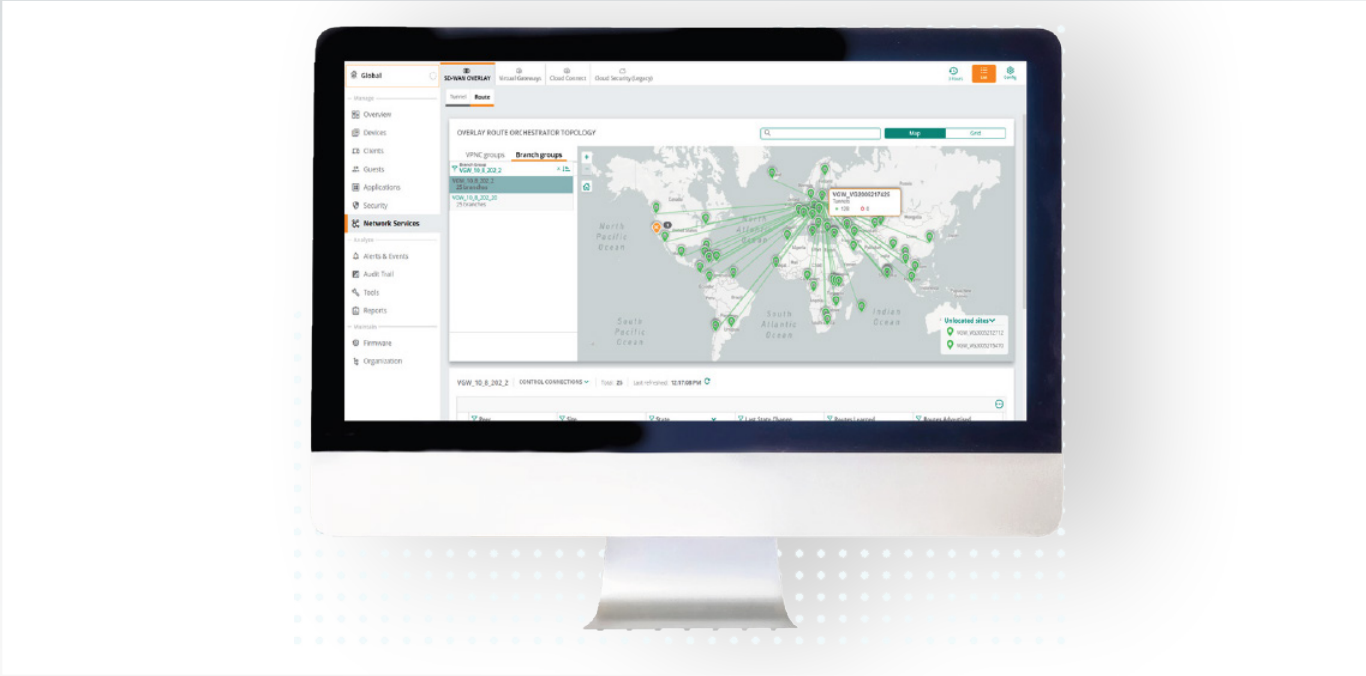
HPE aruba networking

Datenblatt



HPE Aruba Networking EdgeConnect SD- Branch

Abdeckung der gesamten Benutzererfahrung in Remote-Zweigstellen vom Edge bis zur Cloud mit einheitlichem Management, AIOps und Sicherheit für kabelgebundene, Wireless- und WAN-Netzwerke

HPE

Wichtigste Funktionen

— Einheitlicher SASE mit HPE Aruba Networking SSE oder orchestrierte SSE-Integration

— Policy Enforcement Firewall, Deep Packet Inspection und IDS/IPS

— Klassifizierung von Webinhalten, URL-Filterung, IP-Reputation und Geolocation-Filter

— Skalierbare, Cloud-native, mandantenfähige Orchestrierung mit Unterstützung von Hub-and-Spoke-, Hub-Mesh- und Branch-Mesh-Topologien

— Leistungsstarke Zweigstellen-Gateways mit Zero-Touch-Provisioning (ZTP)

— Lizenzen mit unbeschränkter Bandbreite für jedes SD-WAN-Gateway

— Richtlinienbasiertes Routing für über 3700 Anwendungen und Protokolle

— Dynamische Pfadoptimierung für SaaS-Anwendungen mit hoher Priorität

— Optimiert für Microsoft 365

— Optionale virtuelle Gateways und Hub-Routing für Amazon Web Services (AWS), Microsoft Azure und Google Cloud

Decken Sie die gesamte Benutzererfahrung in Remote-Zweigstellen vom Edge bis zur Cloud ab – mit einheitlichem Management, AIOps und Sicherheit für kabelgebundene, Wireless- und WAN-Netzwerke.

Unternehmen wechseln zunehmend zu Cloud-basierten Services und hybriden Arbeitsmodellen. Software-Defined WAN (SD-WAN), eine Schlüsselkomponente des Security Access Service Edge (SASE), bietet ihnen dabei Unterstützung für Cloud-basierte Architekturen und Schutz vor zunehmenden Cybersicherheitsrisiken.

HPE Aruba Networking EdgeConnect SD-Branch ist eine Komplettlösung, mit der Unternehmen nahtlos Netzwerk- und Sicherheitsfunktionen in Zweigstellen bereitstellen und den lokalen Betrieb vereinfachen können. Die Lösung nutzt die enge Integration mit HPE Aruba Networking SSE (Security Service Edge) für die Bereitstellung einer einheitlichen SASE-Plattform, wobei gleichzeitig erweiterte integrierte Sicherheitsfunktionen wie IDS/IPS und Filterung von Webinhalten zum Einsatz kommen. Für eine konsolidierte, sichere Netzwerkinfrastruktur lässt sie sich auch in andere Technologiekomponenten von HPE Aruba Networking wie Wireless-Netzwerke und Switches integrieren, die über eine einzige Konsole in Form von HPE Aruba Networking Central verwaltet werden. Mit seinen fortschrittlichen SD-WAN-Funktionen optimiert EdgeConnect SD-Branch das Routing und verbessert die Transparenz in allen LAN- und WAN-Edge-Bereichen. Auf Endbenutzerrollen, Gerätetyp und Standortkontext basierende Sicherheitsfunktionen, kombiniert mit intelligentem LAN- und WAN-Management, machen EdgeConnect SD-Branch zur idealen Lösung für Zweigstellen in verteilten Unternehmen.

Jedes Unternehmen mit schlanken und zentralisierten Netzwerkteams kann die Zeit für die Bereitstellung, Verwaltung und Wartung von Zweigstellennetzwerken verkürzen und gleichzeitig die Benutzerfreundlichkeit und die Geschäftsabläufe verbessern. EdgeConnect SD-Branch Gateways werden in der Cloud verwaltet und ermöglichen Unternehmen die Bereitstellung einer vollständig softwaredefinierten Lösung für Zweigstellen (SD-Branch)

Intelligentes LAN- und WAN-Management

Durch vereinfachte Workflows kann das Management eines WAN vollständig orchestriert werden, um die Geschwindigkeit der Bereitstellung, die Netzwerkleistung und laufende Konfigurationsänderungen zu verbessern. HPE Aruba Networking Central, eine KI-basierte Plattform für Netzwerkbetrieb, -sicherung und -sicherheit, bietet einen zentralen Kontrollpunkt zur Überwachung aller Aspekte kabelgebundener und drahtloser LANs, SD-WANs und Clouds an Standorten im Campus, in Zweigstellen, an Remote-Standorten und in Rechenzentren. Mit den Vorteilen der Cloud wird die Konfiguration und Bereitstellung sowie die Anzeige von Daten von Zweigstellen-, Hauptstellen- und virtuellen Gateways über HPE Aruba Networking einfacher. Vor Ort müssen keine Managementgeräte aktualisiert oder gewartet werden.

Darüber hinaus beinhaltet HPE Aruba Networking Central eine umfassende AIOps-Lösung für die Automatisierung gängiger Fehlerbehebungsmaßnahmen. AIOps enthält Network Insights zur automatischen Diagnose gängiger Netzwerkprobleme, AI Search für die Suche nach Fehlerbehebungstipps und Lösungsleitfäden in natürlicher Sprache sowie AI Assist für die automatische Erfassung von Protokolldateien und Daten für die Fehlerbehebung. HPE Aruba Networking Central ermöglicht auch die Integration mit anderen IT-Plattformen von Drittanbietern über APIs und Webhooks.

Cloud-basierte Orchestrierung

Basierend auf einer Cloud-nativen, mandantenfähigen Architektur bietet HPE Aruba Networking Central eine End-to-End-Orchestrierung für die mühelose Verteilung von Routen und zur Erstellung von skalierbaren und sicheren Tunneln. WAN-Verbindungen werden automatisch erkannt, und Tunnel werden auf der Grundlage des geschäftlichen Bedarfs und topologischer Anforderungen orchestriert. Der Orchestrator richtet Tunnel nur zwischen Standorten ein, an denen sie benötigt werden. Gleichermaßen werden Routen nur zwischen Gateways angeboten, die einander erreichen können. Der Orchestrator vereinfacht außerdem die Bereitstellung von virtuellen Gateways innerhalb von Amazon AWS, Google Cloud und der Public Cloud-Infrastruktur von Microsoft Azure durch automatische Cloud-Erkennung, automatisches Onboarding und Management..

Unbeschränkte Bandbreite

Im Gegensatz zu anderen Anbietern für SD-WAN bietet HPE Aruba Networking EdgeConnect SD-Branch unbeschränkte Bandbreite für jede Gateway-Lizenz[1].
Das bedeutet, dass Unternehmen Zugang zu unbeschränkten Hardware-Leistungskapazitäten haben – es sind keine Upgrade-Käufe erforderlich

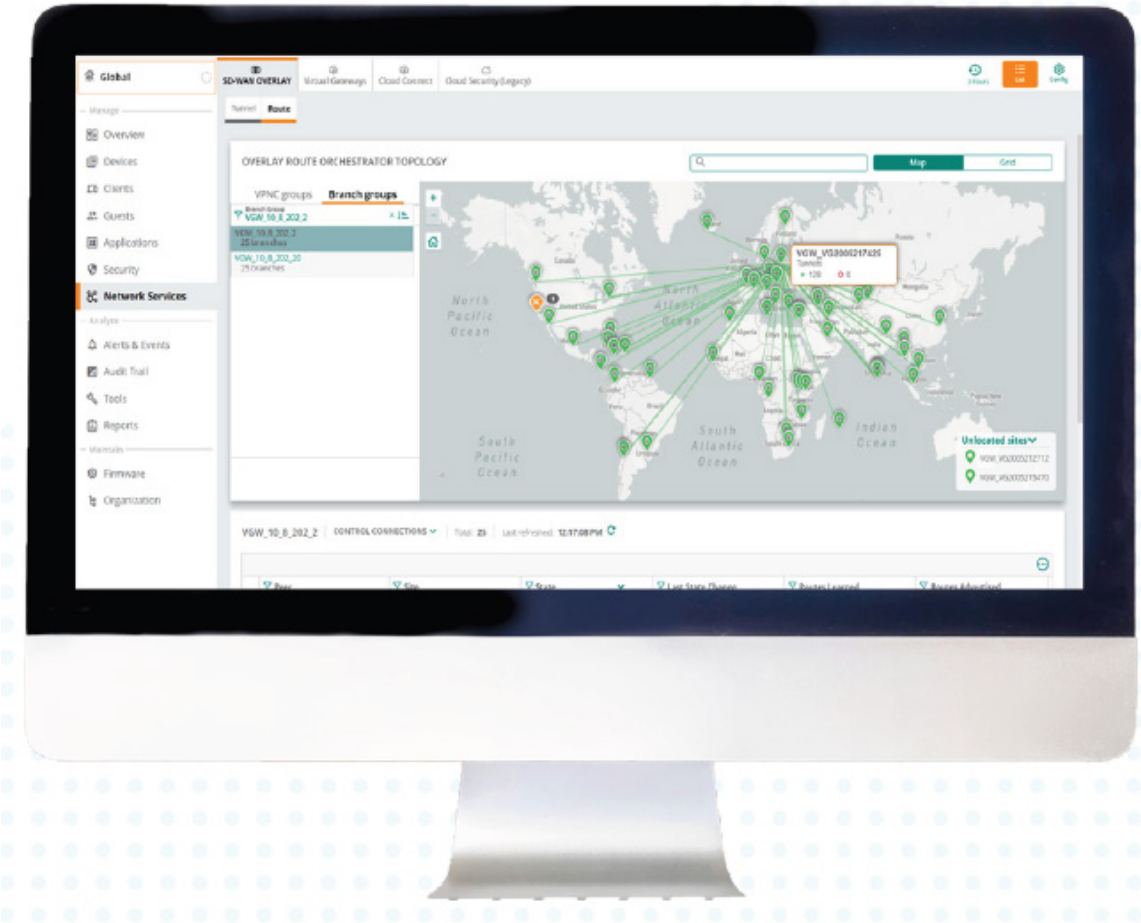


Abbildung 1. HPE Aruba Networking EdgeConnect SD-Branch

[1] Ausgenommen sind virtuelle Gateways in der Cloud

SD-Branch Gateways

Gateways für Zweigstellen

HPE Aruba Networking SD-Branch Gateways sind für die Unterstützung mehrerer WAN-Verbindungen über Breitband-, MPLS- und Mobilfunkverbindungen ausgelegt. Das HPE Aruba Networking 9004-LTE Gateway verfügt über integriertes hardwarebasiertes LTE. Darüber hinaus können Unternehmen, die HPE Aruba Networking 100 Series 5G Cellular Bridge oder ein Plug and Play HPE Aruba Networking USB LTE-Modem nutzen, 5G- oder LTE-Verbindungen auf jedem Branch Gateway im vollen Umfang nutzen. Die 5G Cellular Bridge lässt sich außerdem überall aufstellen und über PoE-Verbindung für bessere Abdeckung und Signalqualität an den Strom anschließen.

Die Verwendung von HPE Aruba Networking Central gewährleistet optimale Konnektivität mit kritischen Anwendungen und Ressourcen, auch wenn die Primärverbindung ausfällt. Es ermöglicht Unternehmen, Datenverkehr zu leiten und zu priorisieren, der an das Rechenzentrum, die Public Cloud-Infrastruktur oder das Internet gesendet wird. Jedes Gateway unterstützt außerdem Anforderungen an hohe Verfügbarkeit (z. B. Aktiv/Aktiv und Aktiv/Standby) und ist damit ideal für Standorte, die volle Redundanz erfordern.

Gateways für das Headend

HPE Aruba Networking Gateways, die am Headend bzw. in Rechenzentren eingesetzt werden, fungieren als VPN-Konzentratoren (VPNCs), um den Datenverkehr von Zweigstellen, Mikrozweigstellen (nur Access Points) und VPN-Endpunkten zu terminieren. Diese Gateways bieten Support für Tausende von Zweigstellen. Zum Beispiel können ein oder mehrere Headend-Gateways verwendet werden, um IPsec-Tunnel zu terminieren, die von Zweigstellen-Gateways in einer Hub-and-Spoke-Topologie aufgebaut wurden.

Gateways für die Public Cloud

Die virtuellen Gateways von HPE Aruba Networking werden in Public Cloud-Infrastrukturen eingesetzt, z. B. einem Microsoft Azure Virtual Network (VNET), einer virtuellen Private Cloud von Amazon Web Services (AWS VPC) oder einer virtuellen Private Cloud von Google Cloud (Google VPC). Diese Gateways dienen als virtuelle Instanz eines Headend-Gateways und ermöglichen eine nahtlose und sichere Konnektivität für alle Zweigstellen und Rechenzentren, die mit Public Clouds verbunden sind. Virtuelle Gateways unterstützen öffentliche Internet- sowie private Verbindungen wie Direct Connect.

Virtuelle Gateways werden von HPE Aruba Networking Central verwaltet und umfassen eine vollständige Orchestrierung, die VNET/VPC-Erkennung, Subnetz-Management, Gateway-Onboarding, Konfigurationen für hohe Verfügbarkeit und Statusüberwachung vollständig automatisiert.

Virtuelle Gateways unterstützen bis zu 4 Gbit/s Durchsatz mit Abonnements mit 1, 3 oder 5 Jahren Laufzeit.

SD-WAN-Integration mit öffentlichem Multi-Cloud-Netzwerk

Das EdgeConnect SD-Branch Gateway bietet orchestrierte, sichere Konnektivität für Zweigstellen direkt zu den globalen Backbone-Netzwerken von Public Cloud-Anbietern. Dadurch wird das SD-WAN-Overlay erheblich vereinfacht, da Zweigstellen direkt mit regionalen Points of Presence (PoPs) mit Zugang zu Cloud-Ressourcen innerhalb einer Region und überregional verbunden werden. Das Overlay unterstützt auch die Kommunikation von Zweigstelle zu Zweigstelle ohne virtuelle Gateways in jedem VPC. Cloud Connect, ein Service innerhalb von HPE Aruba Networking Central, enthält ein einheitliches Dashboard zur Optimierung des Managements und Betriebs von SD-WAN-Integrationen mit AWS Transit Gateway Network Manager und Microsoft Azure Virtual WAN.

Microsoft-Funktionen

Die Integration von HPE Aruba Networking mit Microsoft 365, Teams und Skype for Business liefert einzigartige anwendungsspezifische Einblicke, mit denen Microsoft-Datenverkehr erkannt und gegenüber weniger kritischen Anwendungen priorisiert wird. HPE Aruba Networking Central enthält außerdem spezielle Anrufqualitätsheuristik für zusätzliche Transparenz.

Bevorzugte Lösung von Microsoft

HPE Aruba Networking Virtual Gateways sind eine von Microsoft bevorzugte Lösung auf dem Azure Marketplace. Das bedeutet, dass der Gateway-Anwendung von Microsoft-Experten bescheinigt wurde, dass sie nachweislich über Kompetenzen und Funktionen für die Erfüllung der Anforderungen von Kunden verfügt.

Richtlinienbasiertes Routing und unterstützte Protokolle

Mit richtlinienbasiertem Routing (PBR) kann Datenverkehr basierend auf Anwendungstyp und Link-Status, Geräteprofil, Benutzerrolle und Zielort über mehrere private oder öffentliche WAN-Uplinks geleitet werden. Zu den unterstützen Protokollen gehören BGP, OSPF und statische Routen.

SaaS-Optimierung

SaaS Express stellt sicher, dass SaaS-Anwendungen mit hoher Priorität, wie Microsoft 365, Dropbox und Slack, bei der Übertragung über die Verbindungen mehrerer Internetanbieter auf höchstem Leistungsniveau gehalten werden. Die Lösung klassifiziert Anwendungen bereits ab dem ersten Paket mit der DPI-Engine.

SaaS Express stellt nahtlose und sichere Verbindungen zwischen Benutzern in Zweigstellen und SaaS-Anwendungen her und überwacht ständig die Benutzerfreundlichkeit (Quality of Experience, QoE) von SaaS. Die Schnittstelle beinhaltet ein Drill-Down-Dashboard, mit dem der Benutzer bei SaaS-Leistungsproblemen Ursachenanalysen durchführen kann.

Für diese Funktion ist die HPE Aruba Networking Central SD-WAN Advanced-Lizenz erforderlich. Weitere Informationen entnehmen Sie bitte dem aktuellen Bestellleitfaden für HPE Aruba Networking Central.

Wichtigste WAN-Funktionen

Overlay- und Hybrid-WAN-Management

HPE Aruba Networking EdgeConnect SD-Branch mit Management über HPE Aruba Networking Central führt eine neue Architektur ein, die ein Netzwerk-Overlay für WAN-Verbindungen bietet, um die Transparenz und Kontrolle über private und öffentliche Verbindungen (Hybrid-WAN) zu verbessern.

Orchestrierte SD-WAN-Topologien

HPE Aruba Networking Central ermöglicht die Orchestrierung von Routen und Tunneln für den Aufbau verschiedener Topologien (Hub-and-Spoke, Hub-Mesh, Branch-Mesh), wobei die Konnektivität zwischen allen Standorten vereinfacht und gleichzeitig für Ausfallsicherheit und maximale Flexibilität gesorgt wird. Mit Hub-and-Spoke-Topologien erhalten Zweigstellen den schnellsten Zugang zu den richtigen Ressourcen, Hub-Mesh ermöglicht den Aufbau eines vollständig transitiven Backbone-Netzwerks und Branch-Mesh ermöglicht die nahtlose direkte Kommunikation zwischen Netzwerkspeichen (oder Zweigstellen).

Site-to-Site-VPNs

Sichere Verbindungen können auch von einer Zweigstelle zur anderen anderen über eine öffentliche Internetverbindung erfolgen. Damit können Benutzer von verschiedenen Standorten auf Netzwerkressourcen zugreifen, die innerhalb des Firmennetzwerks gehostet werden, ohne über das Rechenzentrum gehen zu müssen

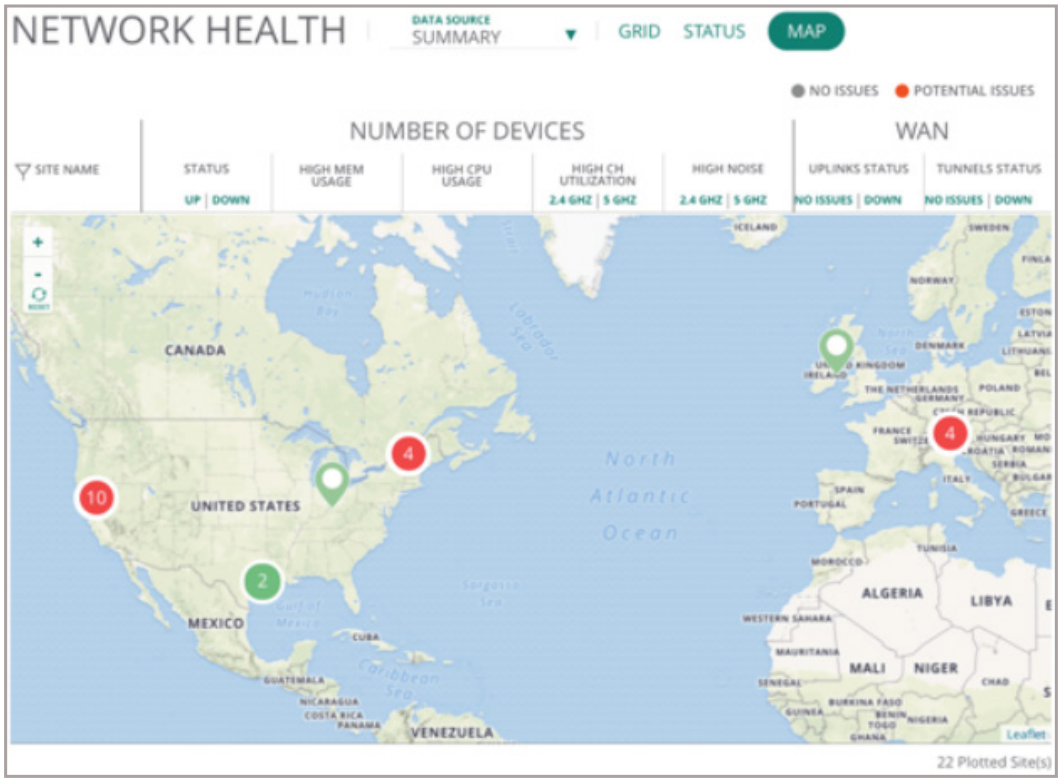


Abbildung 2. HPE Aruba Networking Central Dashboard für den WAN-Zustand

Dynamic Path Steering (DPS)

WAN-Datenverkehr kann anhand von Merkmalen wie WAN-Durchsatz, Latenz, Jitter und Paketverlust automatisch über den besten verfügbaren Uplink geleitet werden. Die Lösung unterstützt auch Vorwärts-Fehlerkorrektur (Forward Error Correction, FEC), mit der Paketverluste während des Datenflusses kompensiert werden, um die Anwendungsleistung zu verbessern.

WAN-Transparenz

HPE Aruba Networking Central bietet mit Deep Packet Inspection-Technologie Überwachung für Anwendungsverkehr, der in einem Zweignetzwerk ein- und ausgeht. Dabei spielt der Uplink-Typ keine Rolle. Dies erleichtert IT-Abteilungen das Management von WAN-Umgebungen, die zunehmend öffentliche WAN-Verbindungen nutzen.

WAN-Komprimierung

IDiese WAN-Komprimierungsfunktion eignet sich ideal für Zeiträume mit Netzwerk-Datenstau und ermöglicht es der IT, zu jedem Zeitpunkt oder in jedem Zeitrahmen mehr Datenverkehr durch dieselbe WAN-Verbindung zu senden.

Unbeschränkte Bandbreite

HPE Aruba Networking Central Lizenzen bieten Zugang zur vollen Bandbreitenspezifikation für jedes Gateway. Es sind keine weiteren Lizenz-Upgrades erforderlich.

Wichtigste Konfigurationsmerkmale

Vereinfachter Installationsassistent

Für die mühelose Konfiguration von Zweigstellen-Gateways bietet HPE Aruba Networking Central den Benutzern eine Schritt-für-Schritt-Navigation, die die Bereitstellung des Netzwerks erleichtert.

Konfigurationshierarchie

In HPE Aruba Networking Central können Netzwerkeinstellungen auf Basis der zweigstellenspezifischen Anforderungen vorkonfiguriert und angepasst werden. Zero-Touch-Provisioning (ZTP) liefert ein einfaches und fehlerfreies Bereitstellungsmodell.

Zero-Touch-Provisioning (ZTP)

Mit Zero-Touch-Provisioning können die Hardware-Gateways werkseitig konfiguriert ausgeliefert und mit HPE Aruba Networking Central bereitgestellt werden. Einstellungen können anhand von Konfigurations- und anderen netzwerkspezifischen Anforderungen vorgenommen werden.

Einfache Bereitstellung über Mobilgeräte

Die Installations-App von HPE Aruba Networking für Mobilgeräte ermöglicht den Mitarbeitern von Ort die mühelose Integration der Gateways. Ein zentrales IT-Team kann Gerätestandort, Lizenzen und Status überprüfen, ohne dass hierzu weitere Schritte erforderlich sind. Die App ist für iOS und Android verfügbar



Wichtigste Sicherheitsmerkmale

Dynamische Segmentierung

Um den kabelgebundenen und Wireless-Netzwerkzugriff zu vereinfachen und besser zu schützen, kann das Zweigstellen-Gateway automatisch Rollen pro Benutzer und pro Gerät in kabelgebundenen und Wireless-Netzwerken durchsetzen. Die Integration mit dem ClearPass Policy Manager ermöglicht ein zentrales Rollen- und Richtlinienmanagement. Dies gewährleistet eine konsistente Richtlinie ungeachtet der Benutzerrolle und des Gerätetyps und eliminiert den Bedarf, unnötige SSIDs, ACLs, VLANs und Subnetze an jedem Node des Netzwerks zu konfigurieren.

HPE Aruba Networking Client Insights nutzt KI-basierte Einblicke, um alle über Kabel oder WLAN verbundenen Benutzer- und IoT-Endpunkte für die Umsetzung von Richtlinien zu identifizieren und klassifizieren.

Große Unternehmen arbeiten häufig mit komplexen, weltweit verteilten Netzwerken. HPE Aruba Networking Central NetConductor erstellt und orchestriert automatisch intelligente Overlays mit EVPN-, VXLAN- und BGP-Protokollen und ermöglicht so eine rollenbasierte Mikrosegmentierung und Richtliniendurchsetzung in komplexen, verteilten Netzwerken. Weitere Informationen zur dynamischen Netzwerksegmentierung mit HPE Aruba finden Sie in der Lösungsübersicht.

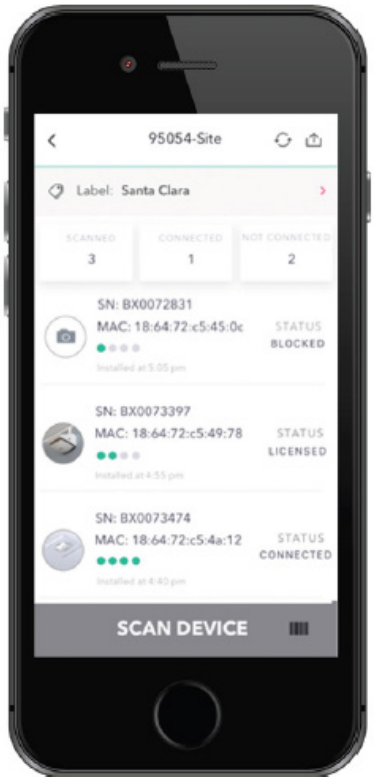


Abbildung 3. Beispiel für das Onboarding von Geräten mit der Installations-App von HPE Aruba Networking für Mobilgeräte

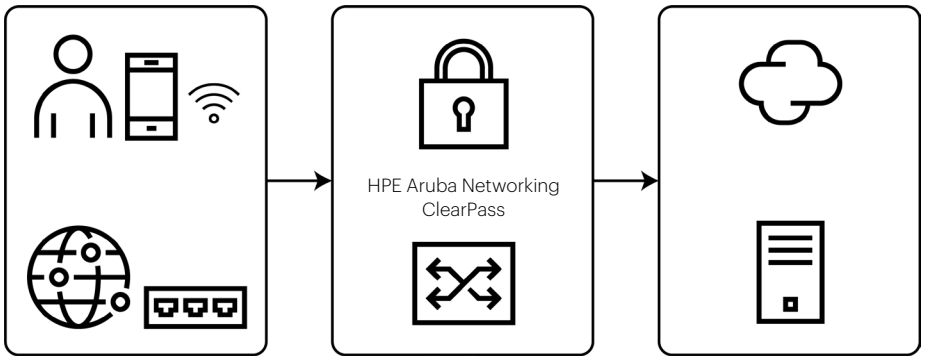


Abbildung 4. Dynamische Segmentierung zum Isolieren des Datenverkehrs von Mobilgeräten von IoT-Verkehr

Policy Enforcement Firewall (PEF)

Die PEF ist in der Foundational-Lizenz enthalten und ermöglicht das Senden von kabelgebundenem und Wireless-Datenverkehr von Benutzern und Anwendungen über GRE-Tunnel zur Überprüfung an ein Zweigstellen-Gateway.

Die Durchsetzung von Richtlinien basiert auf Benutzerrolle, Gerätetyp, Anwendung und Standort und erfolgt durch dynamische Segmentierung.

Anwendungstransparenz und -steuerung

Ebenfalls in der Foundational-Lizenz enthalten ist eine Funktion für Anwendungstransparenz, die Deep Packet Inspection-Technologie (DPI) verwendet, um Leistung und QoS-Richtlinien für über 3700 Anwendungen und Protokolle zu überprüfen und zu optimieren, einschließlich verschlüsseltem und verborgenem Datenverkehr.

Filterung von Webinhalten

Das Web Content Classification-Paket (WebCC) ist in der Basislizenz enthalten und umfasst URL-Filterung, IP-Reputation und Geolocation-Filter. Die URL-Filterung klassifiziert mithilfe von maschinellem Lernen für mehr Geschwindigkeit und Genauigkeit mehr als 80 Website-Kategorien. Der IP-Reputationsservice leitet einen IP-Reputationsindex aus Kontext- und Verhaltenstrends ab und nimmt eine Klassifizierung in fünf Reputationsstufen vor: „Vertrauenswürdig", „Geringes Risiko", „Mäßiges Risiko", „Verdächtig" und „Hohes Risiko". Der Geolocation-Filter verknüpft Quell-/Ziel-IP-Adressen mit dem Standort, um die Kommunikation mit bestimmten Ländern zuzulassen oder mit als bösartig bekannten Ländern zu unterbinden.

Firewall-Protokollierung

Das Firewall-Protokollierungs-Dashboard von HPE Aruba Networking Central stellt die Effektivität der vom Gateway durchgesetzten Firewall-Regeln im gesamten Unternehmensnetzwerk in Grafiken und in tabellarischer Form dar. Zunächst liefert es eine globalen Ansicht der Gateways mit den meisten blockierten Sitzungen. Von dort aus können Sie detaillierte Informationen zu blockierten Sitzungen nach Quell- und Ziel-IP-Adresse und der durchgesetzten Regel abrufen. Die Firewall-Protokollierung ist ebenfalls in der Foundational-Lizenz enthalten.

Bedrohungsschutz mit IDS/IPS

Um die Sicherheit angesichts einer wachsenden Angriffsfläche zu verbessern, bieten die im SD-WAN-Modus bereitgestellten Gateways neben den vorhandenen Sicherheitsfunktionen rollen- und identitätsbasierte Angriffserkennungs- und -präventionsfunktionen (IDS/IPS).

Ein erweitertes Sicherheits-Dashboard stellt IT-Teams eine netzwerkweite Übersicht, multidimensionale Bedrohungsmetriken, Threat-Intelligence-Daten sowie Korrelations- und Störungsmanagement zur Verfügung. Für diese Funktion ist das entsprechende HPE Aruba Networking Central Sicherheitslizenz-Abonnement erforderlich. Bedrohungsereignisse können für erweiterte Transparenz und Überwachung auch an SIEM-Systeme (Security Information and Events Management) wie Splunk gestreamt werden.

Einheitlicher SASE

Um hybrides Arbeiten zu ermöglichen und die mit Cloud Computing verbundenen Sicherheitsprobleme zu bewältigen, wird HPE Aruba Networking EdgeConnect SD-Branch mit HPE Aruba Networking SSE integriert, um eine einheitliche SASE-Plattform zu bilden, die die steigende Nachfrage nach integriertem Netzwerk- und Sicherheitsfunktionen erfüllt. Die einheitliche SASE-Lösung lässt sich als zentrale, eng integrierte Lösung mühelos bereitstellen und bietet vereinfachtes Management.

HPE Aruba Networking SSE bietet mit seinem agentenbasierten und agentenlosen ZTNA (Zero Trust Network Access) Benutzern und autorisierten Drittanwendern eine Zugriffsmodell mit minimalen Berechtigungen. Es schützt Internetbenutzer mit einem Secure Web Gateway (SWG) vor Cyber-Bedrohungen und sorgt mit dem Cloud Access Security Broker (CASB) dafür, dass vertrauliche Daten in SaaS-Anwendungen geschützt bleiben und nicht verloren gehen können. Die Lösung verbessert das digitale Erlebnis und die Produktivität mit Digital Experience Monitoring (DEM).

ZTNA, SWG, CASB und DEM haben eine gemeinsame Codebasis, auf der alle Richtlinien über eine einzige Benutzeroberfläche verwaltet werden, was die Zugriffskontrolle für IT-Administratoren äußerst einfach macht. Zudem vereinheitlicht die Lösung den Zugriff weltweit mittels eines Cloud-Backbones aus Amazon Web Services (AWS), Microsoft Azure, Google Cloud und Oracle Cloud.

EdgeConnect SD-Branch lässt sich auch nahtlos mit Lösungen von externen Sicherheitsanbietern integrieren. Die Orchestrierung ist vollständig automatisiert und verwendet den Cloud Connect Service von HPE Aruba Networking. HPE Aruba Networking Gateways können die Rolle eines On-Premises-Agenten für zentral gehostete Firewalls übernehmen, wie beispielsweise von Palo Alto Networks und Check Point Software angeboten, oder Web-Sicherheits-Gateways wie Zscaler und Symantec.

Technische Daten*

HPE Aruba Networking Branch Gateways (kleine und mittlere)						
Merkmale	**9004**	**9012[2]**	**7005**	**7008**	**7010**	**7024**
Bereitstellungs-modus	Klein/mittel	Klein/mittel	Klein	Klein	Mittel	Mittel
Maximale Clients	Bis zu 2.048[3]	Bis zu 2.048[3]	Bis zu 1.024[3]	Bis zu 1.024[3]	2.048	2.048
Maximale VLANs	128	128	127	127	127	127
Firewall-Durchsatz	4 Gbit/s	6 Gbit/s	2 Gbit/s	2 Gbit/s	8 Gbit/s	8 Gbit/s
Verschlüsselter Durchsatz (AES-CBC)	4 Gbit/s	4 Gbit/s	1,2 Gbit/s	1,2 Gbit/s	2,6 Gbit/s	2,6 Gbit/s
Aktive Firewall-Sitzungen	64.000/128.000[4]	64.000/128.000[4]	64.000	64.000	32.000	32.000
IDS/IPS-Durchsatz	Bis zu 1,1 Gbit/s[5]	Bis zu 1,1 Gbit/s[5]	–	–	–	–
WAN/LAN-Schnittstellen	4	12	4	8	16	24
PoE-Eingang/-Ausgang	–	Ausgang; 120 W	Eingang; E0	Ausgang; 100 W	Ausgang; 150 W	Ausgang; 400 W
USB (WAN)	Ja (1); USB 3.0	Ja (1); USB 3.0	Ja (1); USB 2.0	Ja (2); USB 2.0	Ja (2); USB 2.0	Ja (1); USB 2.0
Formfaktor/ Platzbedarf	Desktop/1RU[6]	Desktop/1RU	Desktop/1RU	Desktop/1RU	1RU	1RU

[2] 9012 kann als Zweigstellen-Gateway oder Headend-Gateway mit IDS/IPS bereitgestellt werden (mit entsprechender Lizenz)

[3] 9004 und 7005/7008 bieten eine Basislizenz für bis zu 75 Clients

[4] 64.000 Sitzungen mit IDS/IPS und 128.000 ohne IDS/IPS

[5] IDS/IPS-Durchsatzergebnisse basierend auf iMix-Traffic mit verlustfreiem Input für AOS SD-WAN Image 2.3 oder AOS 10.2

[6] Eine Rack-Einheit (RU) kann mit einem optionalen Montagesatz zwei 9004-Gateways nebeneinander aufnehmen

HPE Aruba Networking Branch Gateways (groß)							
Merkmale	**7030**	**7210**	**7220**	**7240XM**	**9106**	**9114**	**9240**
Bereitstellungs-modus	Groß	Groß	Groß	Groß	Groß	Groß	Groß
Maximale Clients	4096	16.000	24.000	32.000	8.000	10.000	32.000
Maximale VLANs	255	4096	4096	4096	4096	4096	4096
Firewall-Durchsatz	8 Gbit/s	20 Gbit/s	40 Gbit/s	40 Gbit/s	15 Gbit/s	20 Gbit/s	20 Gbit/s
Verschlüsselter Durchsatz (AES-CBC)	2,6 Gbit/s	6 Gbit/s	20 Gbit/s	30 Gbit/s	10 Gbps	20 Gbit/s	20 Gbit/s
IDS/IPS	n. z.	n. z.	n. z.	n. z.	2,5 Gbit/s	4 Gbit/s	6 Gbit/s
Aktive Firewall-Sitzungen	64.000	2 Mio.	2 Mio.	2 Mio.	2 Mio.	2 Mio.	4 Mio.
WAN/LAN-Schnittstellen	8 (kombiniert)	2 (kombiniert)	2 (kombiniert)	2 (kombiniert)	2 (combo); 2 x 10G SFP+; 2 x 1G (PoE 60W)	4 (kombiniert); 4x 10G SFP+	4 x 25G SFP28
USB (WAN)	Ja (1); USB 2.0	Ja (1); USB 2.0	Ja (1); USB 2.0	Ja (1); USB 2.0	Ja (1); USB 3.0	Ja (2); USB 3.0	Ja (2); USB 3.0
Formfaktor/ Platzbedarf	1 RU	1 RU	1 RU	1 RU	1 RU	1 RU	1 RU
* Die vollständigen Hardware-Spezifikationen entnehmen Sie bitte den entsprechenden Datenblättern.							

HPE Aruba Networking Headend-Gateways										
Merkmale	**7010/7024**	**7030**	**7210**	**7220**	**7240XM**	**7280**	**9012**	**9106**	**9114**	**9240**
Bereitstellungs-modus	VPN-Konzentrator (VPNC)	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC
Verschlüsselter Durchsatz (AES-CBC)	2,6 Gbit/s	2,6 Gbit/s	7 Gbit/s	22 Gbit/s	30 Gbit/s	45 Gbit/s	3,5 Gbit/s	10 Gbit/s	20 Gbit/s	20 Gbit/s
Maximale Anzahl von Tunneln	256	512	1.024	4.096	6.144	8.192	512	8.000	16.000	32.000
Routenska-lierung	4.000	4.000	8.000	16.000	32.000	32.000	12.000	12.000	12.000	32.000
Formfaktor/ Platzbedarf	1RU	1RU	1RU	1RU	1RU	1RU	1RU	1 RU	1RU	1RU

HPE Aruba Networking Virtual Gateways (Public Cloud-Infrastruktur)				
Merkmale	**Amazon Web Services (AWS)**	**Microsoft Azure**	**Google Cloud**	**VMware ESXi™**
Bereitstellungs-modus	EC2-Instanz in VPC	Linux-VM-Instanz in VNET	VM-Instanz in VPC	VM-Instanz mit vSphere
Virtuelle Gateway-Modelle	500 Mbit/s, 2 Gbit/s, 4 Gbit/s	500 Mbit/s, 2 Gbit/s, 4 Gbit/s	500 Mbit/s, 2 Gbit/s, 4 Gbit/s	500 Mbit/s, 2 Gbit/s, 4 Gbit/s
Firewall-Durchsatz	500 Mbit/s, 2 Gbit/s, 4 Gbit/s	500 Mbit/s, 2 Gbit/s, 4 Gbit/s	500 Mbit/s, 2 Gbit/s, 4 Gbit/s	500 Mbit/s, 2 Gbit/s, 4 Gbit/s
Virtuelle CPUs	4, 8 und 16 vCPU	4, 8 und 16 vCPU	4, 8 und 16 vCPU	4, 8 und 16 vCPU
Arbeitsspeicher	7,5 GB, 15 GB und 30 GB	14 GB, 16 GB und 32 GB	16 GB, 32 GB und 64 GB	7 GB, 15 GB und 30 GB
Datenspeicher	15 GB, 30 GB und 60 GB	15 GB, 30 GB und 60 GB	15 GB, 30 GB und 60 GB	15 GB, 30 GB und 60 GB
Anzahl der Schnittstellen	4 (einschließlich Man-agementschnittstelle)	4 (einschließlich Man-agementschnittstelle)	4 (einschließlich Man-agementschnittstelle)	4 (einschließlich Man-agementschnittstelle)
Maximale Anzahl von Tunneln (pro Modell)	512, 4096 und 8192	512, 4096 und 8192	512, 4096 und 8192	512, 4096 und 8192
Infrastrukturkosten	BYOL + Kosten für gehostete Services, einschließlich Computing, Datenspeicher und ausgehender Daten	BYOL + Kosten für gehostete Services, einschließlich Computing, Datenspeicher und ausgehender Daten	BYOL + Kosten für gehostete Services, einschließlich Computing, Datenspeicher und ausgehender Daten	–

Weitere Informationen zur Bestellung und zu den vollständigen Hardware-Spezifikationen des Gateways finden Sie unter:

- HPE Aruba Networking Central Bestellleitfaden
- Datenblatt HPE Aruba Networking Mobility Controller der Serie 7000
- Datenblatt HPE Aruba Networking Mobility Controller der Serie 7200
- Datenblatt für HPE Aruba Networking Gateways der Serie 9000
- HPE Aruba Networking Virtual Gateway Bereitstellungshandbuch

HPE.com besuchen

Jetzt chatten

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Die einzigen Garantien für Produkte und Services von Hewlett Packard Enterprise sind in den ausdrücklichen Garantieerklärungen enthalten, die diesen Produkten und Services beiliegen. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

Google Cloud und Android sind eingetragene Marken von Google LLC. Linux

ist in den USA und anderen Ländern die eingetragene Marke von Linus Torvalds. VMware ESXi und VMware vSphere sind eingetragene Marken oder Marken von VMware, Inc. und seiner Tochterunternehmen in den USA und anderen Ländern. Azure, Microsoft und Skype sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und anderen Ländern. Oracle ist eine eingetragene Marke von Oracle und deren Tochterunternehmen. Alle Drittanbietermarken sind Eigentum ihrer jeweiligen Inhaber.

a00047570DEE, Rev. 3

HEWLETT PACKARD ENTERPRISE

hpe.com