medhurst
making IT work

Networking Security

How Secure Is Your Network?

Aruba Makes It Stronger!

01489 563000
www.medhurst-it.com

CALL OUR SALES TEAM TODAY

medhurst
making IT work

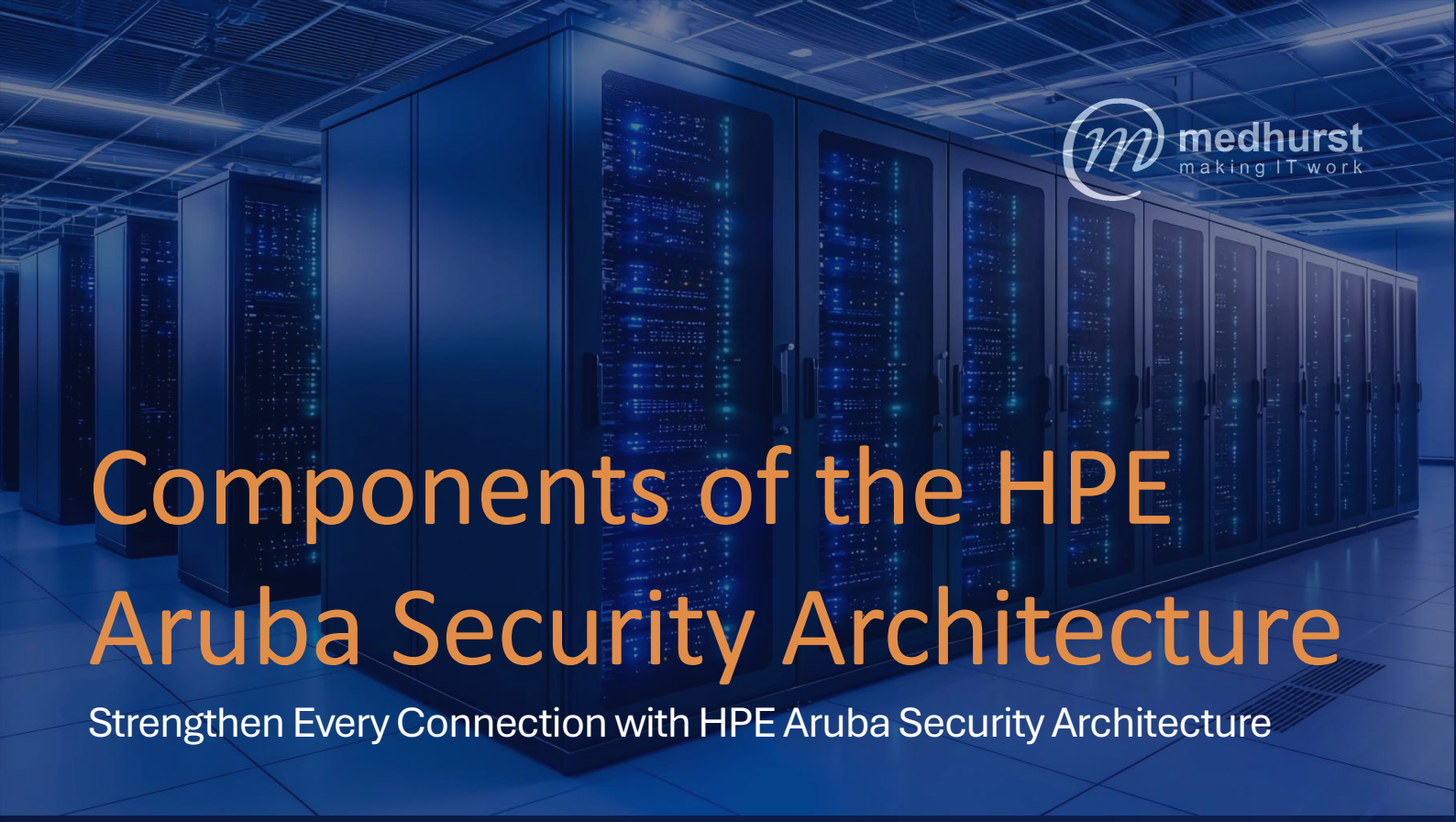
How secure is your Networking Infrastructure

Strengthen Every Connection with HPE Aruba Security Architecture

Modern networks demand more than raw performance—they require intelligence, context, and continuous verification. As organizations adopt cloud services, hybrid work, and an ever-growing range of connected devices, traditional perimeter-based security models simply aren't enough. What's needed is a network that recognizes who and what is connecting, adapts based on real-time conditions, and provides complete visibility from the edge to the cloud.

Aruba's Zero-Trust approach delivers exactly that. Instead of assuming that traffic inside the network is trustworthy, Aruba verifies every user, device, and application before granting access—and continues to validate behaviour throughout the session. Identity becomes the foundation of access, ensuring that each connection receives only the minimum level of permissions required. This reduces risk, limits lateral movement, and keeps critical resources protected even if a device is compromised.

With adaptive policy enforcement, automated segmentation, and unified visibility across wired, wireless, and WAN environments, Aruba transforms the network into a dynamic security platform. The result is a network that's not just fast, but inherently secure ensuring that only the right users and the right devices access the right resources, at the right time, and under the right conditions.



Components of the HPE Aruba Security Architecture

Strengthen Every Connection with HPE Aruba Security Architecture

Aruba User Roles Identity-Driven Access

Aruba User Roles provide a powerful, context-aware method of controlling access across the entire network. Instead of relying on static VLANs, port configurations, or broad firewall rules, User Roles tie access directly to who the user is, what device they are using, and the real-time conditions of the connection.

Identity as the Foundation

Each user or device is assigned a role based on credentials, authentication method, device type, security posture, or group membership. This ensures that employees, contractors, IoT devices, and guests each receive the precise level of access they need—no more, no less.

Consistent Enforcement Everywhere

Whether connecting through wired ports, wireless access points, or remote VPN sessions, Aruba applies the same role-based policies across the entire infrastructure. This consistency eliminates security gaps and ensures uniform behaviour regardless of how or where the user connects.

Security Applied at the Edge

Aruba enforces User Roles directly at the network edge, at the access point, switch port, or VPN gateway, before traffic is allowed deeper into the environment.

- Unwanted, unauthorized, or suspicious traffic is blocked immediately.
- Only validated users and trusted devices are granted access to internal resources.
- Micro-segmentation at the edge dramatically reduces the blast radius of any potential compromise

By stopping threats before they enter the network, Aruba prevents lateral movement and reduces dependency on internal firewalls or legacy segmentation methods.

Components of the HPE Aruba Security Architecture

Strengthen Every Connection with HPE Aruba Security Architecture

Access Control Lists (ACLs) Precision Traffic Control
Aruba's role-based ACLs provide fine-grained, context-aware control over how users and devices communicate across the network. Rather than relying on broad, static rules, ACLs allow administrators to define exactly which applications, destinations, and services each role is permitted to access—creating a precise security posture tailored to every connection

Role-, Application-, and Destination-Aware Filtering
ACLs dynamically enforce traffic policies based on:

- User or device role (employee, guest, IoT, contractor)
- Application type (business-critical, cloud, web, restricted)
- Destination networks, services, or microsegments

This fine-grained approach ensures that traffic flows only where it's explicitly allowed, eliminating the open pathways that attackers often exploit.

Restricts Unnecessary Lateral Communication
By limiting device-to-device communication, ACLs prevent endpoints from interacting unless they have a defined business need.

- IoT devices can't talk to each other unnecessarily.
- Guest clients stay isolated.
- Users can only reach the applications tied to their role.

This drastically reduces the potential attack surface within the network.

Components of the HPE Aruba Security Architecture

Strengthen Every Connection with HPE Aruba Security Architecture

Aruba Central Cloud-Powered Visibility & Intelligence

Aruba Central serves as the unified cloud command centre for end-to-end network operations, security, and user experience optimization. By consolidating management, policy orchestration, monitoring, and AI-driven analytics into a single platform, Central removes the complexity of managing distributed environments and enables organizations to scale with confidence.

Unified Management and Policy Orchestration

Aruba Central provides a centralized dashboard for configuring, monitoring, and managing networks across campuses, branches, remote workers, and data centres

- All network elements—wired, wireless, WAN, and security—are managed through a single interface.
- Role-based access control (RBAC) and granular administrative privileges ensure secure multi-team operations.
- Policy changes can be created once and pushed everywhere, dramatically reducing manual configuration effort.

This unified model removes the need for siloed tools and ensures every location follows the same security and performance standards.

Consistent Role and ACL Deployment Across All Sites

Through Central, administrators can define Aruba User Roles, ACLs, segmentation policies, and onboarding workflows centrally and automatically distribute them across the entire network.

- Every site, from headquarters to remote offices, receives the same policies.
- Updates are validated and synced in real time, minimizing drift between devices.
- Micro-segmentation policies follow users and devices wherever they connect.

This ensures that Zero-Trust principles are enforced consistently across all environments.

Components of the HPE Aruba Security Architecture

Strengthen Every Connection with HPE Aruba Security Architecture

Aruba ClearPass Policy Brain of the Network

Aruba ClearPass is the central intelligence engine that determines who and what is allowed to connect to the network. Acting as the policy decision point (PDP) for Zero-Trust security, ClearPass evaluates identity, device posture, context, and threat signals before granting any level of network access. ClearPass ensures that every connection - wired, wireless, or VPN is authenticated, authorized, and continuously validated.

Robust AAA for Identity Validation

ClearPass provides advanced Authentication, Authorization, and Accounting (AAA) services capable of handling complex enterprise environments.

- Supports 802.1X, certificate-based authentication, SAML, OAuth, TACACS+, and legacy methods.
- Leverages user directories (AD, LDAP, cloud identity providers) for real-time identity verification.
- Enforces fine-grained authorization based on role, group membership, authentication method, or device type.

By ensuring identity integrity from the start, ClearPass forms the foundation of least-privilege access.

Comprehensive Device Posture & Health Checks

Before granting access, ClearPass evaluates device posture to determine trustworthiness.

- OS version, patch level, running services
- Endpoint security status (AV, EDR agents, firewall status)
- Compliance with enterprise policies
- Device category detection (IoT, BYOD, corporate-managed)

If a device fails posture checks, ClearPass can automatically quarantine, limit access, or deny connection preventing risky endpoints from reaching sensitive resources.

Components of the HPE Aruba Security Architecture

Strengthen Every Connection with HPE Aruba Security Architecture

Dynamic Policy Enforcement Through Threat Integration

ClearPass integrates with a wide range of security ecosystems, including EDR/XDR platforms, SIEMs, vulnerability scanners, and firewalls.

- Consumes threat intelligence feeds
- Reacts to alerts (e.g., compromised device, malware event, suspicious activity)
- Automatically adjusts User Roles or ACL policies in real time
- Can trigger quarantine, re-authentication, or VLAN/segment changes

This turns the network into an adaptive security platform capable of responding instantly to evolving threats.

Summary of the Flow

1. Device connects (wired or wireless).
2. Aruba infrastructure fingerprints the device to identify type and OS.
3. ClearPass handles identity authentication using AAA protocols.
4. Posture assessment determines whether the device is healthy/compliant.
5. ClearPass calculates the appropriate User Role (dynamic authorization).
6. User Role is enforced at the edge via ACLs and micro-segmentation.
7. Device gains only the permissions allowed by its role.

www.medhurst-it.com | 01489 563000