

Universal ZTNA

Ken Van Campenhout

September 29th, 2026

HPE Networking for Security? Many places to start!



Unified SASE

Create consistent SD-WAN and SSE experiences

Enforce global policies for remote and on-prem users



Universal ZTNA

Employ zero trust principles for people, IoT devices and workloads

Leverage network as a security sensor to detect and respond dynamically



Hybrid Mesh Firewall

Deploy cloud-native firewall management for branch, DC and VPC

Establish global policies w/ uniform execution (physical, virtual, container & cloud)



Full-Stack AIOps

Manage SD-WAN, Wired & Wireless via one agentic AIOps platform

Implement AI-native service assurance and remediation (LAN/WAN)



The business landscape has shifted

Hybrid and remote access are the new norm

Security is critical for remote and on-premise access

Cloud & on-premise apps require equal security measures

Data governance is critical in a cloud-first and AI world

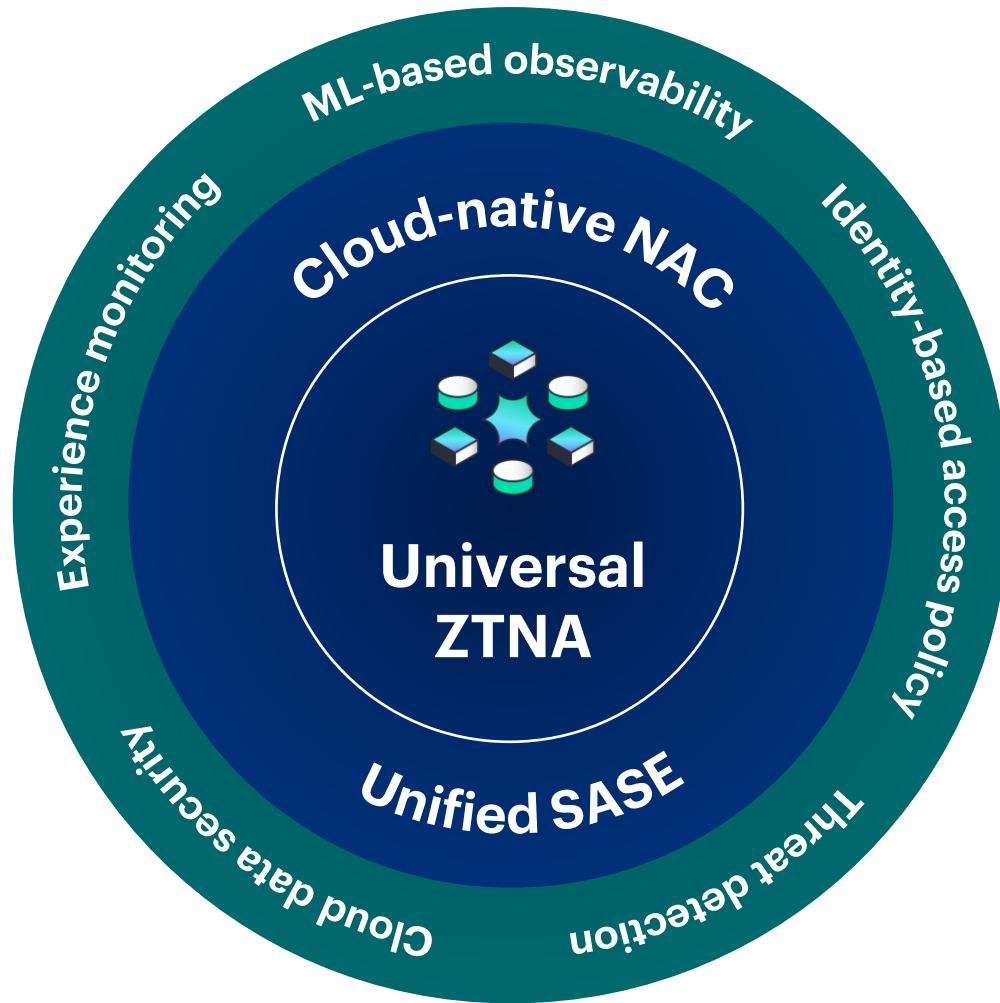
Regulatory & compliance requirements must be maintained



Universal ZTNA, powered by HPE Networking



Universal ZTNA



Zero trust extended to non-human identities

Zero trust everywhere

Centralized policy management



Digital transformation breaks with an old-world approach

Hub & Spoke



Adopting SaaS

Guaranteed level of service, scale and accessibility, cost effective, simple integration – making SaaS security critical



Adopting Public Cloud

Reduces CapEx, rapid app deployment, high performance and availability – making securing across hybrid cloud key



Adopting Mobility

Workforce can connect from anywhere - making user experience more important than ever

The workplace has evolved and it's time secure connectivity did too.



Traditional Network

Built for backhauling traffic to DC from branch and remote sites to network



Traditional Security

Appliance-based products tethered to the data center, focused on protecting the network versus user to application connection



New Advanced Threats

Increase in sophisticated threats exploiting vulnerabilities, including legacy network security architectures



A modern approach to secure connectivity with SSE

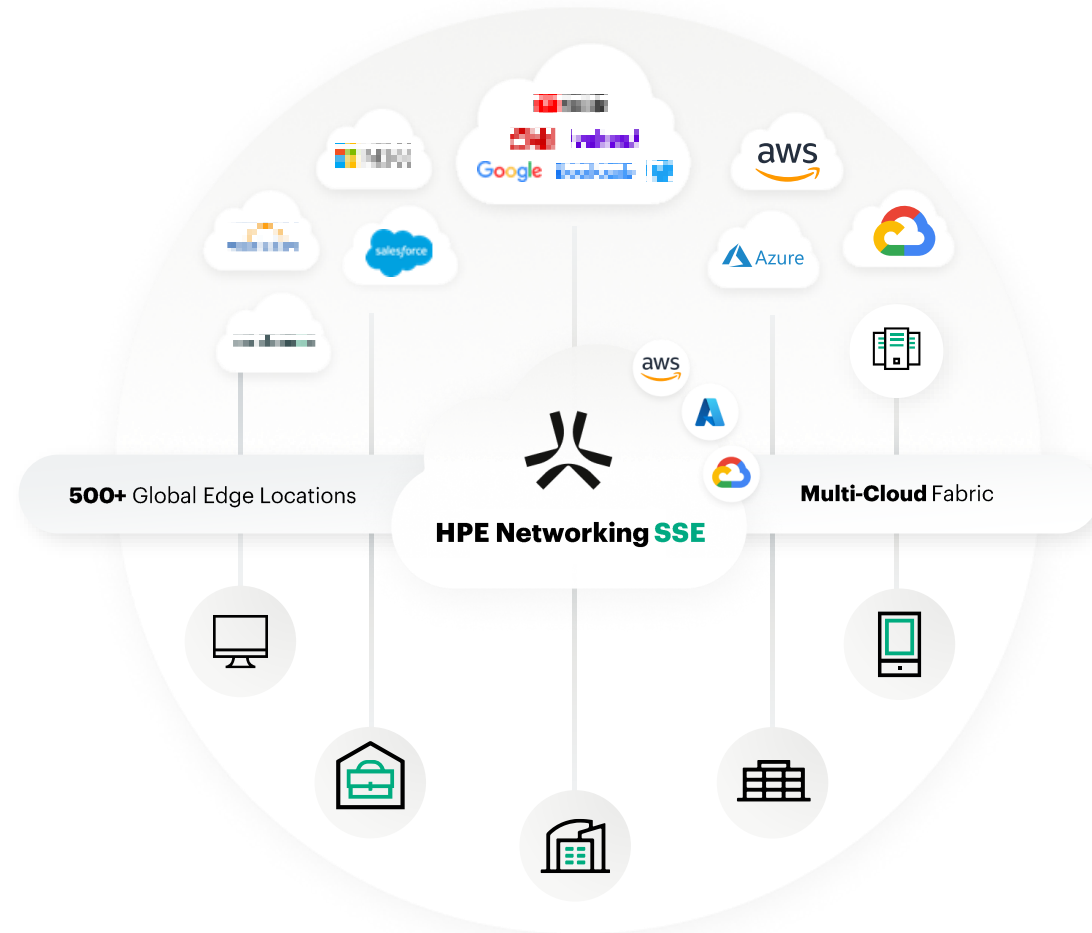
HPE Networking Security Service Edge (SSE)

✓ **Secure access for all resources**

Secure access across any private app, Internet site, or SaaS app - using modern zero trust capabilities

✓ **Unified service – power of one**

Unified ZTNA, SWG, CASB and DEM service with one cloud, one UI, and one policy



✓ **Intelligent cloud global scale**

500+ edges across 5 continents running an AWS, Azure, and Google backbone

✓ **Prioritized user experience**

Smart-routing, SSO/MFA integrations, digital experience monitoring, and an intuitive User Portal



HPE Networking SSE platform

The pillars of SSE

Zero Trust Network Access

Secure access to **private applications** in the data center or cloud.

i.e Minimize app exposure to Internet, remove network access, replace VPN, Inspect traffic, support all private apps

Cloud Access Security Broker

Secure access to **SaaS applications** and protect against data loss.

i.e Control block upload/download from Box, Sharepoint, Facebook, Salesforce



Digital Experience Monitoring

Monitor **user performance** and troubleshoot user access issues for all traffic.

i.e Monitor performance of each session, minimize mean time to remediation of user issues

Secure Web Gateway

Secure access to **the Internet** and protect against malicious online threats.

i.e Filtering, SSL inspection, malware scanning, reputation-based blocking, Sandboxing

Firewall as a Service

Cloud-native firewall enforcement that **protects and governs network traffic**.

i.e 5-Tuple Firewall enforcement, supports full protocol and traffic control, RFI/RFP and compliance requirements



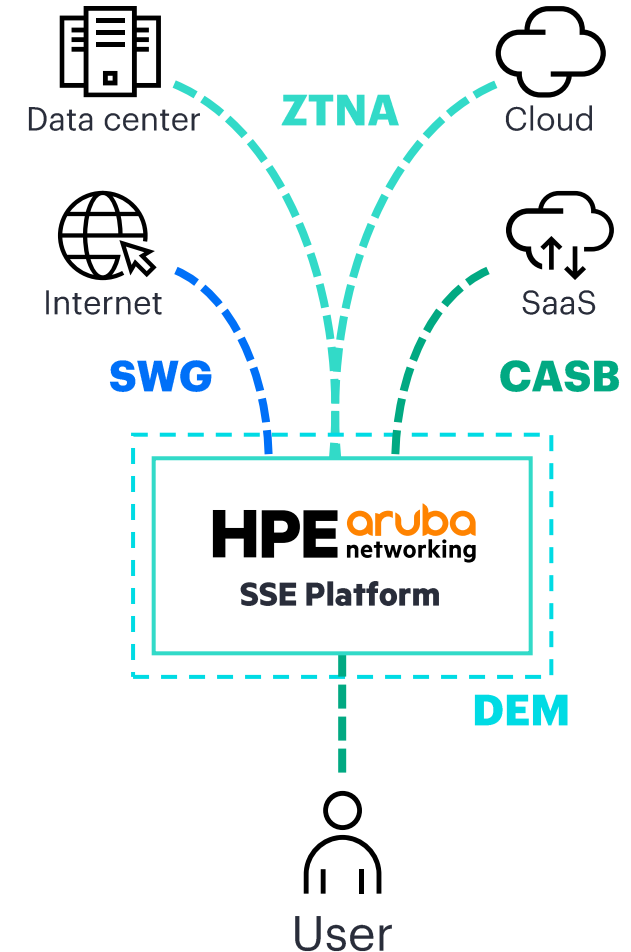
What's so different about HPE Aruba Networking SSE

Focus is on unify – one UI, one policy, one platform (ZTNA, SWG, CASB, FWaaS, DEM)

Goal is to **simplify policy & inspect any traffic** for Internet, SaaS, and legacy apps (SSH, RDP, VOIP, AS400, ICMP etc.)

Ability to **harmonize access across the world** via smart routing and a cloud-backbone on AWS, Azure, Google, and Oracle

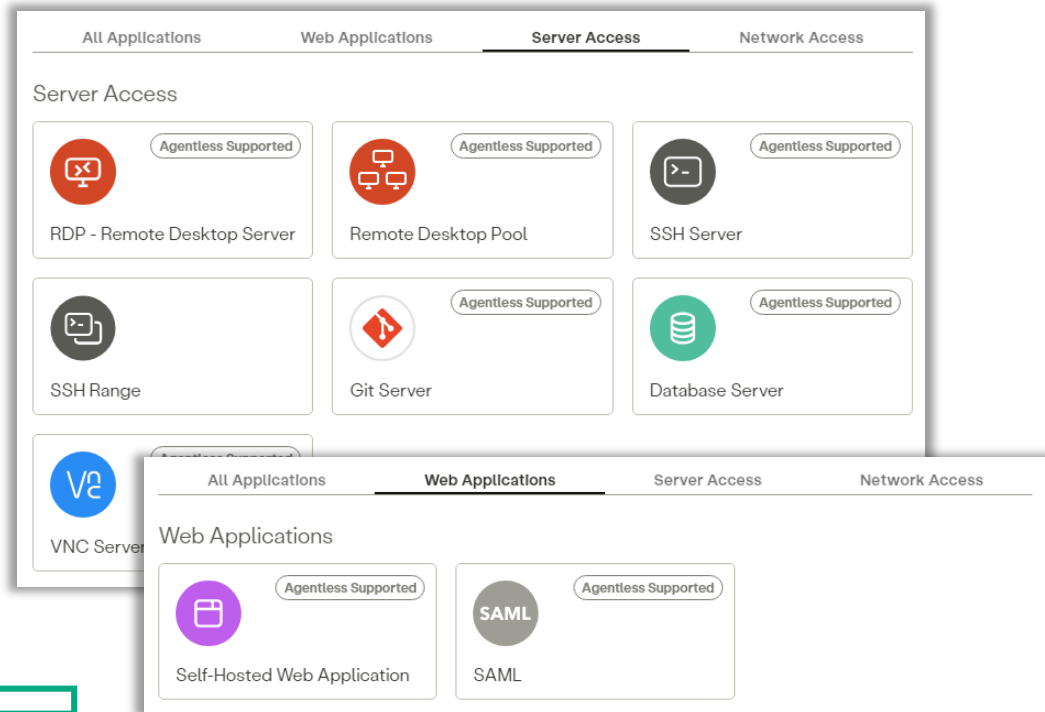
Purposely designed to enable users to access resources **with or without an agent**



Every user the right access

Agentless access for BYOD / External Users

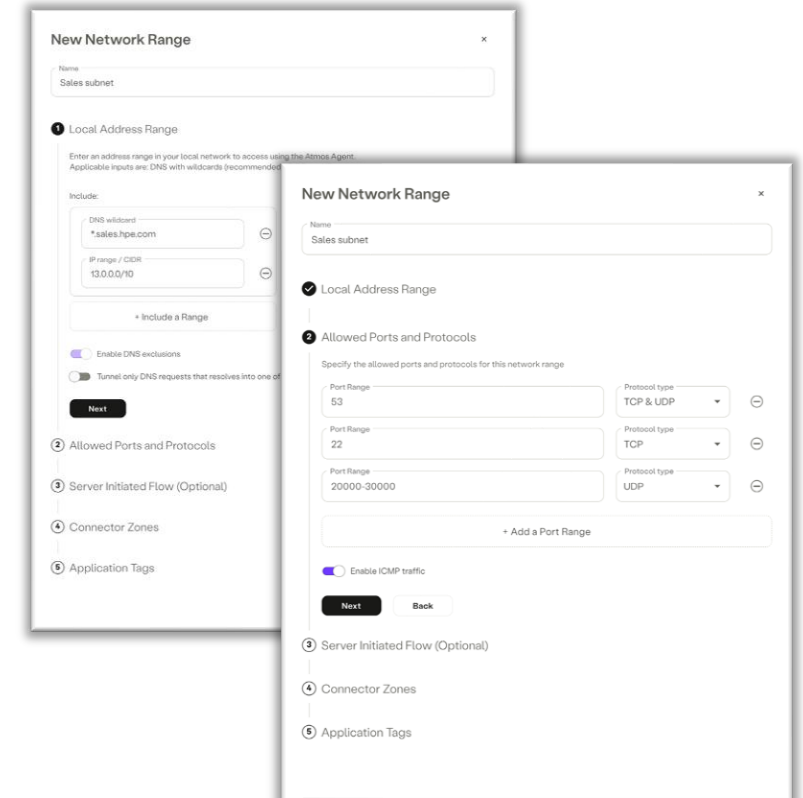
Access to Web, RDP, SSH, Git, and DB applications with a seamless user experience and granular visibility and control



Agent/IPsec for internal users and things

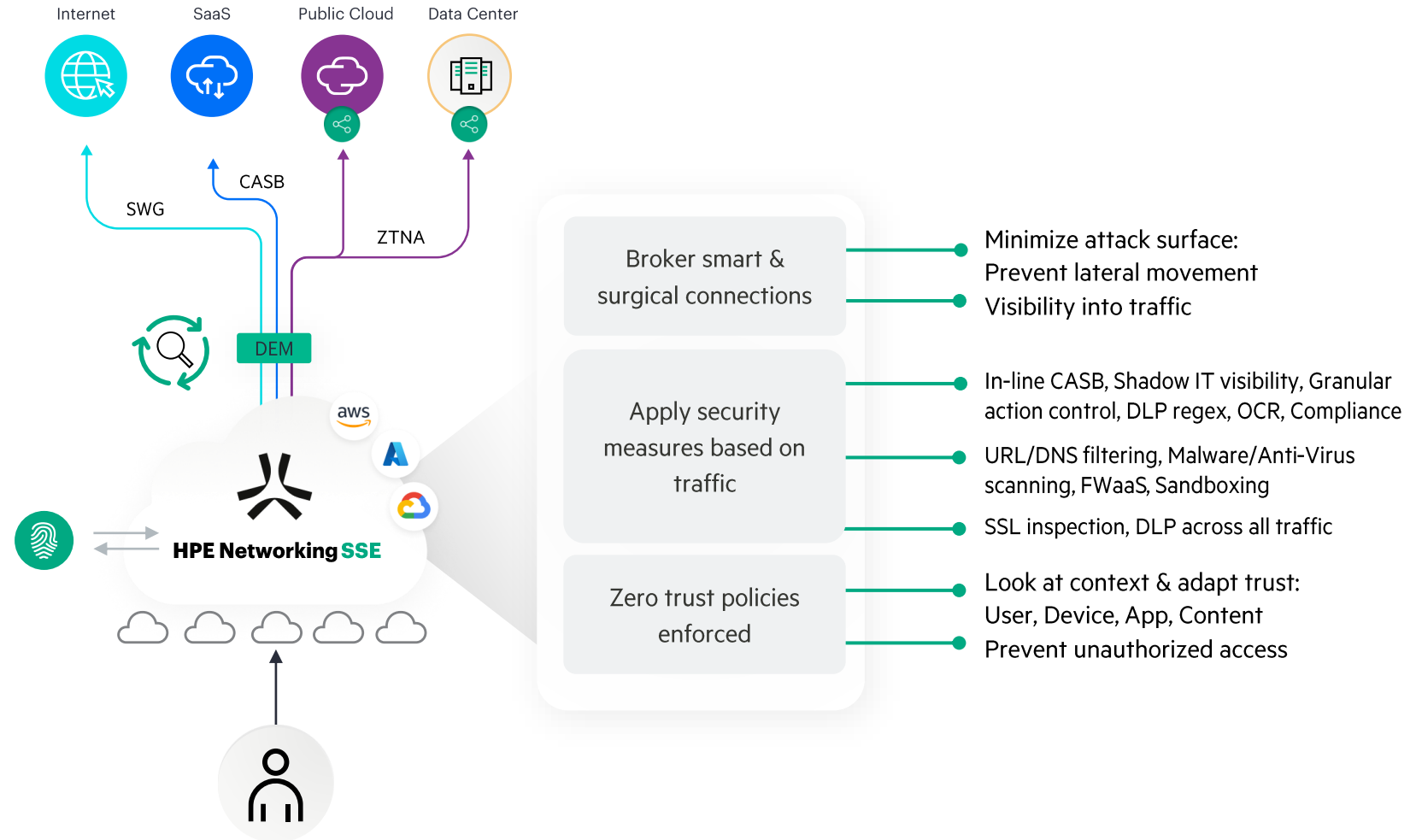
Define **granular access** based:

- Domain name
- IP level
- ...



HPE Networking SSE in action

- 1 User requests access**
Agent or agentless access with automatic end-point security profiling
- 2 SSE mediates request**
Auto-routes traffic to closest of 500 global edge locations
- 3 User is identified and authenticated**
Process traffic for access authorization and Identity + MFA verification
(Support of multiple IDPs)
- 4 Policies are enforced and security measures applied**
Access is brokered through 1:1 connections, securing every connection
- 5 Policy is continuously inspected,**
adapting access as needed, enforcing security, and monitoring user performance



Single user-centric policy for all SSE traffic

Insights	Policy Filter.. Last changes applied on October 31st 3:03 am by or@axissecurity.com New Rule							
Policy	Priority	Enabled	Name	Users	Context	Destinations	Action	Profiles
Settings	1	☒	SSH internal	Daniel Reisel	Any	Any Application	Allow	Default Profiles
Experience	2	☒	High Risk Nations	Any	Iraq Russia North Korea	Any Application	Block	Default Profiles
	3	☒	Block Malware, Gambling, Dropbox Uploads	All Full Time Employees...	Windows Baseline Mac Baseline	DropBox - Managed Box Managed Pornography and Adult Malware Sites Gambling	Block	Client SSL Inspection And 5 Default Profiles
	4	☒	All Employees - Managed Devices	All Full Time Employees...	Windows Baseline Mac Baseline iOS Device Posture	Salesforce All Employee Apps VOIP SSL Exclusion Category	Allow	Default Profiles
	5	☒	All Employees - BYOD	All Full Time Employees...	Any	All Employee Apps SSL Exclusion Category	Allow	BYOD Policy And 5 Default Profiles
	6	☒	Accounting Team - Accounting Apps	Accounting	Any	Accounting Apps	Allow	Default Profiles
	7	☒	HR Team - HR Apps	Human Resources	Windows 10 + patches Crowdstrike Enabled	HR Apps	Allow	Default Profiles
	8	☒	Contractors - Contractor Apps	Contractors	Any	Contractor Apps	Allow	Contractors RDP Profile

Block access from risky destinations

Define access to internal and external apps in a single policy

Leverage rich device posture for context

Use app tags to simplify management

≡ 4	☒	All Employees - Managed Devices	👤 All Full Time Employees...	🔧 Windows Baseline 🔧 Mac Baseline 🔧 iOS Device Posture	☁ Salesforce 📄 All Employee Apps 📄 VOIP 🌐 SSL Exclusion Category	✅ Allow	Default Profiles
≡ 5	☒	All Employees - BYOD	👤 All Full Time Employees...	Any	📄 All Employee Apps 🌐 SSL Exclusion Category	✅ Allow	📄 BYOD Policy - And 5 Default Profiles
≡ 6	☒	Accounting Team - Accounting Apps	👤 Accounting	Any	📄 Accounting Apps	✅ Allow	Default Profiles
≡ 7	☒	HR Team - HR Apps	👤 Human Resources	🔧 Windows 10 + patches 🔧 Crowdstrike Enabled	📄 HR Apps	✅ Allow	Default Profiles
≡ 8	☒	Contractors - Contractor Apps	👤 Contractors	Any	📄 Contractor Apps	✅ Allow	📄 Contractors RDP Profile > BYOD / Contractor Policy 📄 Contractors Web App Pr... 📄 Contractors SSH Range ... 🔗 Contractor Git Profile 📄 Default Client Security P...
≡ 9	☒	3rd Parties - Web RDP	👤 Self-Guided Users	Any	📄 3rd Party Apps	✅ Allow	📄 Web-Only > BYOD / Contractor Policy 📄 Contractors Web App Pr... 📄 Contractors SSH Range ... 🔗 Contractor Git Profile 📄 Default Client Security P...
≡ 10	☒	Developer Access	👤 Dev Admins 👤 AWSSolutionArchitects...	Any	↔ DevOps AWS 📄 SA Team 📄 Developer Apps	✅ Allow	Default Profiles
≡ 11	☒	Axis App Discovery - Managed Devices	👤 All Full Time Employees...	🔧 Windows Baseline 🔧 Mac Baseline 🔧 iOS Device Posture	↔ Axis App Discovery	✅ Allow	Default Profiles
Default	☒	Applications Default Rule	Any	Any	Any Application ①	❌ Block	Default Profiles
Default	☒	Web Traffic Default Rule	Any	Any	Web Traffic ①	✅ Allow	📄 Client SSL Inspection - And 5 Default Profiles

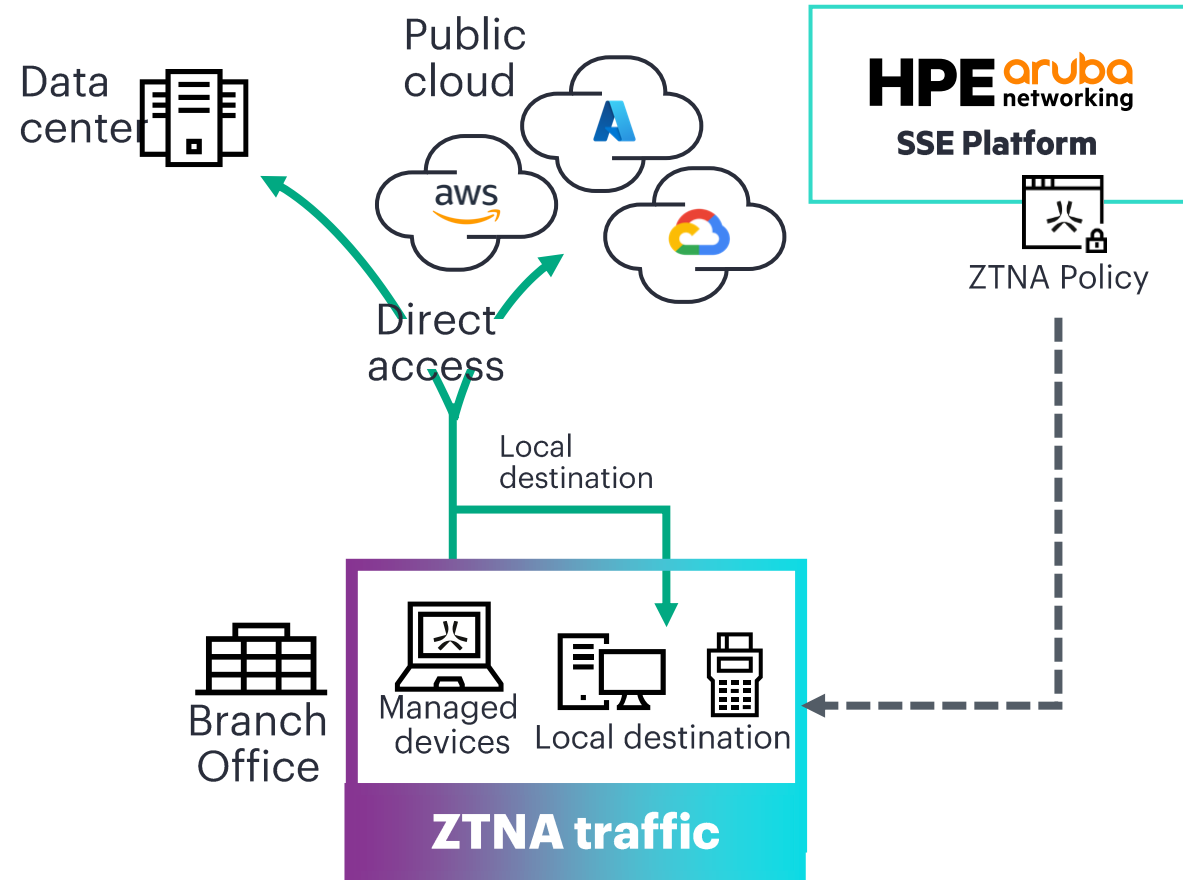
Securely enable developer workflows

HPE Aruba Networking ZTNA Private Edge

Eliminate the need to route local traffic to the cloud

ZTNA Private Edge

- Ensures that on-prem traffic stays local, eliminating hairpin routing to the cloud and boosting performance
- Enforces the same access control policies defined for remote users
- Included in each ZTNA license



46% of teams start their SSE journey with ZTNA



Secure third-party access

Secure access for your highest-risk users while empowering a more productive and connected business ecosystem



VPN Replacement

Empower your remote and hybrid workforce with seamless, secure remote access, no VPN required



Accelerate Mergers & Acquisitions

Speed up, simplify, and secure IT integration for your next mergers and acquisitions project

SD-WAN + SWG

**Continue your
SASE journey**

**Universal ZTNA
(NAC + ZTNA)**





Now that I have
cloud-native security,
why do I need NAC?



ZTNA & NAC are complimentary

ZTNA

Controls access to **applications** (on-prem & cloud)

Provides **identity-based, per-application access control**

Secures users **anywhere** (remote or internal)

HPE products: HPE Security Services Edge

NAC

Controls access to the **network** (LAN/WLAN)

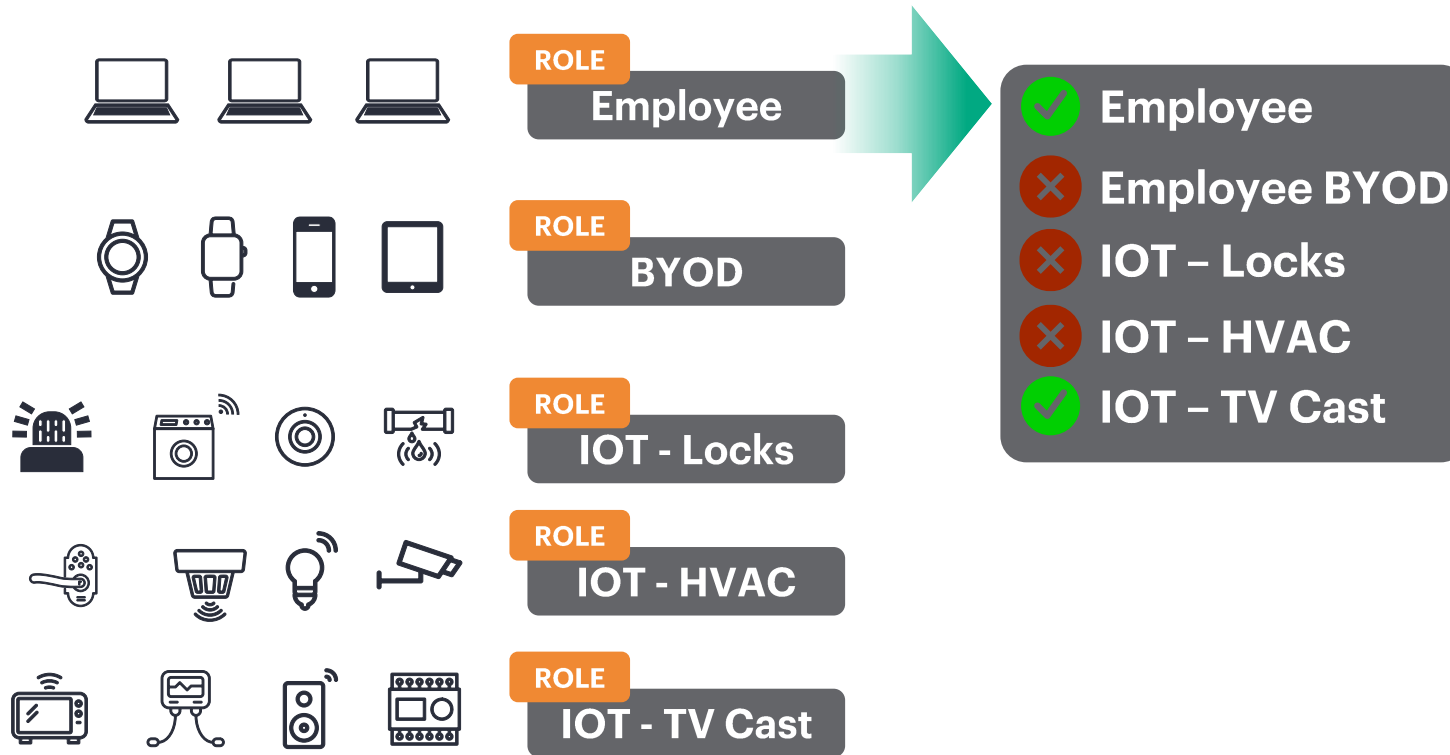
Provides **device visibility, profiling, and segmentation**

Secures users and devices **inside the network**

HPE products: ClearPass, Cloud NAC

Even in a full SSE implementation NAC remains important to segment IoT devices within the local network.

HPE Aruba Networking User Roles



DYNAMIC SEGMENTATION

Software defined approach eliminates VLAN sprawl and simplifies policy implementation

Delivers wired, wireless, and SD-WAN micro-segmentation needed for securing end-user and IoT devices

What is Central NAC?



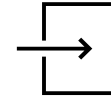
**Most advanced, market leading
cloud delivered Network Access Control solution**



Authentication



Authorization



Visitor Access

Delivered via HPE Aruba Networking Central, enabling customer to



Rapidly deploy Zero
Trust security



Create and deploy a
unified security policy
across campus and branch



Secure network with a robust
NAC, at no extra cost



Leverage AI powered
profiling for advanced
network access control

Included in Central Foundation License

Central NAC - core



Granular security policies
for wired and wireless



Simplified configuration,
management, and monitoring



Seamless and secure
visitor (guest) access



Role based authorization –
context derived from Client
Insights, category, groups.



Support for various Authentication
methods:

- EAP-TLS
- MAC Auth Bypass,
- MPSK - named and admin (limited to 5K)
- 802.1X – wired/wireless,
- Captive Portal – with customization



**Robust Authentication, Authorization, and
Guest Access delivered via Cloud**

Ad-on license – Central NAC subscription

Central NAC - pro

Central NAC – core features



Integration with multiple IDPs

- Microsoft Entra ID
- Google Workspace
- Workforce Identity Cloud



Third-party NAD support



Support for Bring-your-own
CA/Certs (BYOC)



Supports robust authorization
policy with more context
parameters



Support for unlimited MPSK



Ease of implementation

Intuitive UI – easy to use
Very short learning curve for IT
teams



Cost saving

No hardware - buying,
deploying, or maintaining



NAC at no extra cost

NAC core functions included in
Central Foundation License



Enterprise scalability and uptime

Leverages cloud scalability and high
uptime redundancy



ClearPass trust

Developed by the same ClearPass team
trusted by customers & analysts across
the globe



HPE ClearPass: The on-premises alternative

End-to-end user & device visibility, control, and automation



Vendor-neutral—**no lock-in**



Questions?



Thank you!

ken.van-Campenhout@hpe.com

