Monitoring (DEM) zur Optimierung des Benutzererlebnisses und des Betriebs.

  ZTNA, SWG, CASB und DEM integrieren sich nahtlos in eine zentrale Codebasis. Dies ermöglicht ein einfacheres Richtlinienmanagement über eine einzige Oberfläche und Richtlinien-Engine. Zudem vereinheitlicht die Lösung den Zugriff weltweit mittels eines Cloud-Backbones aus Amazon Web Services (AWS), Microsoft Azure, Google Cloud und Oracle Cloud.
- **Automatisierte Orchestrierung für SSE-Drittanbieter:** HPE Aruba Networking EdgeConnect SD-WAN automatisiert die Integration mit führenden Partnerlösungen für Cloud-Sicherheit von Zscaler, Netskope, Check Point, Palo Alto Networks, McAfee, Symantec und weiteren Anbietern und schafft so eine nahtlose SASE-Architektur. Mithilfe der automatisierten Orchestrierung über eine Drag-and-Drop-Oberfläche kann die IT-Abteilung konsistente unternehmensweite Sicherheitsrichtlinien auf der Grundlage geschäftlicher Anforderungen konfigurieren.
- **Next-Generation Firewall:** EdgeConnect SD-WAN umfasst eine Next-Generation Firewall, die in einer einzigen Entität fortschrittliche Sicherheitsfunktionen wie Deep Packet Inspection, Intrusion Prevention, DDoS-Abwehr 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.
- **Rollenbasierte Segmentierung:** Erstellen Sie sichere End-to-End-Zonen für beliebige Kombinationen von Benutzern, Anwendungsgruppen und virtuellen Overlays und übermitteln Sie Konfigurationsaktualisierungen im Einklang mit der geschäftlichen Absicht an verschiedene Standorte.

  Die Integration von HPE Aruba Networking ClearPass mit EdgeConnect SD-WAN erweitert die Anwendungsintelligenz um Benutzer- und Geräteidentität sowie rollenbasierte Richtlinien und ermöglicht somit eine fein abgestufte Segmentierung. Der zusätzliche identitätsbasierte Kontext ermöglicht eine konsistente Durchsetzung von Sicherheitsrichtlinien, die netzwerkweit vom Edge bis zur Cloud durchgesetzt werden können, und beschleunigt gleichzeitig die Fehlerbehebung und Problemlösung.

  Darüber hinaus sind die Funktionen von HPE Aruba Networking Central NetConductor in EdgeConnect SD-WAN integriert. Dank dieser kombinierten Lösung können Unternehmen eine unternehmensweite Zero-Trust-Architektur implementieren, und zwar auch in komplexen Multi-Vendor-LAN-Umgebungen. Ermöglicht wird dies durch die offenen EVPN-/VXLAN-Standards.

  EdgeConnect SD-WAN kann Rolleninformationen durch die gesamte Fabric transportieren, unabhängig davon, ob der Datenverkehr sich an eine VXLAN-basierte Campus-Fabric richtet, die mit HPE Aruba Networking Central NetConductor verwaltet wird, oder an eine Campus-Fabric-Lösung eines Drittanbieters, die gruppenbasierte EVPN-/VXLAN-Richtlinien unterstützt. IT-Architekten können mühelos Rolle-zu-Rolle-Mikrosegmentierungsrichtlinien erstellen, die auf das gesamte Unternehmen angewendet werden können. Falls das Netzwerk VXLAN nicht unterstützt, leitet RADIUS-Snooping die Rolle direkt aus RADIUS-Transaktionen für die Authentifizierung und Autorisierung ab oder empfängt sie über eine API als Anmeldungs- und Abmeldungsereignisse von HPE Aruba Networking ClearPass.
- **Angriffserkennung und -verhinderung (IDS/IPS):** HPE Aruba Networking EdgeConnect SD-WAN integriert ein regelbasiertes System für die Angriffserkennung und -verhinderung (IDS/IPS) und nutzt das gemeinsame HPE Aruba Networking Unified Threat Management (UTM)-Framework. Das signaturbasierte System überwacht den Netzwerkverkehr, um Muster zu finden, die einer bestimmten Angriffssignatur entsprechen. Durch die Integration in die EdgeConnect SD-WAN Next-Generation Firewall ermöglicht das System die Auswahl auf Anwendungsebene für die Prüfung auf der Grundlage von Firewall-Zonen und bietet Aktionen wie das Verwerfen, Untersuchen und Zulassen von Datenverkehr. Das System kann entweder im Inline-Modus oder im Performance-Modus arbeiten. Im Inline-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 effizienter ist.

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. So wird es der IT ermöglicht, schnell Maßnahmen zu ergreifen.

- **DDoS-Abwehr:** HPE Aruba Networking EdgeConnect SD-WAN erkennt und verhindert Angriffe wie beispielsweise Protokollangriffe, ICMP-Floods, SYN-Floods, IP-Spoofing-Angriffe usw. Mithilfe von Firewall-Schutzprofilen gewährleistet die Lösung eine strenge Handhabung von Zuständen und begrenzt die Anzahl schädlicher Anfragen durch Aktionen 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. Mit Firewall-Schutzprofilen können Administratoren unterschiedliche Niveaus von DDoS-Schutzmaßnahmen im gesamten Unternehmen durchsetzen, indem sie Firewall-Schutzprofile an Firewall-Zonen binden. Ebenso kann die Lösung eine Liste von IP-Adressen bekannter Angreifer blockieren und den Datenverkehr im Falle eines DDoS-Angriffs dynamisch über nicht betroffene Netzwerk-Links umleiten, um die Business Continuity zu gewährleisten.
- **Routing:** EdgeConnect SD-WAN unterstützt standardmäßige Layer-2- und Layer-3-Open-Networking-Protokolle wie VLAN (802.1Q), LAG (802.3ad), IPv4- und IPv6-Weiterleitung, GRE, IPsec, VRRP, WCCP, PBR, BGP (Version 4), OSPF.
- **Hochverfügbarkeit:** Der EdgeConnect SD-WAN HA-Cluster bietet Schutz vor Hardware-, Software- und Transportausfällen. Hochverfügbarkeit wird erzielt, indem Fehlertoleranz auf Netzwerkseite (WAN) und auf Geräteseite ermöglicht wird. Die EdgeConnect SD-WAN-Appliances sind über einen HA-Link miteinander verbunden, der Tunnel über jedes Underlay ermöglicht, um eine Verbindung zu beiden Appliances herzustellen.
- **Zero-Touch-Bereitstellung:** Ein Plug-and-Play-Bereitstellungsmodell ermöglicht die Bereitstellung von HPE Aruba Networking EdgeConnect SD-WAN in einer Filiale in Sekundenschnelle. Die Verbindung mit anderen EdgeConnect SD-WAN-Instanzen im Rechenzentrum, in anderen Filialen oder in Cloud-Infrastructure-as-a-Service (IaaS) wie Amazon Web Services, Microsoft Azure, Oracle Cloud Infrastructure und Google Cloud Platform wird automatisch hergestellt.
- **WAN-Härtung:** Jedes WAN-Overlay wird Edge-to-Edge mittels Tunneln mit 256-Bit-AES-Verschlüsselung geschützt. Nicht autorisierter externer Datenverkehr kann nicht in die Zweigstelle eindringen. Mit der Option, EdgeConnect SD-WAN direkt im Internet bereitzustellen, schützt die WAN-Härtung Filialen ganz ohne den Appliance-Wildwuchs und die Betriebskosten, die bei der Bereitstellung und Verwaltung dedizierter Firewalls entstehen.
- **LTE-Links:** Das HPE Aruba Networking USB-LTE-Modem ist eine praktische Lösung für Unternehmen, die schnelle WAN-Konnektivität zur Unterstützung von kleinen Büros/Homeoffice, Zweigstellen und Pop-up-Standorten benötigen, da es ein unkompliziertes Hinzufügen von primären oder Backup-LTE-WAN-Links ermöglicht. Mithilfe eines Plug-and-Play-USB-LTE-Modems mit EdgeConnect SD-WAN können Unternehmen ihre LTE-Geräte vollständig mit SD-WAN Orchestrator verwalten und dabei optimale Verbindungen zu unternehmenskritischen Anwendungen und Ressourcen gewährleisten, auch wenn die primären Verbindungen ausfallen oder unzuverlässig werden. Unser USB-LTE-Modem wird global von fast allen großen Netzbetreibern unterstützt und ist mit vielen EdgeConnect SD-WAN Gateway-Modellen kompatibel.

Wichtigste Merkmale von HPE Aruba Networking EdgeConnect SD-WAN Orchestrator

- **Verwaltung über einen zentralen Bildschirm:** Ermöglicht die schnelle und einfache Implementierung netzwerkweiter Business-Intent-Richtlinien und beseitigt somit komplexe und fehleranfällige Richtlinienänderungen in jeder Zweigstelle
- **Echtzeit-Überwachung und historische Berichterstellung:** Liefert spezifische Details zu Anwendungs-, Standort- und Netzwerkstatistiken, einschließlich einer kontinuierlichen Leistungsüberwachung auf Verluste, Latenz und Paketreihenfolge für den Netzwerkpfad jedes Unternehmenskunden. Sämtlicher HTTP- und nativer Anwendungsverkehr wird anhand von Name und Standort identifiziert, und Alarme und Warnmeldungen ermöglichen eine schnellere Behebung von Netzwerkproblemen
- **Berichte zu Bandbreitenkosteneinsparungen:** Dokumentiert die Kosteneinsparungen bei der Umstellung auf Breitbandkonnektivität

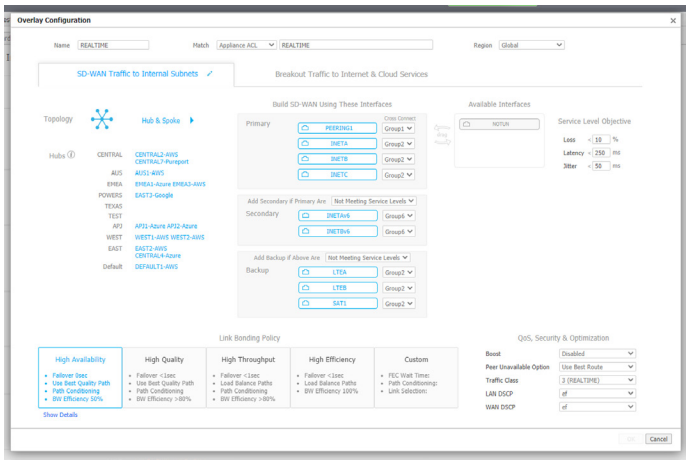


Abbildung 3. HPE Aruba Networking EdgeConnect SD-WAN Orchestrator ermöglicht die zentralisierte Definition und automatisierte Verteilung netzwerkweiter Business-Intent-Richtlinien an mehrere Filialen.

Integration mit Microsoft Azure Virtual WAN (vWAN) und AWS Transit Gateway Network Manager (TGNM)

Durch die Integration der REST-APIs von Microsoft Azure vWAN und AWS Transit Gateway Network Manager (TGNM) ermöglicht HPE Aruba Networking EdgeConnect SD-WAN Kunden den schnellen Aufbau eines Cloud-Onramps

und die Automatisierung von Netzwerkbereitstellungen. Dies macht komplexe manuelle Aufgaben zur Verbindung von Filialen mit lokalen Azure- oder AWS-Points-of-Presence (PoPs) unnötig. Die API-Integration ermöglicht HPE Aruba Networking EdgeConnect SD-WAN die Identifizierung der Standorte von Zweigstellen im Netzwerk und die Bestimmung des nächstgelegenen VPN-Gateways (vWAN-Hub oder Head-End-Gateway in AWS), mit dem eine Verbindung hergestellt werden soll. EdgeConnect SD-WAN errichtet automatisch standardbasierte IPsec-Tunnel und konfiguriert beide Tunnel-Endpunkte für jede Zweigstelle zu einem VPN-Gateway.

Wesentliche Merkmale:

- Automatisierung der Zweigstellenkonnektivität mit Azure- und AWS-Points-of-Presence (PoPs)
- Vereinfachung der Netzwerkerweiterung und Fehlerbehebung
- Schnelleres Onboarding von Anwendungen und Workloads – in und aus Azure und AWS
- Optimiertes Routing im Azure- oder AWS-Netzwerk
- Zentralisierte Netzwerküberwachung
- Globale Netzwerktransparenz
- Kohärente Richtlinienkonfiguration

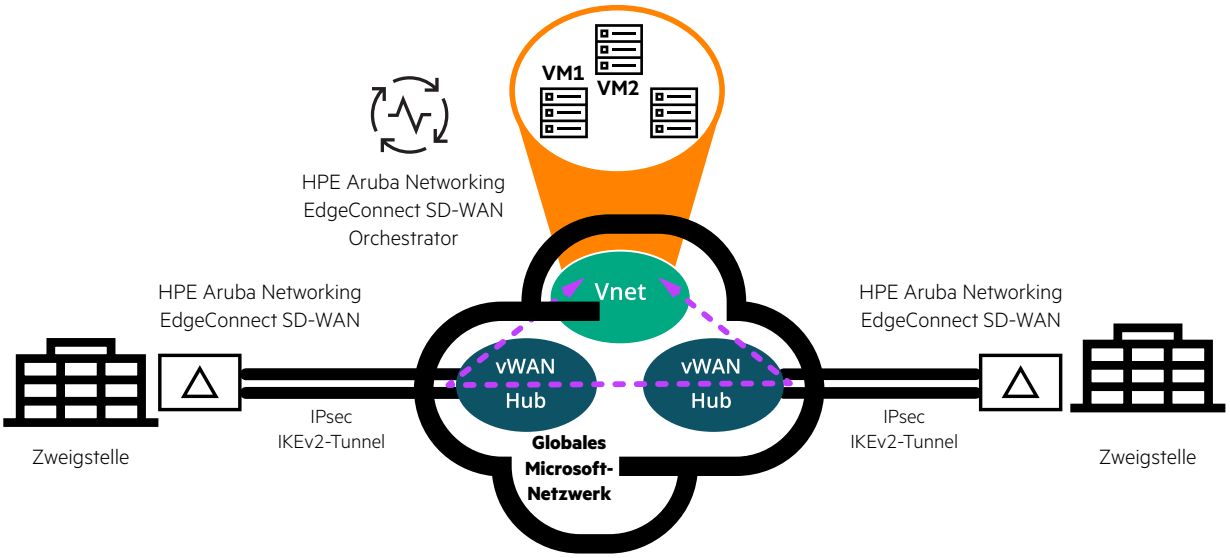


Abbildung 4. HPE Aruba Networking EdgeConnect SD-WAN Zweigstelle-zu-Cloud- und Zweigstelle-zu-Zweigstelle-Konnektivität mit vWAN

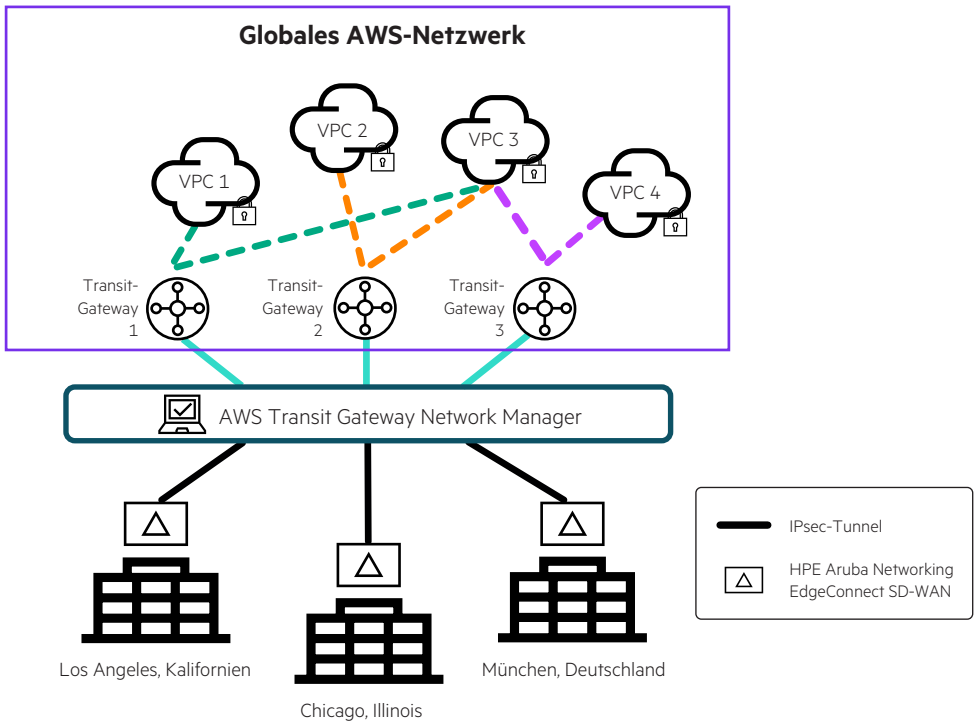


Abbildung 5. HPE Aruba Networking EdgeConnect SD-WAN Zweigstelle-zu-Cloud- und Zweigstelle-zu-Zweigstelle-Konnektivität mit AWS TGNM

Bestmögliche Qualität für Microsoft 365

Mit der REST-API-Integration für Microsoft 365 kann HPE Aruba Networking EdgeConnect SD-WAN kontinuierlich lernen und neue Microsoft 365-Endpunkte und/oder -IP-Adressen erkennen. Die Lösung wird automatisch neu konfiguriert, wenn ein neuer, näher gelegener Microsoft 365-Endpunkt verfügbar wird. Auf diese Weise erhalten die Benutzer stets eine optimale Microsoft 365-Konnektivität und -Leistung, da die Round-Trip-Time (RTT) reduziert wird. HPE Aruba Networking EdgeConnect SD-WAN wurde unabhängig getestet und für die Unterstützung der Konnektivitätsprinzipien von Microsoft 365 zertifiziert. Als Ergebnis der unabhängigen Tests wurde die EdgeConnect SD-WAN-Plattform in das Microsoft 365 Networking Partner Program aufgenommen und erhielt die offizielle Bezeichnung „Works with Microsoft 365".

Ausweitung der WAN-Fabric auf die Cloud

Stellen Sie virtuelle HPE Aruba Networking EdgeConnect SD-WAN-Appliances in einer Public Cloud wie AWS, Azure, Google Cloud Platform oder Oracle Cloud bereit, um die Verbindungen zwischen Filialstandorten und der Cloud zu optimieren und dabei von sämtlichen Vorteilen von SD-WAN zu profitieren. Bei einem Stromausfall wird der Datenverkehr über den/die verbleibenden Link(s) weitergeführt, sodass die Benutzer keine Unterbrechung von Sprachanrufen, Audio- und Videokonferenzen oder anderen Anwendungen bemerken. Das robuste erste Stück zwischen der Zweigstelle und der Public Cloud bietet eine bessere Netzwerkleistung, Zuverlässigkeit und Qualität.

AppExpress

AppExpress optimiert das Benutzererlebnis von unternehmenskritischen Anwendungen – privaten und SaaS-Anwendungen – wie Zoom, Workday, SAP, Microsoft 365 und weiteren Anwendungen. AppExpress macht sich die Pfadvielfalt von SD-WAN zunutze und wählt automatisch den besten Pfad für jede Anwendung aus. Mithilfe von synthetischer Abtastung und Echtzeit-Beobachtung des Benutzerverkehrs steuert diese Funktion den Datenverkehr intelligent und unabhängig vom Breakout des Anwendungsverkehrs. Dies umfasst:

- **Lokaler Breakout:** Der Datenverkehr wird effizient unter automatischer Auswahl des besten Links im Hinblick auf optimale Leistung über MPLS, Internet, 4G/5G oder Satellitenlinks geleitet.
- **Optimierte Steuerung zu IaaS:** Das System steuert den Datenverkehr automatisch zu einer virtuellen Instanz von HPE Aruba Networking EdgeConnect SD-WAN, die auf IaaS-Plattformen wie AWS, Azure oder Google Cloud gehostet wird, und gewährleistet so einen effizienten Datenfluss.
- **SSE-PoP:** AppExpress wählt den besten SSE-Point-of-Presence (PoP) mit der höchsten Leistung und verbessert damit das Benutzererlebnis.

Um zu bestimmen, wie der Datenverkehr zu steuern ist, und um die Leistung zu melden, nutzt AppExpress den Application Performance Index bzw. Apdex. Apdex ist ein Industriestandard zur Messung des Benutzererlebnisses auf der Grundlage einer Stichprobe von Latenzmessungen mit normalisierter Punktzahl zwischen 0 und 100. Zur Berechnung der Apdex-Punktzahl wird jede Messung in drei Reaktionsfähigkeitskategorien unterteilt: „Satisfied" (Zufrieden), „Tolerating" (Annehmbar) und „Frustrated" (Frustriert).

Die Apdex-Punktzahl wird kontinuierlich überwacht, damit je nach Netzwerkbedingungen dynamisch der beste Pfad ausgewählt werden kann. Damit ist sichergestellt, dass Benutzer beim Zugriff auf kritische Geschäftsanwendungen von einem einzigartigen Benutzererlebnis profitieren.

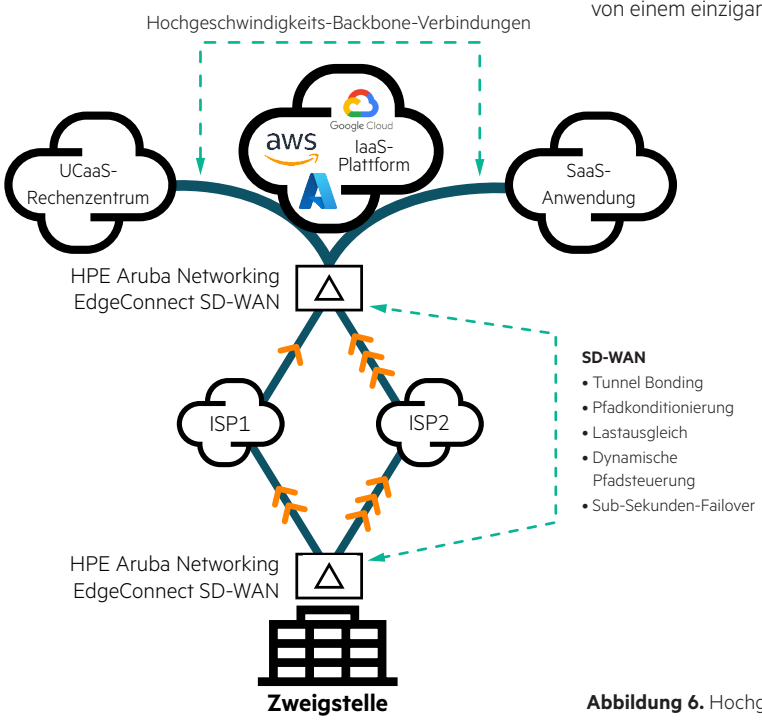


Abbildung 6. Hochgeschwindigkeits-Backbone-Verbindungen

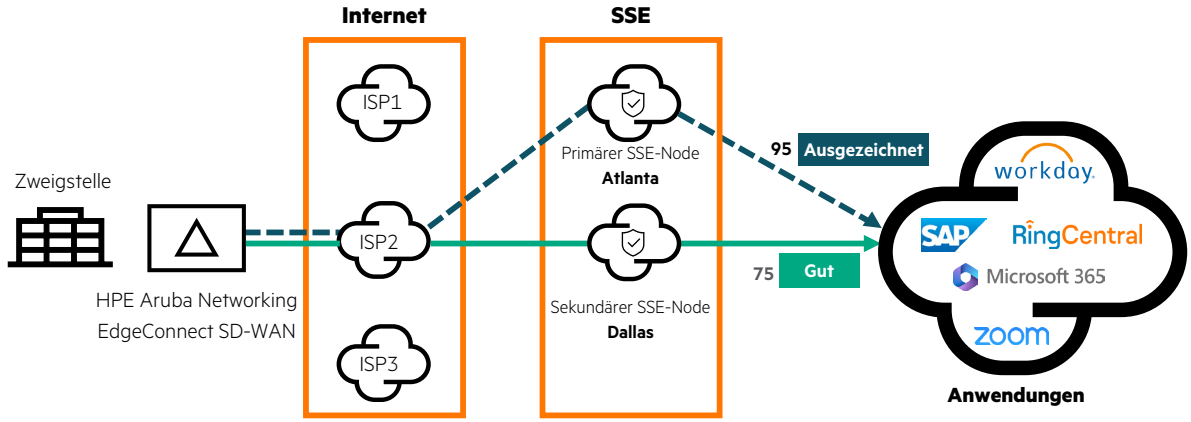


Abbildung 7. Optimierung der Anwendungsleistung, einschließlich SSE-Onramp mit AppExpress

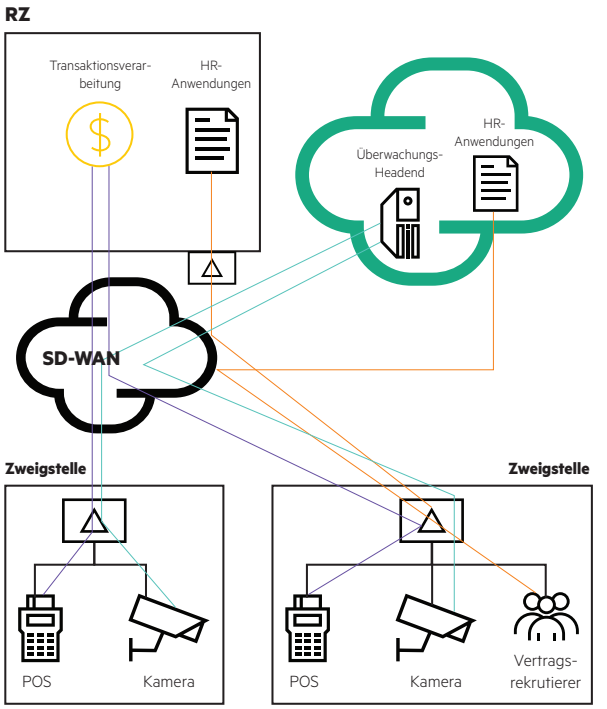
Zero Trust: Schutz des Edge nach Rolle, Kontext und Anwendung

Angesichts der Zunahme von Mobilgeräten, Remote-Mitarbeitenden, in der Cloud gehosteten Anwendungen und IoT-fähigen Geräten müssen Unternehmen ihre Sicherheitsrichtlinien auf der Grundlage ihrer geschäftlichen Absichten ausrichten, dürfen dabei aber auch die Konsistenz nicht außer Acht lassen. Die Integration von HPE Aruba Networking ClearPass mit HPE Aruba Networking EdgeConnect SD-WAN erweitert die Anwendungsintelligenz um Benutzer- und Geräteidentität sowie rollenbasierte Richtlinien und ermöglicht somit eine fein abgestufte Segmentierung. Dieser zusätzliche identitätsbasierte Kontext ermöglicht eine konsistente Durchsetzung von Sicherheitsrichtlinien, die netzwerkweit vom Edge bis zur Cloud durchgesetzt werden können, und beschleunigt gleichzeitig die Fehlerbehebung und Problemlösung.

Wenn sich ein neuer Benutzer bzw. ein neues Gerät mit dem Netzwerk verbindet und über ClearPass registriert wird, stellt HPE Aruba Networking EdgeConnect SD-WAN Orchestrator eine Verbindung zur ClearPass API her. Der SD-WAN Orchestrator gibt sämtliche Sicherheitsrichtlinieninformationen in Bezug auf Benutzer, Gerätetyp, Rolle und Sicherheitsniveau an alle EdgeConnect SD-WAN-Appliances im Netzwerk weiter.

Da IoT-Geräte agentenlos sind, ist es nicht möglich, einen VPN- oder ZTNA-Client eines Drittanbieters auf ihnen auszuführen. Daher bewältigt eine SASE-Architektur nicht sämtliche Sicherheitsherausforderungen von IoT-Geräten im Unternehmensnetzwerk. Mit dem ClearPass Zero-Trust-Sicherheitsframework kann das Netzwerk IoT-Geräte und -Datenverkehr an der Netzwerkperipherie identifizieren und segmentieren und von anderem Datenverkehr im Netzwerk isolieren. Diese Kontextebene ermöglicht eine fein abgestimmte Segmentierung ohne komplexes Management mehrerer VLANs.

Beispielsweise kann eine fein abgestimmte Segmentierungsrichtlinie verhindern, dass IoT-Sicherheitskameras auf Kreditkartentransaktionen oder HLK-Systeme zugreifen. Eine dynamische Zero-Trust-Segmentierung hilft Unternehmen dabei, potenzielle Sicherheitsbedrohungen nach Gerätetyp, Rolle und Anwendung zu isolieren, und unterstützt sie bei der Erfüllung von Compliance-Vorgaben wie PCI, HIPAA und SOX.



Zero-Trust-Segmentierung ermöglicht, dass Benutzer und Geräte nur mit solchen Zielen kommunizieren können, die ihrer Rolle im Unternehmen entsprechen.

Abbildung 8. Zero-Trust-Segmentierung ermöglicht, dass Benutzer und Geräte nur mit solchen Zielen kommunizieren können, die ihrer Rolle im Unternehmen entsprechen.

Segmentierung mit virtuellem Routing und Forwarding (VRF)

Netzwerkmanager können mit HPE Aruba Networking EdgeConnect SD-WAN separate Adressierungs-, Routing- und Sicherheitsrichtlinien konfigurieren und verwalten. Diese werden konsistent auf End-to-End-Segmente und -Mikrosegmente für Datenverkehr angewendet, der die Netzwerke von großen multinationalen Unternehmen und Verbänden von unabhängigen Unternehmen durchquert.

Fortschrittliche Segmentierung beseitigt die anstrengende Aufgabe, VRF-, Firewall- und NAT-Richtlinien in Handarbeit konsistent zusammenzufügen. So vereinfacht sie das Management diverser Szenarien erheblich und bietet beispiellose Flexibilität bei der Handhabung überlappender IP-Adressbereiche.

Splunk-Integration

SIEM-Tools (Security Information and Event Management) helfen bei der proaktiven Identifizierung potenzieller Sicherheitsbedrohungen und Schwachstellen, bevor diese den Geschäftsbetrieb unterbrechen und Einnahmen beeinträchtigen können. HPE Aruba Networking hat eine spezielle Anwendung für Splunk eingeführt: die HPE Aruba Networking EdgeConnect Security App. Diese App kann ganz einfach von Splunkbase heruntergeladen werden und nutzt die von der HPE Aruba Networking EdgeConnect SD-WAN-Plattform bereitgestellten Daten mit den umfassenden Untersuchungs- und Visualisierungsfunktionen von Splunk, um erweiterte Sicherheitsberichte und Analysen auszugeben. Die EdgeConnect Security App ist mit Splunk Enterprise und Splunk Cloud kompatibel und bietet eine Dashboard-Ansicht aller Benachrichtigungen über Sicherheitsereignisse, die von EdgeConnect SD-WAN-Geräten stammen. Mithilfe von Splunk kann die IT die gesammelten Benachrichtigungen über Sicherheitsereignisse, die in der gesamten SD-WAN-Fabric generiert wurden, allgemeine Trends und Top-Talker filtern, sortieren, navigieren und anzeigen, um Unternehmen bei der Erkennung von Netzwerkereignissen zu unterstützen, die eine weitere Untersuchung erfordern.

Unterstützung für benutzerdefinierte Anwendungen

Viele Unternehmen unterstützen nach wie vor Anwendungen, die speziell für das Unternehmen angepasst wurden um im Rechenzentrum des Unternehmens gehostet werden. Solche benutzerdefinierten Anwendungen sind von kritischer Bedeutung für das Unternehmen, und mit HPE Aruba Networking EdgeConnect SD-WAN können Benutzer die optimale Leistung dieser Anwendungen gewährleisten. Über HPE Aruba Networking EdgeConnect SD-WAN Orchestrator kann die IT mühelos eine benutzerdefinierte Anwendungsdefinition konfigurieren, die EdgeConnect SD-WAN die Identifizierung solcher Anwendungen im ersten Paket ermöglicht.

Effiziente Auflösung von DNS-Anfragen

Ein kritischer Schritt im DNS-Proxy ist die schnelle Auflösung von DNS-Anfragen. Mit HPE Aruba Networking EdgeConnect SD-WAN können Kunden DNS-Server in der Nähe von Zweigstellen erreichen und so das Backhauling der DNS-Anfrage in Remote-Rechenzentren, in denen die DNS-Server des Unternehmens gehostet werden, vermeiden. In der Zweigstelle selbst können DNS-Anfragen direkt an globale DNS-Server gesendet werden. Dies verringert die Auswirkungen von Latenz bei der Einrichtung von SaaS-Anwendungssitzungen und verbessert somit die SaaS-Anwendungsleistung.

SD-WAN Orchestrator ermöglicht schnellere SD-WAN-Bereitstellungen

HPE Aruba Networking EdgeConnect SD-WAN Orchestrator ermöglicht die Zero-Touch-Bereitstellung von HPE Aruba Networking EdgeConnect SD-WAN-Appliances in Zweigstellen. SD-WAN Orchestrator automatisiert die Zuweisung von Business-Intent-Richtlinien, um eine schnellere und einfachere Konnektivität zwischen mehreren Zweigstellen zu gewährleisten. So verhindert er die Konfigurationsabweichungen, die durch die manuelle Aktualisierung von Regeln und Zugriffskontrolllisten (ACLs) Standort für Standort entstehen können.

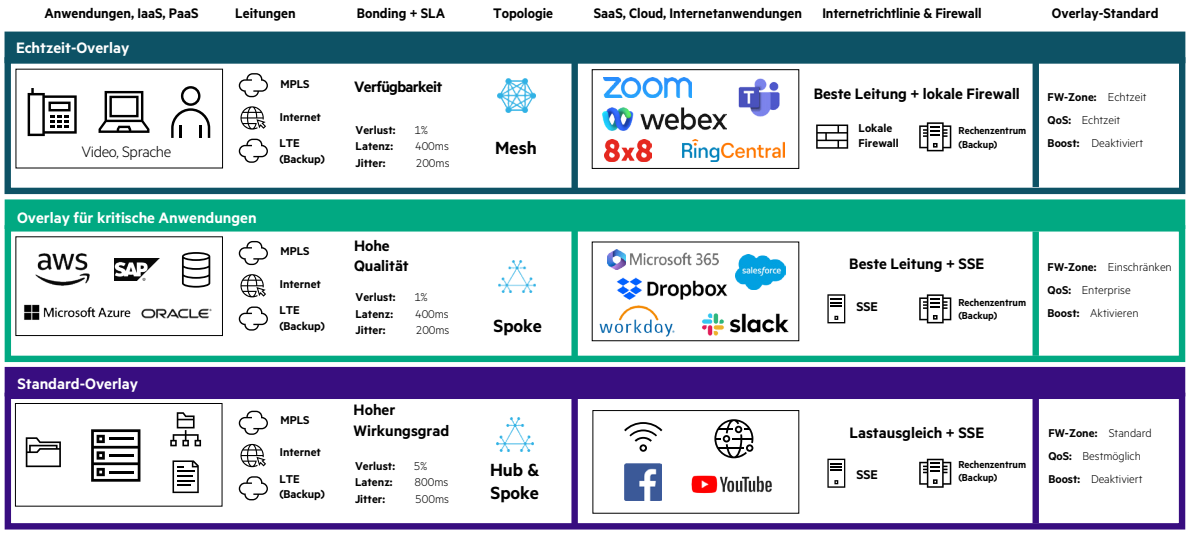


Abbildung 9. Mit HPE Aruba Networking EdgeConnect SD-WAN Orchestrator konfigurierte Business Intent Overlays

Mit HPE Aruba Networking EdgeConnect SD-WAN Orchestrator können Kunden:

- WAN-Neukonfigurationen vermeiden, indem Benutzern die Anwendungen in speziellen virtuellen Overlays zur Verfügung gestellt werden
- Die Anwendungsbereitstellung durch virtuelle WAN-Overlays auf der Grundlage der geschäftlichen Absicht an Geschäftszielen ausrichten
- Zweigstellenbereitstellungen mit EdgeConnect SD-WAN-Profilen vereinfachen, in denen die virtuelle und physische Konfiguration des Standorts beschrieben wird

Zusätzlich zur zentralisierten und automatisierten Kontrolle der gesamten SD-WAN-Topologie liefert SD-WAN Orchestrator spezifische Details zur WAN-Leistung:

- Detaillierte Berichte zu Anwendungs-, Standort- und Netzwerkstatistiken
- Kontinuierliche Leistungsüberwachung von Durchsatz, Verlust, Latenz, Jitter und Paketreihenfolge für alle Netzwerkpfade
- Identifizierung von sämtlichem Anwendungsverkehr nach Name und Standort
- Alarme und Warnmeldungen zur Visualisierung und Priorisierung von Software- und Hardwareproblemen im WAN ermöglichen eine schnellere Problemlösung
- Bericht zu Bandbreitenkosteneinsparungen zur Dokumentation der Kosteneinsparungen durch die Umstellung auf Breitband

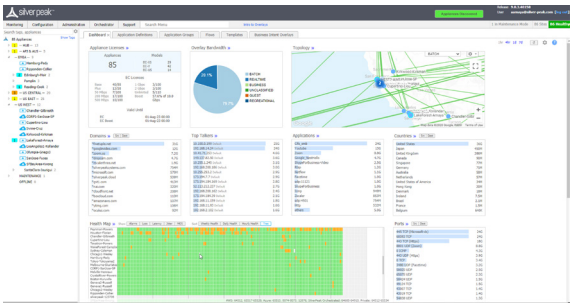


Abbildung 10. HPE Aruba Networking EdgeConnect SD-WAN Orchestrator ermöglicht zentralisiertes und automatisiertes Overlay-Management.

Kontrolle über die Cloud

Machen Sie sich ein genaues Bild davon, wie Infrastructure-as-a-Service (IaaS) und Software-as-a-Service (SaaS) in Ihrem Unternehmen zum Einsatz kommen.

- Namensbasierte Identifizierung und Meldung aller Cloud-Anwendungen
- Tracking des Netzwerkverkehrs von SaaS-Anbietern
- Cloud-Intelligenz stellt eine Internet-Zuordnung für den optimalen Zugang zu SaaS-Services bereit

Sicherheit vom Edge bis zur Cloud

Cloud-basierte Sicherheit wird immer wichtiger, daher lässt sich HPE Aruba Networking EdgeConnect SD-WAN nahtlos in HPE Aruba Networking SSE integrieren und bildet so eine einheitliche SASE-Plattform, die die SASE-Bereitstellung beschleunigt und das Management vereinfacht. Diese integrierte Plattform bietet moderne Sicherheitsfunktionen wie ZTNA (Zero-Trust-Netzwerkzugriff), SWG (Secure Web Gateway) und CASB (Cloud Access Security Broker), um die Netzwerk- und Sicherheitsherausforderungen von Cloud-orientierten Unternehmen und hybriden Arbeitsszenarien zu bewältigen. Insbesondere bietet sie robuste webbasierte Bedrohungsabwehr und Datensicherung für SaaS-Anwendungen und gewährleistet einen sicheren Zugriff für Remote-Mitarbeitende.

Darüber hinaus optimiert die EdgeConnect SD-WAN-Lösung den Orchestrierungsprozess für SSE-Drittanbieter und bietet Unternehmen die nötige Flexibilität, damit sie SASE mit den Sicherheitsservices ihrer Wahl einführen oder reibungslos in ein bestehendes Sicherheitsökosystem integrieren können.

Der sichere Internet-Breakout ist eine wichtige Funktion, die den Datenverkehr intelligent und im Einklang mit den vorgegebenen Sicherheitsrichtlinien, gesetzlichen Vorschriften und geschäftlichen Absichten an SSE-Services, Rechenzentren oder die Cloud leitet.

Die SD-WAN-Lösung beinhaltet integrierte Next-Generation-Firewall-Funktionen, sodass Unternehmen Legacy-Firewalls in ihren Filialen austauschen können. Zudem stellt sie Unternehmen fortschrittliche Mechanismen zur Bedrohungsabwehr zur Verfügung, z. B. Angriffserkennung und -verhinderung sowie DDoS-Schutz.

Um die Sicherheit noch weiter zu stärken, ermöglicht die Lösung die dynamische Segmentierung von Benutzern, Anwendungen und WAN-Services in sichere Zonen auf der Grundlage von Identität, Zugriffsberechtigungen und Sicherheitsniveau. Unter Anwendung des Prinzips der geringsten Zugriffsrechte stellt sie sicher, dass Benutzer und Geräte nur mit solchen Zielen kommunizieren können, die mit ihren jeweiligen Rollen übereinstimmen.

IT-Teams profitieren von einer zentralisierten und automatisierten Steuerung von Sicherheitsrichtlinien durch Zero-Touch-Bereitstellung, Optimierung von Managementprozessen und Minimierung von Konfigurationsfehlern.

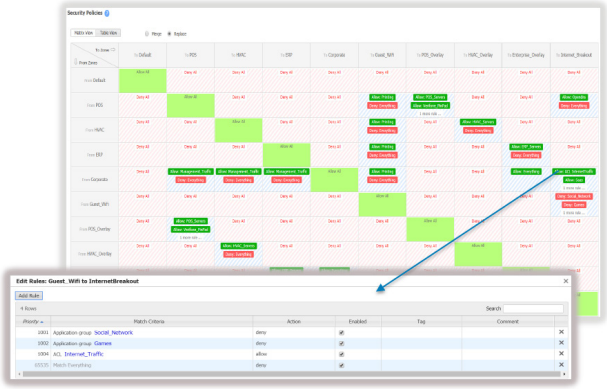


Abbildung 11. Eine Matrixansicht von HPE Aruba Networking EdgeConnect SD-WAN Orchestrator bietet eine einfach zu lesende und intuitive Visualisierung der konfigurierten Zonen und der definierten Ausnahmen auf der Whitelist.

Secure SD-WAN-Zertifizierung durch ICSA Labs

Die HPE Aruba Networking EdgeConnect SD-WAN-Plattform hat die Secure SD-WAN-Zertifizierung von ICSA Labs erhalten. Hierfür musste sie strenge Tests auf Basis einer umfassenden und robusten Reihe von SD-WAN-Funktionen und Anforderungen an die Plattformsicherheit bestehen.

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

- **Erweiterte SD-WAN-Funktionen** wie Tunnel Bonding, dynamische Pfadauswahl und Zero-Touch-Bereitstellung
- **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**

Die weltweit anerkannte Zertifizierung bescheinigt die Verwendung einer sicheren SD-WAN-Lösung, die von einer unabhängigen Drittorganisation zertifiziert wurde. Ebenso wird Unternehmen die Vereinfachung ihrer Netzwerkarchitektur ermöglicht, indem sie traditionelle Zweigstellen-Firewalls sicher durch HPE Aruba Networking EdgeConnect SD-WAN ersetzen.

Steigerung der Anwendungsleistung nach Bedarf

HPE Aruba Networking EdgeConnect WAN Optimization ist ein optionales Leistungspaket mit folgenden Inhalten:

- **Latenzverringerung:** Beschleunigungstechniken für TCP und weitere Protokolle werden auf sämtlichen Datenverkehr angewendet, um die Auswirkungen von Latenz auf die Anwendungsleistung zu minimieren und die Reaktionszeiten von Anwendungen im gesamten WAN erheblich zu verbessern.
- **Datenreduktion:** Durch Datenkomprimierung und -deduplizierung wird die wiederholte Übertragung duplizierter Daten verhindert. WAN Optimization untersucht den WAN-Datenverkehr auf Byte-Ebene und speichert Inhalte in lokalen Datenspeichern. Moderne Fingerprinting-Techniken erkennen sich wiederholende Muster für die lokale Bereitstellung. Die Datenreduktion kann auf alle IP-basierten Protokolle angewendet werden, inklusive TCP und UDP.

Was spricht für WAN Optimization?

HPE Aruba Networking EdgeConnect SD-WAN-Appliances allein ermöglichen eine bessere Anwendungsleistung für Breitband- oder hybride WAN-Bereitstellungen. Hierzu nutzen sie das integrierte paketbasierte Tunnel Bonding, dynamische Pfadkontrolle (DPC) und Pfadkonditionierung, um die nachteiligen Auswirkungen von Paketverlusten und ungeordneten Paketen zu überwinden, die häufig bei Internetverbindungen auftreten.

Allerdings wird manchmal zusätzliche Leistung für bestimmte Anwendungen oder Standorte benötigt. Wenn die Distanz zwischen zwei Standorten über das WAN zunimmt, wird die Anwendungsleistung schwächer. Dies ist nicht auf die verfügbare Bandbreite zurückzuführen, sondern vielmehr auf die Zeit, die benötigt wird, um Datenpakete über die Distanz zu senden und zu empfangen, sowie darauf, wie oft Daten erneut gesendet werden müssen.

Anwendungsbeispiele für WAN Optimization

- Kunden, die eine Datenreplikation an einen DR-Standort (Disaster Recovery) in Tausenden Kilometern Entfernung durchführen, sollten mit WAN Optimization sicherstellen, dass ihre Recovery Point Objectives (RPOs) nicht gefährdet werden.
- Unternehmen mit Remote-Standorten in ländlichen Gebieten oder mit Standorten, die sehr weit vom Rechenzentrum des Unternehmens entfernt sind, sollten mithilfe von WAN Optimization die Auswirkungen von hoher Latenz ausgleichen. Mit diesem Leistungspaket erhalten Kunden die nötige Flexibilität, um verbesserte WAN-Optimierungsfunktionen überall dort zu ermöglichen, wo sie für eine vollständig integrierte Lösung benötigt werden.

Ausgleichen der Auswirkungen von Latenz

Die Zeit, die benötigt wird, um Informationen vom Absender zum Empfänger und zurück zu senden, wird als Netzwerklatenz bezeichnet. Da die Lichtgeschwindigkeit eine Konstante ist, ist die WAN-Latenz direkt proportional zur zurückgelegten Distanz zwischen den zwei Netzwerkendpunkten. Wir bieten eine Reihe von TCP-Beschleunigungstechniken zum Ausgleich der WAN-Latenz, darunter Window Scaling, Selective Acknowledgement, Round-Trip Measurement und High Speed TCP.

Windows und andere Anwendungen, die sich auf das Common Internet File System (CIFS) verlassen, brauchen oftmals mehr Zeit, um häufige Dateivorgänge über die Distanz auszuführen, beispielsweise den Abruf und die Freigabe von Dateien. WAN Optimization hilft diesen Anwendungen, indem sie nicht nur den zugrundeliegenden TCP-Transport verbessert, sondern auch CIFS durch CIFS Read-Ahead, CIFS Write-Behind und CIFS-Metadatenoptimierungen beschleunigt.

Erhöhung des Durchsatzes

Wenn Pakete über HPE Aruba Networking EdgeConnect SD-WAN-Appliances fließen, untersucht WAN Optimization den WAN-Datenverkehr auf Byte-Ebene und speichert Inhalte in lokalen Datenspeichern. Kommen neue Pakete an, berechnet sie die Fingerabdrücke der Daten innerhalb der Pakete und prüft, ob diese Fingerabdrücke mit den lokal gespeicherten Daten übereinstimmen.

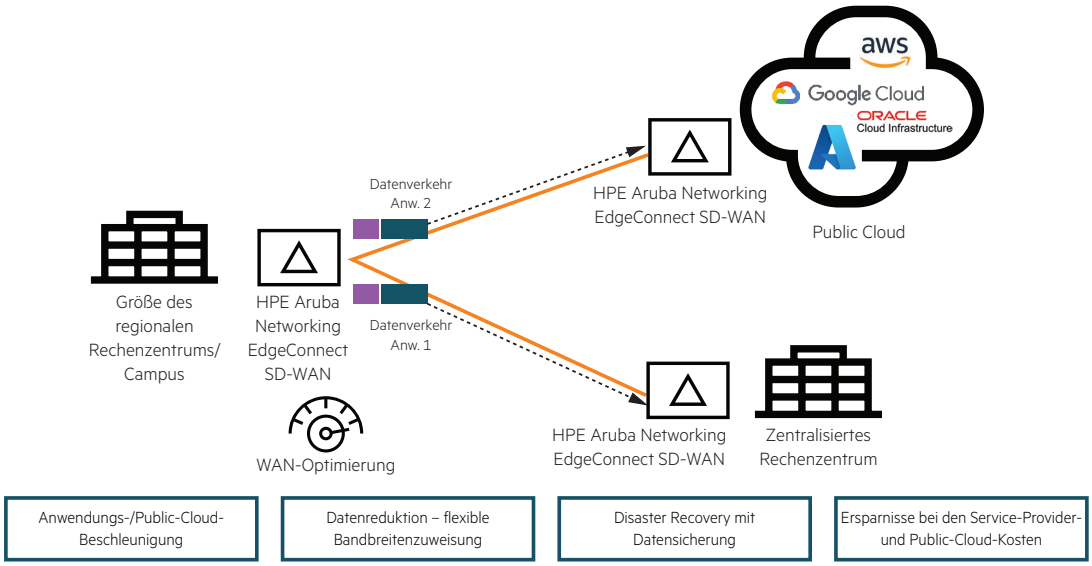


Abbildung 12. HPE Aruba Networking EdgeConnect WAN Optimization beschleunigt Anwendungen und maximiert die verfügbare Bandbreite für andere Anwendungen

HPE Aruba Networking EdgeConnect SD-WAN-Hardwareportfolio

	EdgeConnect SD-WAN US	EdgeConnect SD-WAN 10104	EdgeConnect SD-WAN XS	EdgeConnect SD-WAN 10106	EdgeConnect SD-WAN S-P	EdgeConnect SD-WAN M-H	EdgeConnect SD-WAN L-H	EdgeConnect SD-WAN XL-H
								
Modell	EC-US	EC-10104	EC-XS	EC-10106	EC-S-P	EC-M-H*	EC-L-H*	EC-XL-H*
Typische Bereitstellung	Kleine Zweigstelle/ Homeoffice	Kleine Zweigstelle/ Homeoffice	Kleine Zweigstelle	Kleine Zweigstelle	Große Zweigstelle	Hauptsitz/RZ Großer Hub	Großer Rechenzentrums-Hub	Großer Rechenzentrums-Hub
Typische WAN-Bandbreite**	1–200 Mbit/s	2–500 Mbit/s	2–1000 Mbit/s	2–1000 Mbit/s	10–3000 Mbit/s	50–5000 Mbit/s	2–10 Gbit/s	2–10 Gbit/s
Gleichzeitige Verbindungen	256.000	256.000	256.000	256.000	256.000	2.000.000	2.000.000	2.000.000
Empfohlene WAN-Optimierung bis zu	25 Mbit/s	200 Mbit/s	250 Mbit/s	250 Mbit/s	500 Mbit/s	1 Gbit/s	1 Gbit/s	5 Gbit/s
IDS/IPS	Nicht unterstützt	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Redundanz/ FRUs*	Nein	Nein	Nein	Nein	SSD und Stromversorgung (AC oder DC)	SSD und Stromversorgung	SSD und Stromversorgung	SSD, NVMe, Stromversorgung
Datenpfad-Schnittstellen	3x RJ45 10/100/1000	4x RJ45 10/100/1000	4x RJ45 10/100/1000	2x 10G SFP+ 2x Combo (SFP/1 GbE) 2x GbE (PoE)	8x RJ45 4x 1/10G optisch	8x RJ45 4x 1/10G optisch	6x 1/10G optisch	6x optische Schnittstellen EC-XL-H: 6x 1/10/25G EC-XL-H-10G: 6x 1/10G

* EC-XL-H und EC-XL-H-10G sind für maximale WAN-Optimierung ab Werk mit NVMe ausgestattet

** EC-S-P, EC-M-H, EC-L-H und EC-XL-H unterstützen einsteckbare optische Einheiten

*** Siehe Softwarekompatibilitätstabelle für die mindestens erforderlichen Software-Releases zur Unterstützung der neuen EC-H-Modelle

**** Bei der WAN-Bandbreite wird von bidirektionalem Datenverkehr ausgegangen (symmetrischer Uplink und Downlink). Für den Gesamtdurchsatz des WAN (Rx+Tx) multiplizieren Sie diese Zahlen mit 2.

***** Für die bestmögliche Leistung wird EdgeConnect SD-WAN Betriebssystemversion 9.1 oder neuer empfohlen

****** FRU-Netzteile sind eine zusätzliche SKU

HPE Aruba Networking EdgeConnect SD-WAN-Plattform – Datenblätter

ULTRAKLEIN | 10104 | EXTRAKLEIN | 10106

KLEIN | MITTELGROSS | GROSS | EXTRAGROSS

HPE Aruba Networking EdgeConnect SD-WAN – technischer Support

Laufzeit	Support ist in der HPE Aruba Networking EdgeConnect SD-WAN-Abonnementlizenz inbegriffen
Webbasiertes Support-Portal	Unbegrenzter Zugriff rund um die Uhr mit Software-Downloads, technischer Dokumentation und Online-Wissensdatenbank
Software-Updates	Große und kleine Feature-Releases; Wartungs-Releases
Technischer Support	Rund um die Uhr, telefonisch/E-Mail/Web (globale Technical Assistance Center – TAC)
Reaktionszeit	30 Minuten bei hoher Priorität (P1) – kritisch
Hardwaregarantie und -wartung	Weitere Informationen zu den Garantie- und Wartungsrichtlinien von HPE Aruba Networking EdgeConnect SD-WAN finden Sie im Datenblatt

Flexible Bereitstellungsmodelle

- HPE Aruba Networking EdgeConnect SD-WAN Virtual (EC-V): Ermöglicht weltweit das Herunterladen und Installieren von EdgeConnect SD-WAN. Die Software kann auf allen gängigen Hypervisoren ausgeführt werden, darunter VMware ESXi, Microsoft Hyper-V, Citrix XenServer und KVM. Kunden, die über eine IaaS-Präsenz in AWS, Microsoft Azure, Oracle Cloud Infrastructure oder Google Cloud Platform verfügen, können EdgeConnect SD-WAN in ihrer gehosteten Cloud-Umgebung bereitstellen.
- EdgeConnect SD-WAN Physical (EC): Unternehmen, die über keine Virtualisierung in Zweigstellen verfügen, können eines der EdgeConnect SD-WAN-Hardware-Appliance-Modelle für die Plug-and-Play-Bereitstellung auswählen.

HPE Aruba Networking EdgeConnect SD-WAN-Abonnementlizenzen

Die HPE Aruba Networking EdgeConnect SD-WAN-Plattform ist als Software-Abonnement verfügbar. Ihnen stehen zwei Abonnementstufen (Foundational und Advanced) mit ein- oder mehrjährigen Laufzeiten (1, 2, 3, 4, 5, 6 und 7 Jahre) und mit mehreren Bandbreitenstufen zur Verfügung.
Der gemischte Einsatz von Abonnementstufen wird nicht unterstützt, d. h. auf jeder EdgeConnect SD-WAN-Appliance in einer SD-WAN-Fabric muss entweder die Foundational- oder die Advanced-Lizenz ausgeführt werden.

Foundational-Lizenzstufe: Die Foundational-Lizenzstufe beinhaltet grundlegende SD-WAN-Funktionen sowie alle erweiterten NGFW-Funktionen. Die Foundational-Lizenz ist mit Bandbreiten von 100 Mbit/s, 1 Gbit/s und 10 Gbit/s verfügbar.

Außerdem unterstützt die Foundational-Lizenz Hub-and-Spoke-Topologien (4 Hubs/Region) und eine begrenzte Anzahl an VRFs und enthält ein HPE Aruba Networking EdgeConnect SD-WAN Orchestrator Abonnement (Foundation OaaS). Die Foundational-Lizenz unterstützt drei BIOs sowie alle wesentlichen QoS-Parameter und grundlegenden Datenaufbewahrungsfunktionen. Damit eignet sie sich ideal für Kunden, die ein einfaches, managementfreundliches SD-WAN mit umfassenden NGFW-Funktionen benötigen.

Advanced-Lizenzstufe: Die Advanced-Lizenzstufe beinhaltet alle erweiterten SD-WAN-Funktionen von HPE Aruba Networking EdgeConnect SD-WAN sowie alle erweiterten NGFW-Funktionen. Die Advanced-Lizenz ist mit Bandbreiten von 20 Mbit/s, 50 Mbit/s, 100 Mbit/s, 200 Mbit/s, 500 Mbit/s, 1 Gbit/s, 2 Gbit/s sowie unbegrenzter Bandbreite verfügbar. Darüber hinaus unterstützt die Advanced-Lizenz unbegrenzte Topologien und 64 VRFs und enthält ein in der Cloud gehostetes HPE Aruba Networking EdgeConnect SD-WAN Orchestrator Abonnement (Advanced OaaS). Advanced OaaS richtet sich an Unternehmen, die eine SD-WAN-Managementlösung ohne CapEx und ohne den Kapitalaufwand und die Komplexität des Managements einer On-Premises-Infrastruktur bevorzugen. Die Advanced-Lizenz unterstützt bis zu sieben BIOs, erweiterte QoS-Parameter und erweiterte Datenaufbewahrungsfunktionen. Damit eignet sie sich ideal für Kunden, die keine Kompromisse bei ihren SD-WAN-Funktionen eingehen wollen und umfassende NGFW-Funktionen erwarten.

Unternehmen, die eine On-Premises-Bereitstellung von HPE Aruba Networking SD-WAN Orchestrator benötigen, können mit der Advanced On-Premises-Lizenzstufe eine separate Reihe von SKUs erwerben. Die On-Premises-Edition der Advanced-Lizenz bietet den gleichen umfassenden Funktionsumfang wie die Advanced-Lizenz, ermöglicht Unternehmen allerdings das Management ihrer eigenen Instanz von SD-WAN Orchestrator. Sie eignet sich insbesondere für Kunden, die eine private Installation ihrer SD-WAN-Managementsoftware benötigen.

Optionale Lizenzen für HPE Aruba Networking EdgeConnect SD-WAN

Dynamic Threat Defense: Unternehmen, die umfassende, in EdgeConnect SD-WAN integrierte IDS-/IPS-Funktionen benötigen, können optional die Lizenz für Dynamic Threat Defense bereitstellen.

WAN Optimization: HPE Aruba Networking EdgeConnect WAN Optimization ist ein optionales Leistungspaket, das flexibel bestellt und an Standorten bereitgestellt werden kann, die eine Anwendungsbeschleunigung benötigen. WAN Optimization wird in Blöcken von 100 Mbit/s oder 10 Gbit/s angeboten.

Darüber hinaus können große globale Unternehmen mit mehreren Geschäftsbereichen (BUs) oder Tochterunternehmen, die unterschiedliche regionale QoS- oder Sicherheitsrichtlinien unterstützen müssen, optional HPE Aruba Networking SD-WAN Orchestrator Global Enterprise bereitstellen (nicht zutreffend für Advanced On-Premises-Lizenz).

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

Kontakt

Besuchen Sie **ArubaNetworks.com**

Hewlett Packard Enterprise

DS_Aruba-EdgeConnect-Solution_AG_022124 a00109847dee