HPE NETWORKING ARUBA UND JUNIPER – TOGETHER

TAKTIKANALYSE FÜR EIN PERFEKTES PASSSPIEL

Webinar 2026

IHRE PRÄSENTATOREN

Christoph Semmelmann
Solution Engineer
Standort Regensburg

Christoph.Semmelmann@acp.de
+49 941 20605 450

Nathalie Greiner
Solution Engineer
Standort Hauzenberg

Nathalie.Greiner@acp.de
+49 8586 9604 166

AGENDA

1. Begrüßung & Einführung
2. Campus Networking bei HPE
3. Architekturvergleich
4. Juniper Kernkomponenten
5. Management & Monitoring
6. NAC-Vergleich
7. Mikrosegmentierung
8. Ausblick
9. Q&A

AUSGANGSLAGE: HPE + JUNIPER

Was ist passiert?

- HPE hat die Übernahme von Juniper Networks am 2. Juli 2025 abgeschlossen
- Zwei vollständige Campus-Portfolios unter einem Dach: HPE Networking Aruba und HPE Networking Juniper

Was bedeutet das für Ihr Netzwerk?

- Beide Plattformen werden parallel weiterentwickelt -> es gibt keinen erzwungenen Migrationspfad
- Geräteplattformen werden künftig in beiden Umgebungen einsetzbar sein

Ziel dieses Webinars

- Portfolio, Architektur, Management, NAC und Mikrosegmentierung im direkten Vergleich
- Entscheidungshilfe: Welche Plattform passt zu welchem Szenario?

2 CAMPUS NETWORKING BEI HPE

HARDWARE-PORTFOLIO

HPE aruba networking


AP 500 Series


AP 600 Series


AP 700 Series


Gateways



Outdoor AP


Remote AP

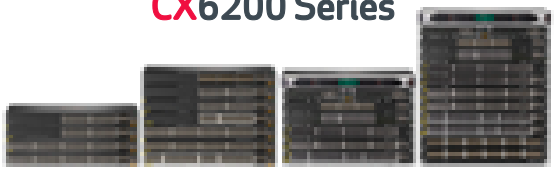

Hospitality


Cellular Bridge


CX6000/6100 Series


CX6200 Series


CX5420


CX6300 + CX6400 Series


CX4100i


AP-723H Dual Platform

HPE juniper networking


WIFI 5 Series


WIFI 6 Series


WIFI 7 Series


vBLE


EX3300/3400 Series

EX4000/4100 Series


EX4400/4600 Series


EX9200

WESHALB ZWEI PLATTFORMEN?

Zwei gewachsene, eigenständige Stacks

- Aruba: AOS-CX / AOS-10, Aruba Central, ClearPass, EdgeConnect
- Juniper: Junos, Data Center und Routing Lösungen, Mist als cloud-native AI-Plattform inkl. Access Assurance

Warum HPE beide Plattformen weiterführt

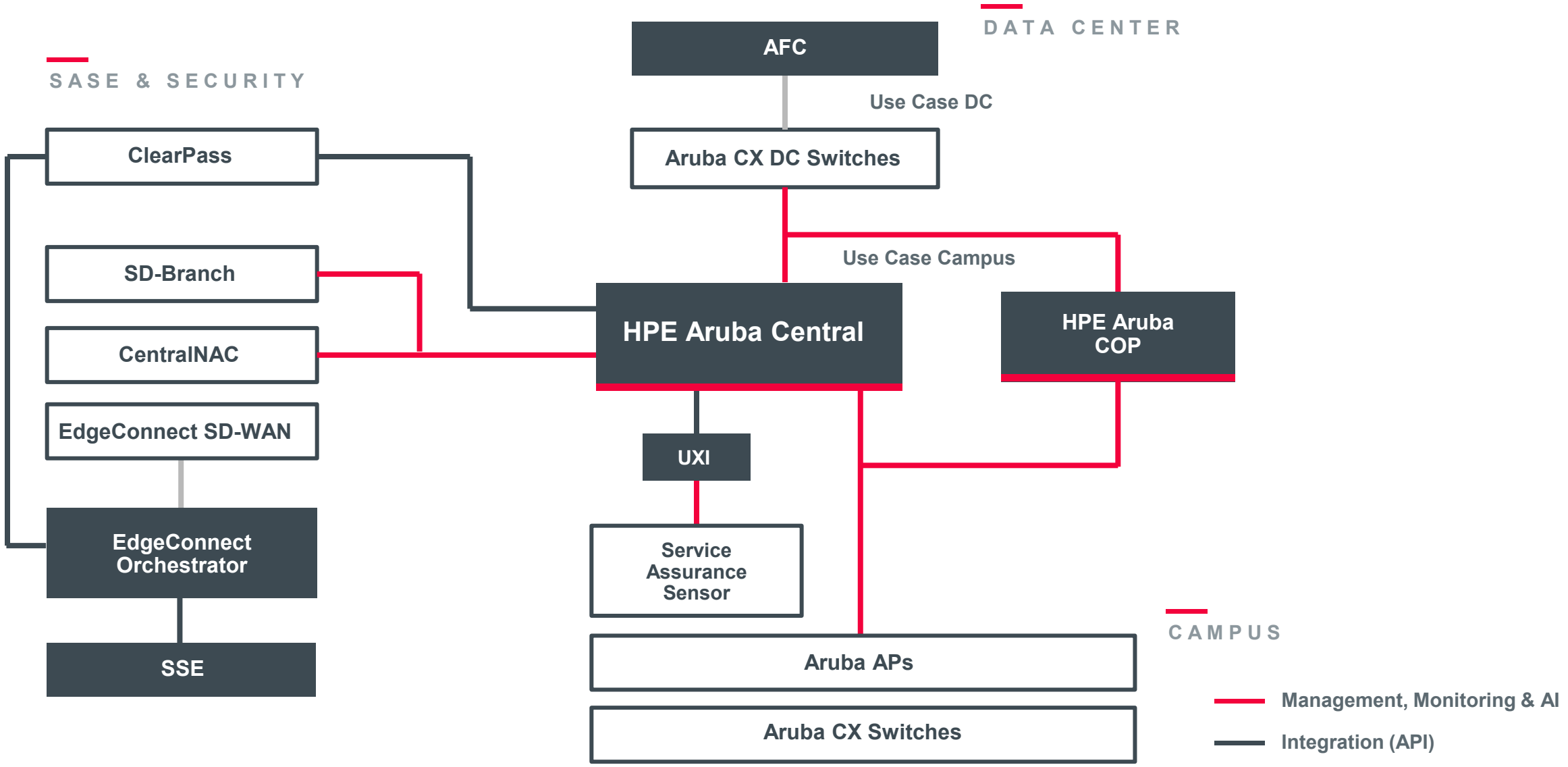
- Große, produktive Umgebungen auf beiden Seiten
- Komplementäre Stärken: Aruba im Campus, Branch und SASE; Juniper bei AIOps, EVPN-VXLAN-Fabric und Routing
- HPE Networking wird Central und Mist parallel weiterzuentwickeln

Was bereits zusammenwächst

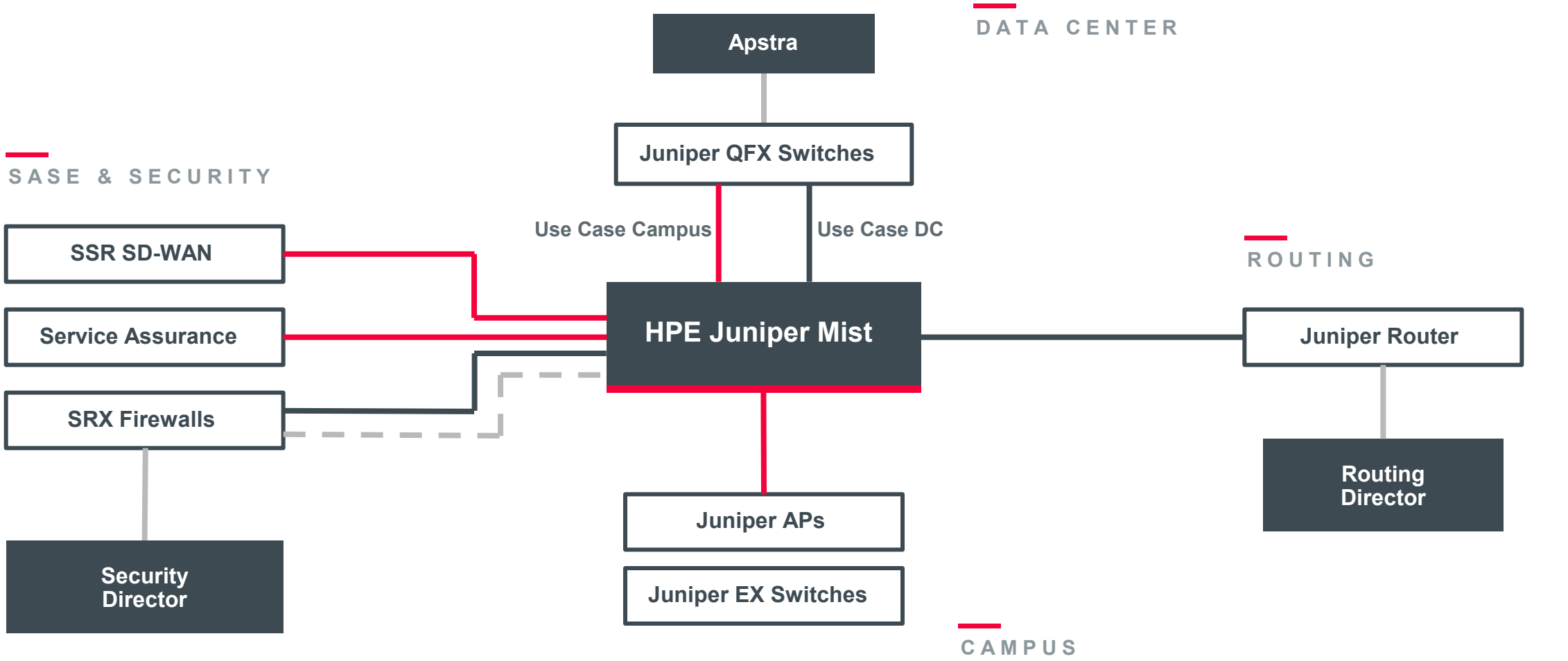
- Funktionsaustausch beider Plattformen: Mist Marvis nach Central, Arubas Agentic Mesh nach Mist
- Dual-Platform-Hardware wie der AP-723H

3 ARCHITEKTURVERGLEICH

HPE ARUBA



HPE JUNIPER



ARCHITEKTURVERGLEICH – KERNUNTERSCHIEDE

Ebene	HPE Aruba	HPE Juniper
Management	Aruba Central Cloud oder On-Premises	Mist Cloud
Campus-Switching	AOS-CX	Junos EX
WLAN	AOS-10 APs optional mit Gateways	Mist APs, cloud-terminiert
Fabric	EVPN-VXLAN mit AFC , AFC im Data Center	EVPN-VXLAN nativ, Apstra im Data Center
NAC	ClearPass oder Central NAC	Mist Access Assurance
AIOps	Central AIOps, Agentic Mesh, UXI-Sensoren	Marvis inkl. Conversational Interface, Marvis Minis
Segmentierung	Dynamic Segmentation: UBT/GRE und EVPN-GBP	Group-Based Policy mit SGT: Intra-Switch oder Fabric

4 JUNIPER KERNKOMPONENTEN

JUNIPER KERNKOMPONENTEN

Mist Cloud – die Plattform

- **Cloud-native:** Konfiguration deklarativ über Org → Sites → Templates statt Box-für-Box
- **API-First:** jede GUI-Funktion ist auch über REST-API, WebSocket-Telemetrie und Webhooks verfügbar

Kernkomponenten

- **Mist Access Points:** vBLE-Antennen-Array für Location Services, dynamische Paketerfassung, Junos-basiert
- **Junos EX Switches:** Wired Assurance, Zero-Touch-Provisioning, Campus-Fabric-Workflows aus der Cloud
- **SRX Firewalls:** Juniper Firewalls, Zentralisiertes Policy Management, Junos-basiert
- **Mist Access Assurance:** NAC mit 802.1X, MAB, EAP-TLS/TTLS und IdP-Anbindung
- **Marvis:** AI-Engine mit Conversational Interface, Marvis Actions und Marvis Minis

Lizenzierung

- **Subscription je Gerät und Funktion:** Wired/Wireless Assurance, Marvis, Access Assurance, Premium Analytics

5 MANAGEMENT & MONITORING

FULLSTACK-ANSATZ: CENTRAL VS. MIST

HPE Aruba Central – Fullstack für Campus, Branch und SASE

- Eine Konsole für Switching, WLAN, Gateways und die Central NAC-Integration
- Betriebsmodell wählbar: Cloud oder Central On-Premises – relevant für regulierte Umgebungen
- AIOps mit Agentic Mesh; UXI-Sensoren liefern herstellerunabhängige User-Experience-Messungen

HPE Juniper Mist – Fullstack für Wired, Wireless, WAN und NAC

- Eine Konsole für APs, EX-Switches, SSR/SD-WAN, SRX, Access Assurance und Marvis – konsequent cloud-only
- Einheitliche SLE-Sicht über alle Layer: Wired, Wireless und WAN Assurance im selben Datenmodell
- Marvis Minis als eingebaute Service Assurance – ohne separaten Sensor-Rollout

Worauf es im Betrieb ankommt

- Wird OnPrem tatsächlich benötigt? Oft reicht ein Gespräch mit dem Datenschutzbeauftragten
- Befinde ich mich bereits auf einer der beiden Lösungen?

| LIVE DEMO: ARUBA CENTRAL

Proaktives Monitoring und KI-gestützte Fehleranalyse für durchgängig verlässliche Netzwerke.

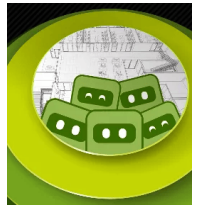
UXI

Sensor & agentenbasierte User-Experience-Insights

- ✓ Vendor-agnostic
- ✓ LAN & WLAN
- ✓ HW Sensor & User-Agent
- ✓ Path-Analytics
- ✓ Central Integration

Marvis Minis

Eingebaute, KI-gestützte Assurance ohne Zusatzhardware



- ✓ Built-in Solution für APs & EX Switches
- ✓ Inkludiert in Marvis für Wireless & Wired Subscription

| LIVE DEMO: UXI & MIST AI

6 NAC-VERGLEICH

Cloud-nativer NAC direkt in Aruba Central

- Neue, cloud-native NAC-Engine innerhalb Aruba Central ohne separate Appliance oder eigenen Cluster
- Policy-Konfiguration in derselben Konsole wie Switching und WLAN
- Verfahren: 802.1X mit EAP-TLS/TTLS/PEAP sowie MAC-Authentifizierung (MAB)

Policy-Modell

- Regeln matchen auf Identität, Gerätetyp und Standort
- Direkte Kopplung an Dynamic Segmentation wo die User Role die Mikrosegmentierung steuert
- IdP-Anbindung an Entra ID, Okta und Google Workspace optional Lokale PKI mit NAC Pro Lizenz

Reife und Einsatzbereich

- Funktionsumfang wächst schrittweise, aktuell geringer als ClearPass
- Zielgruppe: Central-Kunden ohne ClearPass, die auf eine einzige Cloud-Konsole setzen wollen

CLEARPASS IM DETAIL

On-Premises-NAC mit voller Funktionsbreite

- ClearPass Policy Manager, on-premises oder virtualisiert betrieben
- Herstellerunabhängig, auch Cisco-, HPE- und Drittanbieter-Infrastruktur anwendbar
- Verfahren: 802.1X mit EAP-TLS/TTLS/PEAP, MAC-Authentifizierung sowie TACACS+

Policy und Zusatzfunktionen

- Profiling zur automatischen Geräteerkennung, Gast-Portale, BYOD-Self-Onboarding, Endpoint-Posture-Checks
- ClearPass Extensions/Exchange binden SIEM, MDM und ITSM per API oder Syslog an
- Ergebnis der Policy: Radius IETF Attribute sowie Vendor Specific Attributes z.B. VLAN ID, User Role oder SGT

Betrieb

- On-Premises-Cluster erfordert eigenes Patch-, Kapazitäts- und Hochverfügbarkeitsmanagement
- Sinnvoll bei heterogener Infrastruktur, Cloud-Ausschluss oder TACACS+/Posture-Anforderungen

MIST ACCESS ASSURANCE IM DETAIL

Cloud-nativer NAC ohne Appliance

- Kein RADIUS-Cluster im Rechenzentrum: die Authentifizierung terminiert redundant in der Mist Cloud
- Verfahren: 802.1X mit EAP-TLS, EAP-TTLS und PEAP sowie MAC-Authentifizierung (MAB)
- Identitätsquellen: Entra ID, Okta, Google Workspace, LDAP/AD sowie eigene PKI bzw. SCEP-Anbindung

Policy-Modell

- Auth-Policies matchen auf User-Gruppe, Zertifikatsattribute, Gerätetyp, MAC, Standort und Zeit
- Ergebnis der Policy: VLAN, Rolle oder Security-Group-Tag – identisches Regelwerk für LAN und WLAN
- Zero Trust: das zugewiesene Tag geht direkt in die Mikrosegmentierung über (GBP)

Betrieb und Troubleshooting

- Client-Journey zeigt alle Auth-Events pro Client – keine separate NAC-Loganalyse erforderlich
- Marvis benennt Fehlerursachen wie abgelaufene Zertifikate, falsche Trust-Chain oder IdP-Timeouts

NAC: ENTSCHEIDUNGSHILFE

Stärken Central NAC

- Vereinfachte Implementierung und unkompliziertes Deployment (Basis 802.1X und MAB ohne eigene Zertifikate)
- In der Aruba Central Subscription enthalten (für eigene Zertifikate → Advanced Lizenz notwendig)

Stärken ClearPass

- Größte Funktionsbreite: Profiling, Guest, BYOD-Onboarding, TACACS+, Posture, Drittanbieter-Integration
- On-Premises betreibbar und herstellerübergreifend – auch für Nicht-Aruba-Infrastruktur

Stärken Mist Access Assurance

- Kein Appliance-Lifecycle: Skalierung, Updates und Georedundanz sind Teil des Service
- Ein Policy-Modell für LAN und WLAN, IdP-zentrisch, direkt gekoppelt an Marvis und GBP

Entscheidungshilfe

- Cloud-first, IdP-basiert, Juniper-Infrastruktur → Mist Access Assurance
- Heterogene Umgebung, TACACS+, Posture-Anforderungen oder Cloud-Ausschluss → ClearPass

7 MIKROSEGMENTIERUNG

MIKROSEGMENTIERUNG – ANSÄTZE IM ÜBERBLICK

Warum Mikrosegmentierung

- IoT, OT, Gäste und BYOD teilen denselben Campus – VLAN-Grenzen genügen als Sicherheitsgrenze nicht mehr
- Ziel: die Rolle folgt Nutzer und Gerät, unabhängig von Port, VLAN und Standort (Zero Trust)

Die drei Umsetzungsvarianten

- Aruba Dynamic Segmentation mit User-Based Tunneling: GRE zum Gateway, Durchsetzung per Stateful-Firewall
- EVPN-VXLAN mit Group-Based Policy: das Tag reist im Overlay, Durchsetzung fabricweit
- Juniper GBP Intra-Switch: das Tag bleibt lokal am EX-Switch, Durchsetzung per Firewall-Filter

Gemeinsame Bausteine

- Identität aus 802.1X oder MAB – über ClearPass, Central NAC oder Mist Access Assurance
- Rolle bzw. Tag ist die einzige Policy-Referenz; nur explizit erlaubte Kommunikation wird zugelassen
- Beide Hersteller nutzen die VXLAN-GBP-Semantik – gleicher Ansatz, unterschiedliche Werkzeuge

8 AUSBLICK

Zwei Plattformen, ein gemeinsamer Weg

- ✓ Beide Plattformen werden weiterhin getrennt betrieben (Mist und Central)
- ✓ Weitere Dual-Platform-Geräte folgen
- ✓ Juniper-Geräte werden künftig in New Central unterstützt
- ✓ Aruba-Geräte werden künftig in Mist inkl. Konfiguration unterstützt
- ✓ Marvis wird in Aruba Central integriert

9 Q&A – IHRE FRAGEN, UNSERE ANTWORTEN

VIELEN DANK

FÜR IHRE AUFMERKSAMKEIT

ACP | IT FOR INNOVATORS