CASE STUDY: Enterprise SD-WAN Transformation & Zero-Trust Architecture

Organization: Cahaba Medical Care (FQHC)

Scale: 32 Multi-State Clinical Locations | 2500+ Endpoints

Architect: David Culp, Principal Solutions Architect

---

1. EXECUTIVE SUMMARY

In response to a hyper-growth phase (expanding from 7 to 32 sites), I architected a unified, resilient network infrastructure to replace a fragmented patchwork of consumer-grade DSL and cable connections. The objective was to eliminate downtime, ensure HIPAA/HITECH compliance, and create a scalable "Clinic-in-a-Box" deployment model.

---

2. THE CHALLENGE

- **Operational Risk:** Clinical sites faced frequent "dark periods" due to unreliable local ISPs, stopping patient care and EHR access.
- **Security Gaps:** Lack of centralized visibility made consistent firewall policy enforcement and threat detection impossible.
- **Scaling Bottlenecks:** Manual configuration of new sites was slow, prone to "configuration drift," and required excessive on-site engineering hours.

---

3. THE ARCHITECTURAL SOLUTION

I engineered a **Zero-Trust SD-WAN** utilizing the **Fortinet Security Fabric** and **AT&T FirstNet** as the backbone for healthcare continuity.

A. Connectivity & Resiliency

- **Primary Path:** Dedicated AT&T MPLS Fiber.
- **High-Availability Path:** Integrated FirstNet LTE/5G Cellular gateways.
- **Logic:** Implemented sub-second automated failover. During a primary fiber cut, the SD-WAN orchestrator maintains active VoIP sessions and EHR data streams without user intervention.

B. Standardized Network Segmentation (The "Clinic-in-a-Box")

To ensure security and auditability, I developed a standardized 6-VLAN logical schema deployed identically across all 32 sites:

VLAN ID	Name	Purpose	Access Control
VLAN 10	Clinical	EHR & Medical Imaging	Zero-Trust (Internal Only)
VLAN 20	Admin	Staff Workstations	RADIUS/MFA Protected
VLAN 100	Servers	Local Proxmox HA Clusters	Isolated / Mgmt Only
VLAN 172	Test	Sandbox & Dev	Air-gapped from Clinical
VLAN 192	BYOD	Guest/Patient Wi-Fi	Internet Only; No LAN Access
VLAN 200	Backup	Offsite ZFS Replication	High-Bandwidth Dedicated

C. Global IP Management (IPAM)

I implemented a hierarchical IP addressing scheme to allow for massive scale and simplified routing. By utilizing a predictable "Golden Schema" (e.g., 10.[Site_ID].x.0/24), we achieved:

- **Global Firewall Policies:** One security policy could be pushed to 32 sites simultaneously.
- **Predictable Troubleshooting:** IT staff can identify device types and locations instantly based on the IP address.

---

4. KEY TECHNOLOGIES

- **Edge Security:** FortiGate Next-Generation Firewalls (NGFW).
- **Wireless:** Ubiquiti UniFi managed access points with WPA3-Enterprise.
- **Identity:** Duo MFA integrated with FreeIPA/RADIUS for "Road Warrior" VPN access.
- **Monitoring:** Centralized "Single Pane of Glass" via FortiManager and ELK Stack for real-time threat maps.

---

5. BUSINESS OUTCOMES

- **100% Uptime:** Successfully maintained clinic operations through regional ISP outages and severe weather events.
- **Deployment Velocity:** Reduced "Time-to-Online" for new clinics from **3 weeks to 48 hours**.

- **Audit Compliance:** Passed all external security audits with zero findings related to network segmentation or unauthorized access.
- **Cost Efficiency:** Repurposed existing hardware for local "Drop Box" vulnerability scanning (OpenVAS), saving thousands in licensing fees.

---

6. TECHNICAL DOCUMENTATION INDEX

- **Network Diagram:** [Link to 32-Site MPLS Map]
- **VLAN Logic:** [Link to Remote Clinic PDF]
- **Configuration Data:** [Link to IPAM Spreadsheet]
- **Code Base:** [GitHub.com/davidculp-tech/OpenClinical-AI]