



HPE Aruba Networking Dynamic Segmentation

Identitätsbasierte Zugriffskontrolle für Zero-Trust-Sicherheit und SASE vom Edge bis zur Cloud im globalen Maßstab



Die Zunahme von IoT-Geräten (Internet der Dinge) und die Einführung von hybriden Arbeitsinitiativen haben zu komplexen, geografisch verteilten Netzwerken geführt, die einzigartige Herausforderungen hinsichtlich Sichtbarkeit und Sicherheit darstellen. Angesichts der Tatsache, dass Unternehmen die digitale Transformation beschleunigen, um die geschäftliche Effizienz zu steigern, sehen sich IT-Teams mit einer wachsenden Herausforderung konfrontiert, was die Einführung von Zero-Trust-Sicherheits- und SASE-Frameworks (Secure Access Service Edge) vom Edge zur Cloud betrifft.

HPE Aruba Networking Dynamic Segmentation ist ein wichtiges Element der Edge-to-Cloud-Sicherheit, die in das sicherheitsorientierte, KI-basierte Netzwerk von HPE Aruba Networking integriert ist. Dieses Element basiert darauf, den Zugriff auf IT-Ressourcen nach dem Prinzip der geringsten Rechte einzurichten, indem der Datenverkehr auf Grundlage von Rollen und zugehörigen Zugriffsberechtigungen segmentiert wird. Bei diesem grundlegenden Konzept eines Zero-Trust- und SASE-Frameworks basiert Vertrauen auf Rollen und Richtlinien – und nicht darauf, wo und wie sich die Geräte von Benutzern verbinden.

HPE Aruba Networking Dynamic Segmentation vereinheitlicht den rollenbasierten Zugriff und die Durchsetzung von Richtlinien in kabelgebundenen, kabellosen und WAN-Netzwerken und stellt sicher, dass Benutzer und Geräte nur mit Zielen kommunizieren können, die ihrer Rolle entsprechen – so bleibt der Datenverkehr sicher und getrennt.

Hauptvorteile

- **Einfacherer Netzwerkbetrieb** – Sparen Sie Zeit und verhindern Sie die VLAN-Ausbreitung durch die Reduzierung der für SSIDs, ACLs, Subnetzwerke und kabelgebundene Ports erforderlichen Konfiguration
- **Erhöhte Sicherheit und Sichtbarkeit** – Stellen Sie durch zentralisierte Richtliniendefinition und rollenbasierten Zugriff sicher, dass Benutzer und Geräte nur mit Zielen im Einklang mit ihrer Aufgabe kommunizieren
- **Cloud-basierte Verwaltung und Automatisierung** – Nutzen Sie absichtsorientierte, benutzerfreundliche Workflows für die Definition von Richtlinien und die Netzwerkkonfiguration
- **Globale Reichweite und Interoperabilität** – Ermöglichen Sie eine globale Skalierung, indem Sie die Interoperabilität mit der Infrastruktur von Drittanbietern gewährleisten
- **Leistung und Effizienz** – Beseitigen Sie den IT-Overhead mit automatisch aktualisierten und fortlaufend durchgesetzten Richtlinien

Identitätsbasierte Segmentierung ist der Schlüssel zu Zero Trust und SASE

Längst hat man erkannt, dass Zugriffskontrollentscheidungen, die auf der Art und Weise basieren, wie und wo sich ein Benutzer oder Gerät verbindet, zu hochgradig manuellen und fehleranfälligen Netzwerkkonfigurationen mit erheblichen Sicherheitslücken führen. Um diese Herausforderung zu bewältigen, wurde vor einem Jahrzehnt Zero Trust eingeführt. Es handelt sich dabei um eine Sicherheitsarchitektur, mit der Unternehmen IT-Zugriffsrichtlinien definieren und durchsetzen können, die den Zugriff auf Ressourcen basierend auf der Identität oder Rolle eines Benutzers oder Kunden begrenzen. So sollte beispielsweise einem Drucker niemals der Zugriff auf einen Server mit Gehaltsabrechnungsdaten gestattet werden.

Ein Zero-Trust-Netzwerk segmentiert den Datenverkehr anhand von Zugriffskontrollrichtlinien – und zwar unabhängig von der Art der Verbindung. Die SASE-Architektur hat vor einigen Jahren die Bedeutung von Cloud-basierten Workloads erkannt und Zero Trust auf SD-WAN und Sicherheitsdienste aus der Cloud ausgeweitet. Die Zero-Trust- und SASE-Frameworks bilden die Grundlage für ein sicheres Netzwerk, das sich die identitätsbasierte Netzwerksegmentierung zunutze macht, um das Unternehmen zu schützen.

Die Prinzipien von HPE Aruba Networking Dynamic Segmentation

Hewlett Packard Enterprise ist Marktführer bei der Bereitstellung von Netzwerken, die die von Zero Trust und SASE definierten Zugriffskontrollmechanismen unterstützen. HPE Aruba Networking Dynamic Segmentation kombiniert Identität, Richtlinien und die Netzwerkinfrastruktur, um zu optimieren und zu automatisieren, wie die IT kritische Ressourcen schützt:

Geräte-Entdeckung und Profilerstellung

Da sich immer mehr IoT-Geräte mit dem Netzwerk verbinden, kann die IT nur in begrenztem Umfang alle angeschlossenen Geräte sehen und deren Profile erfassen. Daraus ergeben sich betriebliche und auch sicherheitstechnische Schwachstellen, die zu einer Gefährdung des gesamten Unternehmens führen können. Ein Schlüsselement der HPE Aruba Networking Dynamic Segmentation ist das KI-basierte HPE Aruba Networking Client Insights, Teil von HPE Aruba Networking Central. Diese Lösung nutzt Telemetriedaten aus der HPE Aruba Networking Netzwerkinfrastruktur sowie maschinelles Lernen, um automatisch die Profile zahlreicher verschiedener Clients zu erstellen, die sich mit dem Netzwerk verbinden – einschließlich IoT-Geräte.

HPE bietet auch eine Option für die automatische, KI-basierte Client-Profilerstellung, die bei der Bereitstellung von Drittanbieter-Netzwerken funktioniert. Erfahren Sie mehr über Transparenz und Einblicke in die heutigen IoT-gesteuerten Netzwerke.

Identität und Authentifizierung

Nach der Identifizierung eines Benutzers oder Geräts durch einen Authentifizierungsprozess mit 802.1X oder anderen Verfahren kann die IT-Abteilung

entsprechende Rollen und Zugriffsberechtigungen festlegen, die automatisch angewendet werden. Auf diese Weise werden Zugriffsrechte an die Identität gebunden, unabhängig von der Netzwerkverbindung oder dem Standort des Benutzers oder Geräts.

Rollenbasierte Richtlinien

Eine Rolle ist eine logische Gruppierung von Berechtigungen, die nach Feststellung der Identität eines Benutzers oder Clients zugewiesen werden. Zu den Berechtigungen kann eine Liste der Anwendungen gehören, auf die zugegriffen werden kann, die Dienste und andere Clients, die erreicht werden können, oder sogar die Wochentage, an denen ein bestimmter Benutzer eine Verbindung zum Netzwerk herstellen kann. Rollen und Durchsetzung werden durch den allgemeinen Ansatz eines Unternehmens zu Zero Trust und SASE sowie durch geltende Compliance-Anforderungen wie die DSGVO bestimmt.

Automatisierte Durchsetzung

Sobald die Rollen definiert sind, erfolgt die Durchsetzung durch die Netzwerkinfrastruktur, indem die Zugriffsrechte zur entsprechenden Weiterleitung und Segmentierung des Datenverkehrs verwendet werden. HPE Aruba Networking Dynamic Segmentation bietet eine Auswahl an Durchsetzungsmodellen, die einzeln oder zusammen eingesetzt werden können.

Modelle der HPE Aruba Networking Dynamic Segmentation

HPE Aruba Networking unterstützt zwei Möglichkeiten zur Durchführung der dynamischen Segmentierung basierend auf der gesamten Netzwerkarchitektur eines Unternehmens.

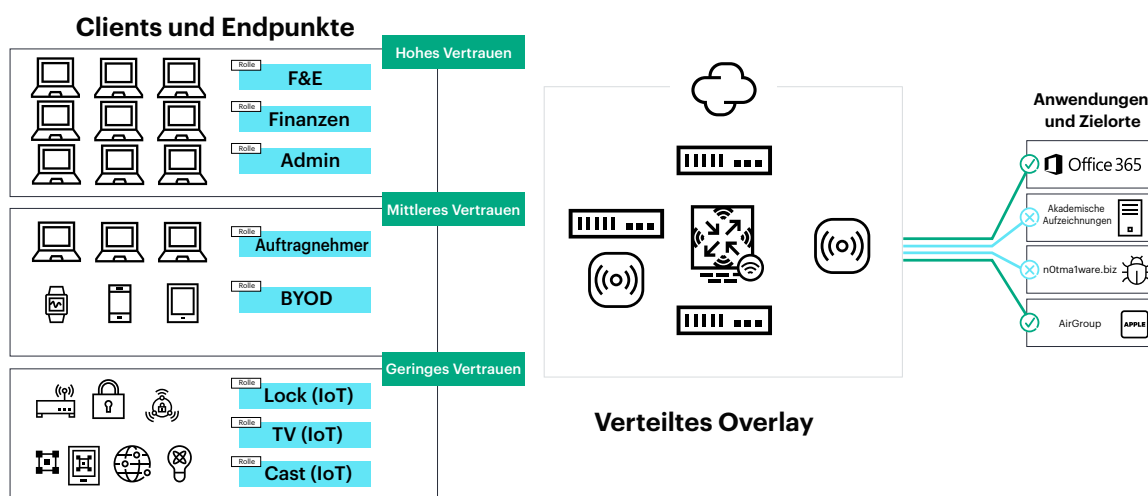


Abbildung 1. HPE Aruba Networking Dynamic Segmentation mit einer verteilten Overlay-Fabric

Verteilte dynamische Segmentierung

Mit der Modernisierung von Netzwerken in Unternehmen durch die Einführung von Overlays und weit verbreiteten Protokollen wie EVPN/VXLAN besteht die Möglichkeit, das Overlay für einen besseren Schutz und eine größere Skalierung mit HPE Aruba Networking Dynamic Segmentation zu nutzen. Mit der Einführung von HPE Aruba Networking Central NetConductor kann die dynamische Segmentierung über die Cloud verwaltet werden, wobei die Zugriffsrichtlinien zentral definiert und verbreitet und über HPE Aruba Networking Switches und Gateways inline durchgesetzt werden können (Abbildung 1).

Auf Geschäftsabsichten basierende Workflows

Die IT-Abteilung kann mit HPE Aruba Networking Central NetConductor einen Fabric-Assistenten verwenden, um die Komplexität des zugrunde liegenden Netzwerks zu entschlüsseln, die Definition von Richtlinien zu vereinfachen und gleichzeitig die Netzwerkdefinition und -konfiguration zu automatisieren. Durch intuitive, grafische Workflows und die Automatisierung per Knopfdruck werden CLI-basierte Programmierung, Routing-Tabellen oder die manuelle Konfiguration von ACLs überflüssig.

Gruppenrichtlinien-Identifikatoren für die Inline-Durchsetzung von Richtlinien

Der Richtlinienmanager von HPE Aruba Networking Central NetConductor definiert Rollen und zugehörige Zugriffsrichtlinien. Diese Richtlinien werden in Gruppenrichtlinien-Identifikatoren (GPIDs) ausgedrückt und das Netzwerk kann Zugriffskontrollinformationen, die die Rolle und Zugriffsberechtigung des Benutzers oder Clients widerspiegeln, über den Datenverkehr selbst übertragen. Die Identifikatoren sind in den Paket-Header integriert und werden von den HPE Aruba Networking CX Switches und Gateways inline interpretiert (Abbildung 2). Wenn sich der Sicherheitsstatus eines Clients ändert, wird die Rolle automatisch geändert, um den Zugriff einzuschränken, und die Rollenänderung wird anschließend im Netzwerk verbreitet.

Die verteilte dynamische Segmentierung verbessert mit GPIDs die Skalierbarkeit der Durchsetzung von Richtlinien erheblich und reduziert gleichzeitig die Latenzzeit und den Datenverkehr-Overhead. Die Identifikatoren basieren auf Industriestandards und unterstützen die bidirektionale Integration mit Drittanbieter-Netzwerken.

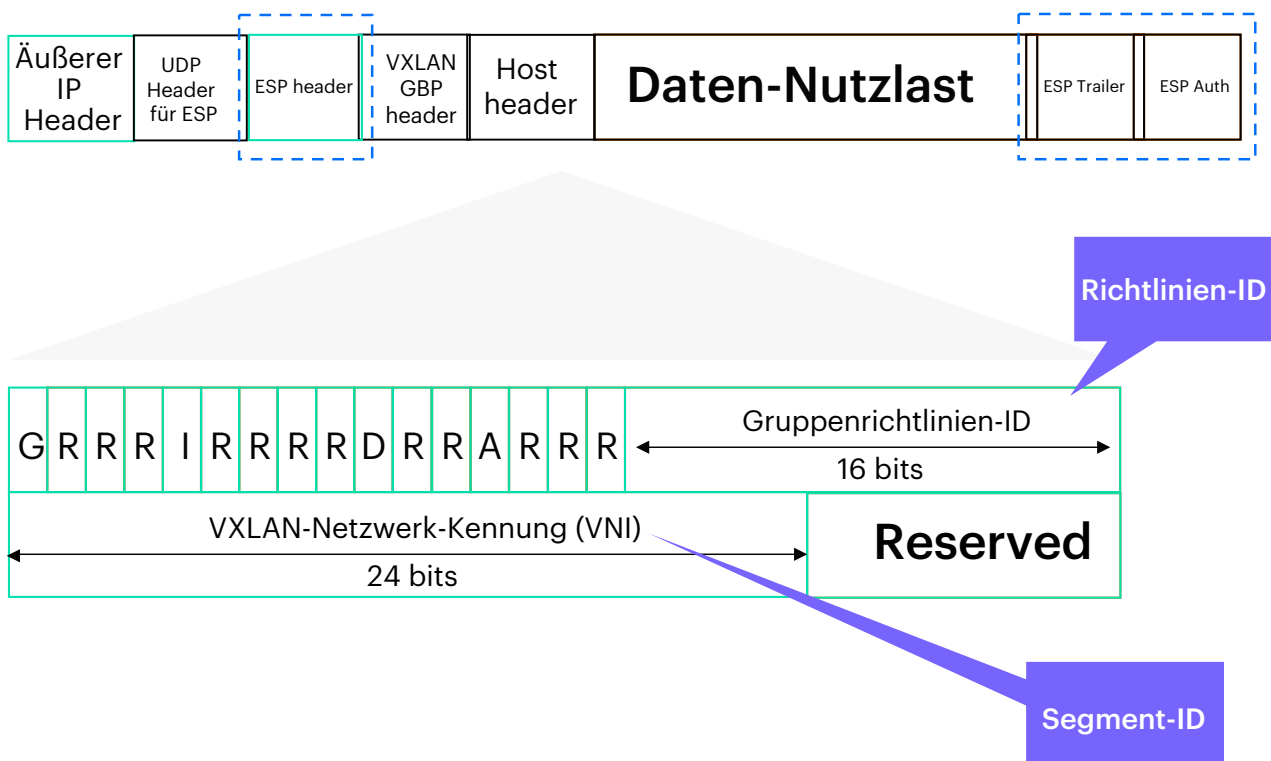


Abbildung 2. GPIDs übertragen Zugriffskontrollinformationen zur Durchsetzung von Inline-Richtlinien über den Netzwerkverkehr

HPE Aruba Networking Client Insights

KI-basierte Sichtbarkeit und Profilerstellung

GPID

Inline-Zugriffsdurchsetzung durch Fabric-fähige HPE Aruba Networking Switches und Gateways



Policy Manager

Richtlinienentwicklung

Cloud Auth (oder) HPE Aruba Networking ClearPass

Authentifizierung, Rollenzuweisung

Abbildung 3. Lösungskomponenten für die verteilte dynamische Segmentierung mit HPE Aruba Networking Central NetConductor

HPE Aruba Networking Central NetConductor – Lösungskomponenten

Die Komponenten von HPE Aruba Networking Central NetConductor ermöglichen eine verteilte dynamische Segmentierung zur Skalierung und Leistungssteigerung, wie in Abbildung 3 dargestellt.

- **HPE Aruba Networking Client Insights** — Die erste und einzige agentenlose Client-Transparenz- und Fingerprinting-Funktion, die in eine Cloud-native Verwaltungsplattform integriert ist und so dabei unterstützt, Schwachstellen im Netzwerk zu beseitigen. Das KI-basierte HPE Aruba Networking Client Insights nutzt die Telemetriedaten der Infrastruktur und ML-basierte Klassifizierungsmodelle, um eine Vielzahl von Clients – einschließlich IoT-Geräte – in der gesamten kabelgebundenen und kabellosen Infrastruktur zu identifizieren und ein präzises Profil zu erstellen
- **Cloud Auth** — Ermöglicht das reibungslose Onboarding von Endbenutzern und Client-Geräten entweder durch eine MAC-Adressen-basierte Authentifizierung oder durch die Integration mit gängigen Cloud-Identitätsspeichern wie Google Workspace™ oder Azure Active Directory, um automatisch die richtige Ebene des Netzwerkzugriffs zuzuweisen
- **Policy Manager** — Definiert Benutzer- und Gerätegruppen und erstellt die zugehörigen Durchsetzungsregeln für den Zugriff auf das physische Netzwerk (Abbildung 4)

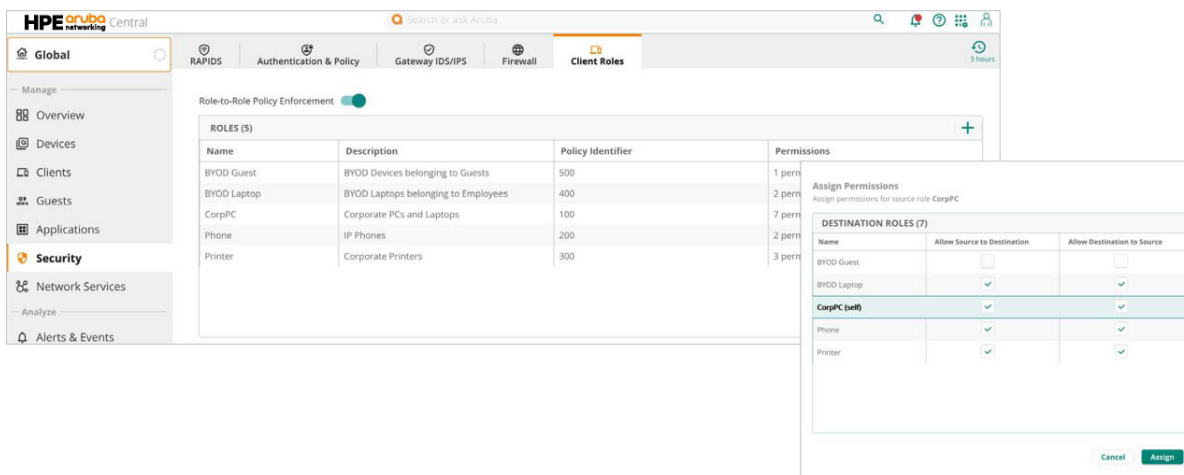


Abbildung 4. Intuitive, grafische Benutzeroberfläche für die Definition globaler Richtlinien

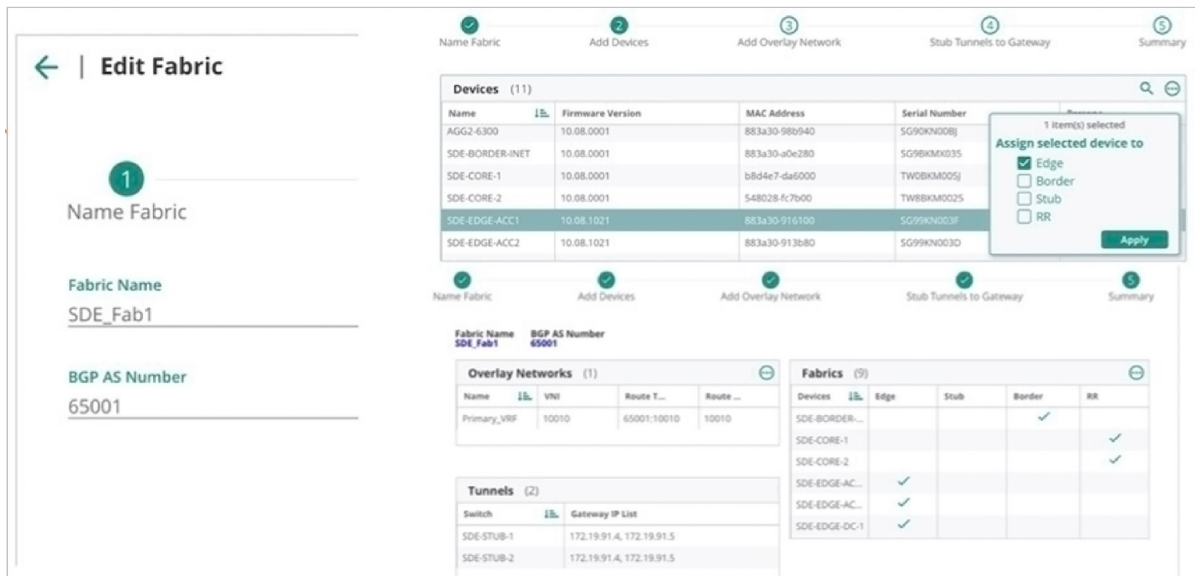


Abbildung 5. Benutzerfreundlicher, grafischer Workflow für eine vereinfachte Konfiguration und automatische Bereitstellung von Fabric-Overlay

- **Fabric-Wizard** — Vereinfacht die Erstellung von Overlays mithilfe einer intuitiven, grafischen Benutzeroberfläche, die die Definition virtueller Komponenten und die Generierung von Konfigurationsanweisungen und deren Weiterleitung an Switches und Gateways erheblich erleichtert (Abbildung 5)
- **GPID** — Überträgt Client-Richtlinieninformationen im Datenverkehr zur Inline-Richtliniendurchsetzung, was den Konfigurations- und Sicherheitsaufwand reduziert und die Mobilität und Skalierbarkeit erhöht
- **Fabric-fähige HPE Aruba Networking Switches und Gateways** — Unterstützen Konfiguration und Durchsetzung basierend auf den Routing-Anweisungen und Zugriffsrechten, die im GPID definiert sind

Hinweis: Netzwerke, die den HPE Aruba Networking Central NetConductor Policy Manager für die Orchestrierung von Richtlinien verwenden, können

entweder HPE Aruba Networking Central Cloud Auth oder HPE Aruba Networking Central ClearPass für die Authentifizierung und Rollenzuweisung nutzen.

Zentralisierte dynamische Segmentierung

Die zentralisierte dynamische Segmentierung war über mehrere Generationen von Netzwerktechnologien hinweg die Grundlage für die IT-Zugangskontrolle. Mit diesem Modell wird der Datenverkehr mithilfe eines zentralisierten Overlay, das aus GRE-Tunneln zwischen Access Points und HPE Aruba Networking Gateways (oder HPE Aruba Networking Mobility Controllern in Controller-basierten Umgebungen) besteht, sicher und getrennt gehalten. Gateways fungieren als Eintrittspunkte zur Durchsetzung von Richtlinien, die über die Rollen der Quell- und Zielclients oder -anwendungen informiert sind (Abbildung 6).

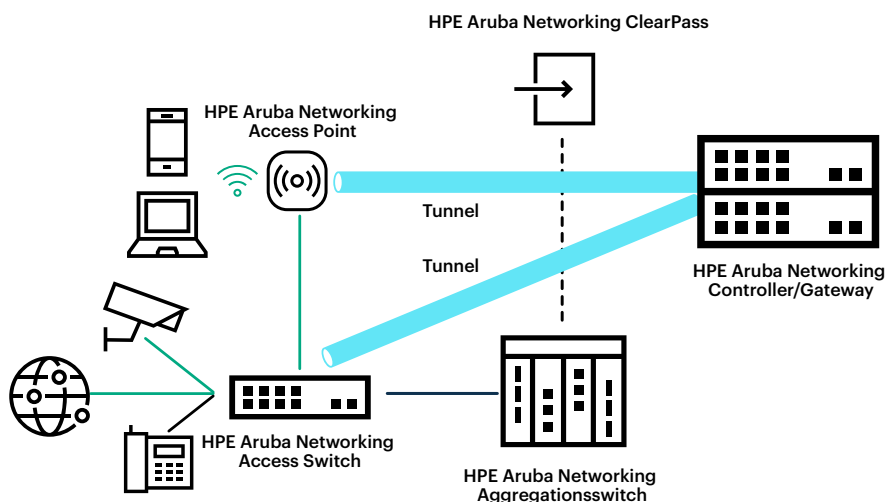


Abbildung 6. Zentralisierte dynamische Segmentierung von HPE Aruba Networking

Richtliniendefinition

Die zentralisierte Richtliniendefinition kann entweder durch HPE Aruba Networking ClearPass oder den HPE Aruba Networking Central NetConductor Policy Manager für das zentralisierte Durchsetzungsmodell erreicht werden.

HPE Aruba Networking ClearPass bietet Authentifizierungs- und Autorisierungsfunktionen sowie zentralisierte Richtliniendefinitionen, die dem Benutzer im gesamten Netzwerk folgen und einheitlich auf kabellose, kabelgebundene und VPN-Verbindungen angewendet werden. Wenn Benutzer zu einem unbekanntem Gerät wechseln oder sich in einem ungesicherten Netzwerk befinden, ändert die Richtlinie automatisch die Berechtigungen.

HPE Aruba Networking ClearPass unterstützt die normenbasierte 802.1X-Durchsetzung und andere Techniken zur sicheren Authentifizierung. Der Richtlinienmanager lässt sich in zahlreiche Authentifizierungslösungen integrieren, unterstützt Multifaktor-Authentifizierung und bietet die Möglichkeit, an wichtigen Punkten im Netzwerk eine erneute Authentifizierung zu erzwingen.

Für die umfassende integrierte Sicherheitsabdeckung und Reaktion unterstützt HPE Aruba Networking ClearPass das HPE Aruba Networking 360 Security Exchange Program mit über 150 Partnerintegrationen.

Erfahren Sie mehr über HPE Aruba Networking ClearPass Policy Manager.

Firewall zur Durchsetzung von Richtlinien

Herkömmliche Firewalls, die IP-basierte VLANs zur Kontrolle nutzen, werden erst nach der Zulassung eines Benutzers oder Geräts zum Netzwerk aktiv und

lassen so eine potenzielle Öffnung für fortgeschrittene Angriffe. Die zustandsabhängige Layer 7 Policy Enforcement Firewall (PEF) von HPE Aruba Networking nutzt Identität, Verkehrsattribute und andere Faktoren, um die Zugriffsrechte zum Zeitpunkt der ersten Verbindung zentral durchzusetzen. Die Inspektion des Datenverkehrs durch PEF liefert detaillierte Informationen über Benutzer, Geräte, Anwendungen und Standorte. PEF dient als zugrunde liegende Netzwerktechnologie, die die Durchsetzung von Richtlinien auf HPE Aruba Networking Gateways (oder Mobility Controllern in Controller-basierten Umgebungen) unterstützt.

Bereitstellung einer Auswahl an HPE Aruba Networking Dynamic Segmentation Modellen

Die Erweiterung von VLAN-basierten Architekturen mit einer EVPN/VXLAN-basierten intelligenten Overlay-Fabric löst isolierte Konfigurations- und Sicherheitsprobleme und unterstützt die Durchsetzung von Richtlinien in komplexen, global verteilten Netzwerken (Abbildung 7). Die Verwendung von allgemein anerkannten Protokollen ermöglicht die Interoperabilität zwischen verschiedenen Anbietern für die Integration mit Drittanbieter-Netzwerken, ohne dass die bestehende Infrastruktur komplett ausgetauscht werden muss.

Kunden können eine zentralisierte oder eine verteilte Overlay-Fabric oder beide Modelle verwenden, da beide Durchsetzungsmodelle in einer Umgebung gleichzeitig bestehen können. Unternehmen, die derzeit einen zentralisierten Ansatz verwenden, können flexibel einen verteilten Ansatz anwenden, bei dem die Durchsetzung durch die Zugriffsgeräte in ihrem eigenen Tempo erfolgt.

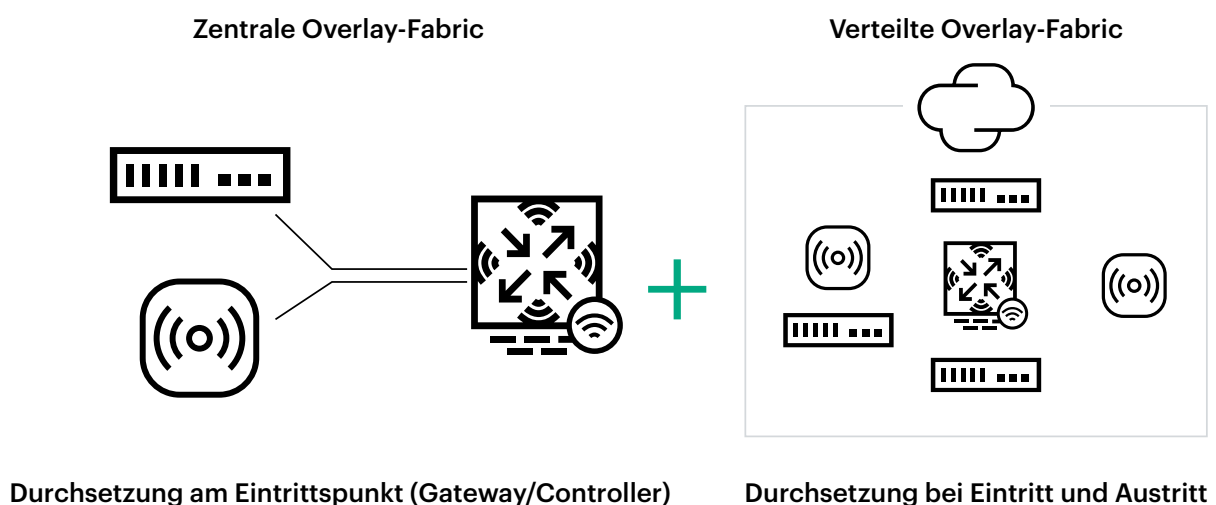


Abbildung 7. Durch Nutzung einer verteilten Overlay-Fabric für die Durchsetzung von Richtlinien an den Eintritts- und Austrittspunkten unterstützt die verteilte dynamische Segmentierung eine größere Skalierbarkeit und Leistung

Zusammenfassung

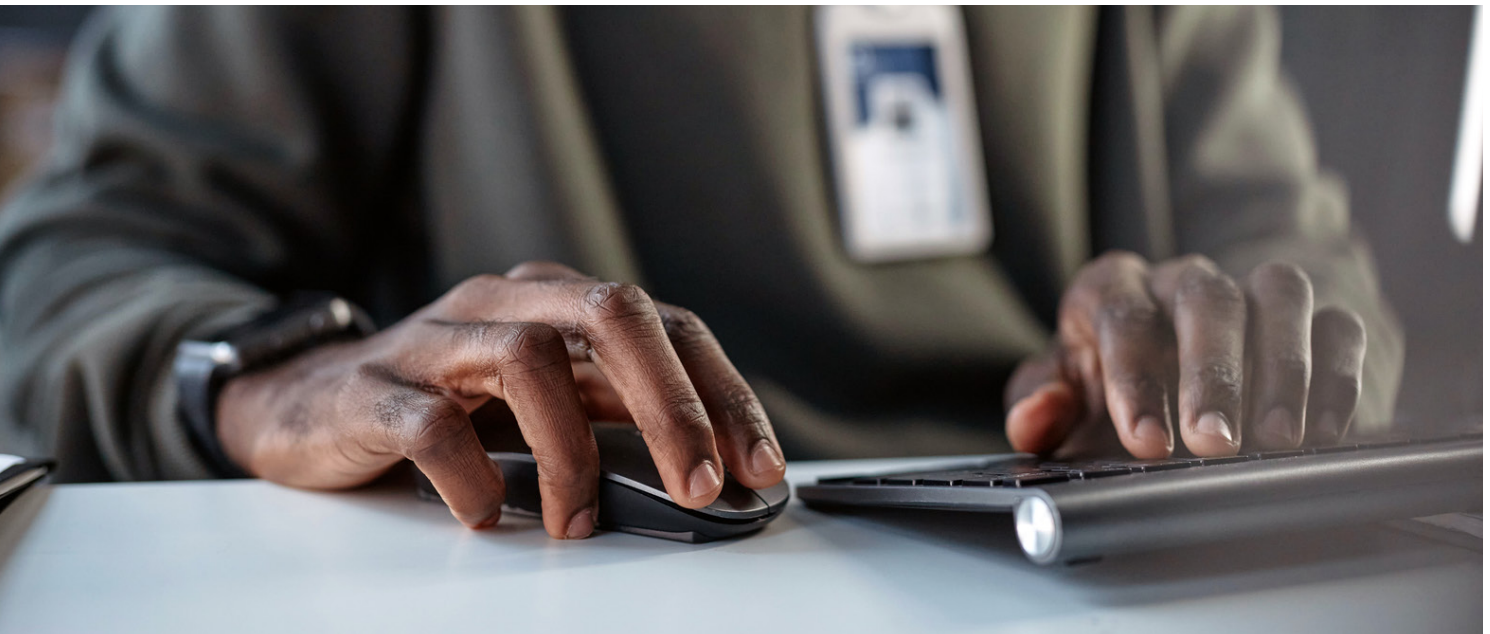
Für Unternehmen, die ihre Netzwerke besser schützen wollen, ist die Segmentierung von IoT, BYOD-Clients und Benutzerverkehr besonders wichtig. Mit dem innovativen Ansatz von HPE Aruba Networking Dynamic Segmentation kann die IT-Abteilung ein für die jeweilige Umgebung am besten geeignetes Modell auswählen, um die Sicherheit durch die dynamische Anwendung einheitlicher Richtlinien und Durchsetzungsfunktionen vom Edge zur Cloud zu verbessern. Dank der detaillierten rollenbasierten Zugriffsberechtigungen, die HPE Aruba Networking Dynamic Segmentation durchsetzt, können kompromittierte Benutzer und Clients ganz einfach von der Beteiligung an einem Angriff abgehalten werden, indem der Endpunkt-Client bei Erkennung eines Angriffs automatisch blockiert oder unter Quarantäne gestellt wird.

[HPE.com besuchen](#)

Weitere Informationen

[HPE.com/ww/
network-security](https://www.hpe.com/network-security)

Durch die Wahl zwischen zentralisierten und verteilten Modellen, die über die Cloud oder vor Ort bereitgestellt werden können, sind Unternehmen in der Lage, die entsprechenden Zugriffs- und Sicherheitsrichtlinien automatisch zu aktualisieren und fortlaufend in jeder Netzwerktopologie durchzusetzen. HPE Aruba Networking Dynamic Segmentation vereinfacht die Umsetzung von Zero-Trust-Sicherheits- und SASE-Frameworks unabhängig von der Größe und Komplexität des Netzwerks im globalen Maßstab.



Jetzt chatten

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Google Workspace ist eine eingetragene Marke von Google Inc. Active Directory und Azure sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Alle Marken von Dritten sind Eigentum der jeweiligen Rechteinhaber.

a00058593DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

