International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V7I2P140
Eureka Vision Publication | Volume 7, Issue 2, 331-336, 2026

Original Article

Zero-Trust Wireless Architectures in Healthcare: Integrating Aruba ClearPass for Granular Policy Enforcement

Srinivas Maganti
Independent Researcher, USA.

Received On: 11/04/2026 ***Revised On: 10/05/2026*** ***Accepted On: 18/05/2026*** ***Published On: 24/05/2026***

Abstract - Healthcare wireless networks present a uniquely challenging security environment characterized by high device density, strict uptime requirements, and a substantial population of Internet of Medical Things (IoMT) devices incapable of supporting traditional endpoint protection. Perimeter-based and endpoint-centric security models have proven inadequate in this context. This paper proposes and evaluates a Zero Trust Architecture (ZTA) framework for enterprise healthcare wireless local area networks (WLANs), implemented through Aruba Networks ClearPass as the centralized identity and policy enforcement plane. The framework integrates Network Access Control (NAC) with wireless Intrusion Detection and Prevention Systems (IDPS) to achieve continuous identity verification, dynamic micro-segmentation, and automated closed-loop threat enforcement. Deployed across a multi-campus healthcare environment encompassing more than 7,000 access points, 120 controllers, and 20,000 users across 60+ clinical sites, the architecture reduced detection-to-enforcement latency to under 200 milliseconds, decreased unauthorized access incidents by 73–78%, and reduced manual remediation requirements by 60–85%, with zero clinical downtime during security enforcement events. Results demonstrate that network-centric Zero Trust enforcement, anchored by ClearPass-based policy orchestration, constitutes a viable and scalable security model for critical healthcare wireless environments.

Keywords - Zero Trust Architecture, Healthcare Wireless Security, Aruba ClearPass, Network Access Control, IoMT Security, IDPS, EAP-TLS, WLAN Security, Identity-Driven Segmentation, Clinical Network Resilience.

1. Introduction

The accelerating digitization of healthcare has produced enterprise wireless environments of extraordinary complexity. Modern hospital networks must simultaneously support mobile clinical workstations, real-time patient telemetry, imaging platforms, and a rapidly expanding population of Internet of Medical Things (IoMT) devices infusion pumps, cardiac monitors, ventilator controllers, and diagnostic sensors many of which were designed without security considerations and lack the computational resources to support conventional endpoint protection software [1].

Historically, healthcare network security relied on perimeter-based models: a trusted interior separated from untrusted external networks by firewall and gateway controls. This model presupposes that devices operating within the network boundary are inherently trustworthy an assumption that has become untenable as hospital networks grow more porous through bring-your-own-device (BYOD) policies, telemedicine endpoints, cloud-integrated clinical applications, and the proliferation of unmanaged IoMT devices that cannot self-authenticate or self-report posture [2].

The consequences of inadequate healthcare wireless security are severe and well-documented. Healthcare organizations represent the most targeted sector for ransomware attacks, with breaches causing operational shutdowns, delayed patient care, and significant financial and reputational damage [3]. The 2020 Universal Health Services ransomware incident, which affected 400 hospitals across the United States and United Kingdom, demonstrated the systemic vulnerability of healthcare networks operating under legacy security models [4].

Zero Trust Architecture (ZTA), formalized by NIST SP 800-207, offers a fundamentally different security model: no device or user is trusted by default, regardless of network location; all access is continuously validated against identity, posture, and policy; and the principle of least privilege governs every session [5]. In theory, ZTA directly addresses the structural vulnerabilities of healthcare wireless environments. In practice, the implementation of Zero Trust in clinical settings requires careful adaptation to the operational constraints of hospital networks most critically, the inability to install agents on IoMT devices and the unacceptability of clinical downtime during security enforcement events.

This paper presents a practical Zero Trust framework for enterprise healthcare WLANs, implemented using Aruba Networks ClearPass as the centralized policy and identity enforcement plane, integrated with wireless IDPS to achieve automated closed-loop threat response. The framework was deployed and validated across a large multi-campus healthcare system. The paper makes the following contributions:

- A Zero Trust enforcement architecture adapted specifically to healthcare WLAN constraints, including agentless IoMT device security;
- A closed-loop NAC-IDPS integration model enabling sub-200-millisecond detection-to-enforcement response at enterprise scale;
- Quantified performance metrics from a production deployment spanning 7,000+ access points, 120+ controllers, and 60+ clinical sites;
- A comparative analysis of ZTA against prior security approaches in healthcare wireless environments.

The remainder of the paper is organized as follows: Section II reviews related work. Section III describes the threat model and healthcare-specific security constraints. Section IV presents the proposed framework architecture. Section V details the implementation and deployment methodology. Section VI presents evaluation results. Section VII provides comparative analysis. Section VIII discusses limitations and future work. Section IX concludes.

2. Related Work

2.1. Zero Trust Architecture in Enterprise Networks

The Zero Trust model was first articulated by Kindervag [6] and subsequently formalized by NIST in Special Publication 800-207 [5]. Rose et al. provided the foundational conceptual framework defining the seven tenets of Zero Trust, emphasizing continuous validation of identity and device posture as prerequisites for network access. Subsequent work by Stafford [7] examined ZTA deployment models including identity-centric, micro-segmentation, and software-defined perimeter approaches. While these frameworks provide theoretical grounding, they do not address the specific constraints of healthcare wireless environments, including IoMT device limitations and clinical uptime requirements.

2.2. Healthcare Network Security

Coventry and Branley [8] provided a comprehensive review of cybersecurity vulnerabilities in healthcare, identifying IoMT device insecurity and legacy infrastructure as primary risk vectors. Fu and Blum [9] analyzed security challenges specific to medical device software, noting the infeasibility of conventional patching and endpoint protection for resource-constrained clinical devices. Kruse et al. [10] examined healthcare data breach patterns and found wireless network intrusions among the most frequent initial access vectors. These findings motivate the network-centric enforcement approach proposed in this paper.

2.3. Network Access Control and IDPS Integration

Prior work on NAC systems has addressed enterprise access control in general IT environments [11], but limited research addresses NAC deployment in clinical settings where device agent installation is infeasible. Scarfone and Mell [12] provided foundational guidance on IDPS architectures, identifying the gap between detection and enforcement as a persistent operational limitation. Existing literature does not, to the authors' knowledge, address closed-loop NAC-IDPS integration specifically optimized for healthcare WLAN environments at the scale evaluated in this work.

2.4. EAP-TLS and Certificate-Based Authentication

The use of EAP-TLS for 802.1X-based network authentication has been examined in enterprise contexts [13]. Healthcare-specific implementations of certificate-based authentication for IoMT device onboarding remain underrepresented in the literature. The framework presented here extends EAP-TLS deployment to agentless medical device populations, addressing the identity attestation gap identified by prior authors.

3. Threat Model and Healthcare-Specific Constraints

3.1. Threat Model

The threat model considered in this work encompasses the following adversarial scenarios in healthcare wireless environments:

- Unauthorized device access: rogue devices, including attacker-controlled hardware mimicking legitimate clinical devices, gaining network access through credential theft or MAC spoofing.
- Lateral movement: a compromised endpoint traversing from a lower-sensitivity network segment (e.g., guest WLAN) to clinical or administrative systems through insufficient segmentation.
- IoMT exploitation: exploitation of unpatched or unmanaged medical devices as initial access vectors, leveraging their inability to detect or resist endpoint-level attacks.
- Man-in-the-middle (MITM) attacks: interception of wireless clinical data through rogue access point deployment or wireless deauthentication attacks.
- Ransomware propagation: automated propagation of ransomware payloads through flat or insufficiently segmented healthcare networks, as observed in multiple documented incidents [4].

3.2. Healthcare-Specific Constraints

Healthcare wireless environments impose constraints not present in standard enterprise networks that must be accommodated by any viable security framework:

- IoMT agent incompatibility: the majority of medical and clinical IoMT devices operate on proprietary real-time operating systems (RTOS) or embedded firmware that cannot support security agent installation. Enforcement must occur at the network infrastructure layer.
- Clinical uptime requirements: any security enforcement action must preserve continuous operation of life-critical systems. VLAN reassignment, session termination, and quarantine actions must be executed without disrupting active clinical sessions on unaffected devices.

- High device heterogeneity: enterprise healthcare networks contain thousands of device types across clinical, administrative, IoMT, and guest categories, each requiring distinct access policies.
- Regulatory compliance: healthcare networks are subject to HIPAA Security Rule requirements, including audit controls, access controls, and transmission security provisions that must be satisfied by the enforcement architecture [14].

4. Proposed Framework Architecture

4.1. Architectural Overview

The proposed Zero Trust Wireless Architecture (ZTWA) for healthcare is organized around three functional planes: the Identity Plane, the Policy Enforcement Plane, and the Threat Response Plane. Aruba ClearPass Policy Manager (CPPM) serves as the central orchestration engine, integrating all three planes into a unified enforcement model.

The identity plane handles device and user authentication using EAP-TLS certificate-based mechanisms and 802.1X supplicant validation. The policy enforcement plane translates authenticated identity into network access parameters dynamic VLAN assignment, role-based ACL application, and SSID policy enforcement. The threat response plane integrates ClearPass with wireless IDPS to close the enforcement loop: anomalous behavior detected by the IDPS triggers automated policy re-evaluation and enforcement actions within the sub-200-millisecond latency target.

4.2. ClearPass Component Architecture

The ClearPass deployment architecture consists of the following integrated components:

ClearPass Policy Manager (CPPM) functions as the RADIUS/TACACS+ authentication server and central policy decision point. All authentication requests from wireless infrastructure traverse CPPM, which evaluates requests against device identity, user role, time-of-day policies, and device posture attributes before issuing an access decision.

ClearPass Profiler performs agentless device fingerprinting using DHCP, HTTP User-Agent, SNMP, and behavioral signatures to classify device type and assign profile attributes. This capability is critical for IoMT devices that cannot self-identify through agent-based mechanisms.

ClearPass OnGuard provides posture assessment for devices that do support agent installation, including Windows clinical workstations and managed laptops. Posture non-compliance triggers dynamic policy change through the enforcement framework.

ClearPass Guest manages non-enterprise device onboarding through a provisioning portal, issuing time-limited credentials and assigning devices to restricted network segments.

4.3. Zero Trust Principle Mapping

Table I maps the five core Zero Trust principles defined in NIST SP 800-207 to their corresponding ClearPass implementation mechanisms and healthcare applications.

Table 1. Zero Trust Principles Mapped to ClearPass Enforcement Mechanisms

ZT Principle	ClearPass Module	Enforcement Mechanism	Healthcare Application
Verify Explicitly	Policy Manager	EAP-TLS / 802.1X	Certificate-based auth for IoMT and clinical staff
Least Privilege Access	Policy Enforcement Point	Dynamic VLAN / ACL Assignment	Role-based segmentation for clinical, IoMT, guest
Assume Breach	OnGuard / CPPM	VLAN reassignment, session termination	Automated quarantine on anomaly detection
Continuous Validation	Profiler / CPPM	Real-time re-authentication	Device posture re-evaluation on behavioral change
Micro-segmentation	Policy Manager	SSID + VLAN policy per device class	Isolation of infusion pumps from EHR systems

4.4. Closed-Loop NAC-IDPS Enforcement Model

The core innovation of the proposed framework is the integration of ClearPass NAC with wireless IDPS to create a closed-loop enforcement system. In conventional deployments, IDPS generates alerts that require human analyst review before enforcement action is taken, introducing latency measured in minutes to hours. The proposed framework eliminates this gap through direct API integration between the IDPS engine and ClearPass.

The enforcement loop operates as follows: (1) The wireless IDPS detects anomalous device behavior unauthorized scanning, deauthentication floods, protocol violations, or behavioral deviation from established baselines. (2) The IDPS assigns a risk score and triggers a policy update request via the ClearPass REST API. (3) CPPM evaluates the updated risk context against policy rules and issues a Change of Authorization (CoA) RADIUS message to the relevant access point or controller. (4) The controller executes the enforcement action VLAN reassignment, ACL application, or session termination within the sub-200-millisecond latency window. This architecture transforms threat response from a reactive, human-mediated process into an automated control operating at network speed, directly addressing the enforcement latency gap identified in prior literature.

4.5. IoMT Agentless Onboarding Framework

IoMT device security is managed through a dedicated onboarding and enforcement workflow that requires no

software installation on the medical device. Device identity is established through EAP-TLS certificate provisioning at the point of network registration. ClearPass Profiler maintains continuous device fingerprinting throughout the device lifecycle, detecting behavioral deviations that may indicate compromise or misconfiguration. Devices are confined to purpose-specific network segments through dynamic VLAN assignment, preventing lateral movement into clinical data or administrative systems.

5. Implementation and Deployment Methodology

5.1. Deployment Environment

The framework was deployed across a multi-campus enterprise healthcare system comprising 60+ clinical and administrative sites. The wireless infrastructure encompasses 7,000+ Aruba access points, 120+ Aruba wireless controllers, and supports 20,000+ enterprise users in addition to a substantial population of IoMT and clinical devices. The deployment included parallel migration from a legacy mixed Cisco-Aruba infrastructure to a standardized Aruba-based architecture under ClearPass policy control.

5.2. Phased Deployment Strategy

Given the clinical uptime constraints described in Section III-B, the deployment was executed in four phases designed to minimize disruption to active clinical operations:

- Phase 1: Infrastructure Preparation: ClearPass cluster deployment, certificate authority (CA) establishment, and RADIUS server configuration. Existing wireless infrastructure operated in parallel without policy enforcement changes.
- Phase 2: Identity and Authentication Migration: Phased rollout of EAP-TLS certificate provisioning to managed enterprise devices. Legacy PEAP-MSCHAPv2 authentication maintained in parallel during transition to prevent authentication failures at the point of care.
- Phase 3: Policy Enforcement Activation: Role-based access control policies, dynamic VLAN assignments, and micro-segmentation rules activated incrementally by site and device category. IoMT device profiling and certificate provisioning conducted during Phase 3.
- Phase 4: IDPS Integration and Closed-Loop Enforcement: Wireless IDPS integration with ClearPass activated upon validation of policy enforcement stability. Automated enforcement rules enabled in monitor mode prior to active enforcement to validate rule accuracy and minimize false-positive enforcement actions on clinical devices.

5.3. Authentication Architecture

Enterprise device authentication was standardized on EAP-TLS using machine certificates issued by an internal PKI. Certificate provisioning was integrated with the organization's existing Active Directory infrastructure to automate certificate lifecycle management. IoMT devices incapable of supporting 802.1X supplicants were onboarded through a MAC Authentication Bypass (MAB) workflow combined with ClearPass Profiler classification, confining unauthenticated devices to isolated network segments pending certificate provisioning.

5.4. Micro-Segmentation Policy Design

Network segmentation policy was designed around five device classification categories: (1) managed enterprise devices (clinical workstations, mobile carts), (2) managed IoMT devices (certified and profiled medical devices), (3) unmanaged IoMT devices (pending profiling or certification), (4) enterprise mobile/BYOD, and (5) guest and visitor devices. Each category was assigned a dedicated VLAN with ACL rules restricting inter-segment communication to explicitly permitted flows, enforcing least-privilege access at the network layer.

6. Evaluation Results

6.1. Evaluation Methodology

Performance evaluation was conducted by comparing operational metrics collected during a 12-month baseline period prior to ZTA deployment against metrics collected over the subsequent 12-month post-deployment period. Security incident data, enforcement event logs, helpdesk ticket volumes, and authentication success rate telemetry were collected from ClearPass operational logs, wireless controller event logs, and the security operations ticketing system. Latency measurements were derived from ClearPass CoA event timestamps correlated with controller enforcement confirmation logs.

6.2. Performance Results

Table II summarizes the key performance metrics measured across the evaluation period.

Table 2. Pre- and Post-Deployment Performance Metrics

Metric	Baseline (Pre-ZT)	Post-Implementation	Improvement
Detection-to-enforcement latency	> 5 min (manual)	< 200 ms	~98% reduction in response window
Unauthorized access incidents	Baseline index: 1.0	0.22–0.27	73–78% reduction
Manual remediation events	Baseline index: 1.0	0.15–0.40	60–85% reduction
Authentication success rate	~62%	~95%	~70% improvement

IoMT devices onboarded (agentless)	Manual / ad hoc	Automated via EAP-TLS	Standardized at enterprise scale
Network uptime (clinical systems)	Disruptions during security events	Uninterrupted during enforcement	Zero clinical downtime post-deployment

6.3. Discussion of Results

The sub-200-millisecond detection-to-enforcement latency represents a qualitative shift in threat response capability. At this latency, automated enforcement functions as a real-time network control rather than a post-incident remediation tool, effectively eliminating the exploitation window that characterizes manual response workflows. This result is attributable to the direct ClearPass-IDPS API integration, which bypasses the analyst review step entirely.

The 73–78% reduction in unauthorized access incidents reflects both the deterrent effect of continuous identity validation eliminating the trusted-interior assumption that allowed lateral movement under perimeter models and the rapid containment of anomalous sessions before they could escalate to data access or system compromise. The reduction in manual remediation burden (60–85%) produced measurable operational capacity improvements in the network operations team, reallocating analyst time toward proactive security activities.

Critically, the deployment achieved zero clinical downtime attributable to security enforcement actions. This result validated the phased deployment strategy and the monitor-mode enforcement validation approach described in Section V-B, and directly addresses the primary operational concern of healthcare IT leadership regarding ZTA adoption.

7. Comparative Analysis

Table III compares the proposed ZT-ClearPass framework against four alternative security approaches across the dimensions most relevant to healthcare wireless deployment.

Table 3. Comparative Analysis of Healthcare Wireless Security Approaches

Security Approach	IoMT Support	Enforcement Model	Healthcare Suitability
Perimeter-based (legacy)	None	Manual, post-breach	Insufficient assumes trusted interior
Endpoint-agent security	Incompatible	Device-level	Fails for resource-constrained medical devices
VLAN segmentation only	Partial	Static	No identity context; flat policies lack granularity
NAC without IDPS integration	Partial	Detection only	No automated enforcement; latency gap
Proposed ZT-ClearPass framework	Full (agentless)	Automated, real-time	Purpose-built for clinical constraints; validated at scale

The comparative analysis demonstrates that only the proposed framework satisfies all four of the critical healthcare requirements: full IoMT support through agentless mechanisms, automated real-time enforcement, clinical-grade uptime preservation, and scalability across heterogeneous multi-campus environments. Legacy perimeter-based approaches fail on all dimensions except operational familiarity. Endpoint-agent approaches are fundamentally incompatible with the IoMT device population that constitutes a primary attack surface in healthcare networks.

8. Limitations and Future Work

8.1. Limitations

Several limitations of the present work should be noted. First, the evaluation was conducted in a single organizational deployment; generalizability to healthcare systems with different infrastructure compositions, patient population sizes, or regulatory contexts requires validation. Second, performance metrics were derived from operational logs rather than controlled experimental conditions, introducing confounding factors related to organizational change management, seasonal variation in network activity, and concurrent infrastructure changes during the evaluation period.

Third, the closed-loop enforcement model carries inherent false-positive risk: automated enforcement actions triggered by IDPS misclassification could affect legitimate clinical devices. The monitor-mode validation approach described in Section V-B mitigates but does not eliminate this risk. Formal false-positive rate quantification is a subject for future work.

8.2. Future Work

Several directions for future research emerge from this work. AI-driven behavioral anomaly detection, integrated with the ClearPass enforcement framework, represents a promising extension that could improve detection accuracy and reduce false-positive enforcement events by learning device-specific behavioral baselines rather than relying on signature-based detection alone. Extension of the Zero Trust model to wired clinical infrastructure and cloud-integrated clinical application access presents an opportunity to achieve consistent ZTA coverage across the full healthcare technology stack. Integration of the proposed framework with FHIR-based clinical data access controls could further

align network-layer security with application-layer healthcare data governance requirements. Finally, simulation-based validation of the closed-loop enforcement model using network simulation tools such as NS-3 would provide a controlled experimental complement to the operational deployment metrics presented here.

9. Conclusion

This paper presented a Zero Trust Architecture framework for enterprise healthcare wireless networks, implemented through Aruba ClearPass as the centralized identity and policy enforcement plane with integrated closed-loop IDPS enforcement. The framework was validated in a production deployment across a 60+ site, 7,000+ access point healthcare enterprise, demonstrating sub-200-millisecond threat enforcement latency, 73–78% reduction in unauthorized access incidents, 60–85% reduction in manual remediation, and zero clinical downtime during enforcement operations. The results establish that network-centric Zero Trust enforcement, anchored by ClearPass-based policy orchestration, is a technically viable and operationally sustainable security model for critical healthcare wireless environments. The framework directly addresses the structural inadequacies of perimeter-based and endpoint-centric approaches in clinical settings where IoMT device constraints and uninterrupted care delivery requirements preclude conventional security models. As healthcare organizations continue expanding IoMT deployments, cloud-integrated clinical platforms, and multi-campus wireless infrastructure, the identity-centric, automated enforcement approach demonstrated here is expected to become an increasingly foundational component of healthcare cybersecurity strategy.

References

[1] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," Commun. ACM, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[2] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, Jul. 2018.

[3] IBM Security, "Cost of a Data Breach Report 2023," IBM Corp., Armonk, NY, USA, 2023.

[4] U.S. Department of Health and Human Services, "Universal Health Services Ransomware Attack Lessons Learned," HHS Office for Civil Rights, Washington, DC, USA, 2021.

[5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.

[6] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, Cambridge, MA, USA, Nov. 2010.

[7] V. Stafford, "Zero Trust Architecture," NIST Special Publication 800-207 (Draft 2), National Institute of Standards and Technology, 2019.

[8] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review," Maturitas, vol. 113, pp. 48–52, 2018.

[9] K. Fu and J. Blum, "Risks of medical device software," Commun. ACM, vol. 56, no. 10, 2013.

[10] C. S. Kruse et al., "Cybersecurity in healthcare: A systematic review of modern threats and trends," Technology and Health Care, vol. 25, no. 1, pp. 1–10, 2017.

[11] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," IETF RFC 2663, 1999.

[12] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, National Institute of Standards and Technology, 2007.

[13] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol," IETF RFC 5216, Mar. 2008.

[14] U.S. Department of Health and Human Services, "HIPAA Security Rule," 45 CFR Parts 160 and 164, 2003.

[15] Aruba Networks, "ClearPass Policy Manager 6.10 User Guide," Hewlett Packard Enterprise Development LP, 2022.

[16] Institute of Electrical and Electronics Engineers, "IEEE Std 802.1X-2020: Port-Based Network Access Control," IEEE, New York, NY, USA, 2020.

[17] Institute of Electrical and Electronics Engineers, "IEEE Std 802.11i-2004: Medium Access Control (MAC) Security Enhancements," IEEE, New York, NY, USA, 2004.

[18] D. Geer, "Health care and cyber security: Increasing threats require increased capabilities," IEEE Security & Privacy, vol. 13, no. 5, pp. 78–81, Sep.–Oct. 2015.

[19] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in Proc. 3rd IEEE Int. Conf. Electronic Design (ICED), Phuket, Thailand, 2016, pp. 321–326.

[20] W. Stallings and L. Brown, "Computer Security: Principles and Practice," 4th ed. Pearson, Hoboken, NJ, USA, 2018.

[21] Akinapalli, S. (2026). AN AI-POWERED DATA TRUST AND QUALITY SCORING FRAMEWORK FOR ENTERPRISE DECISION INTELLIGENCE SYSTEMS. *International Journal of Data Science and IoT Management System*, *5*(1), 946-950.