Group 5 - NetShark Innovators

Joshua Marzan & Daniel Rivera

NetShark Innovators

Miami Dade College

Introduction

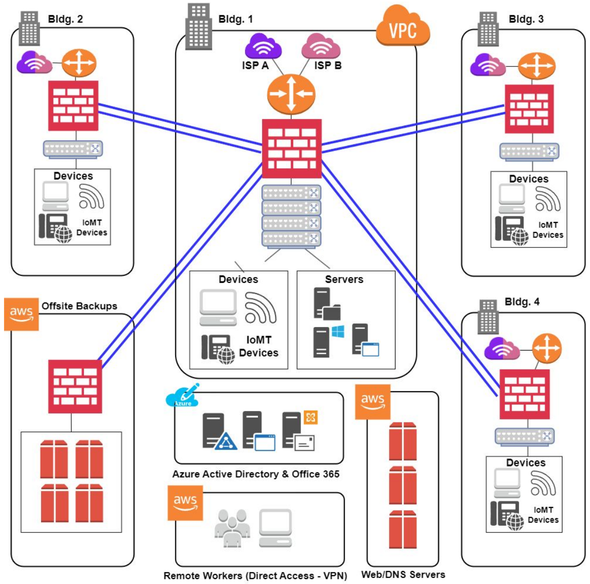
Providence Medical Center faced a recent cybersecurity setback impacting critical network operations, prompting a change in their IT infrastructure. PMC needed a new network that supports over 3,000 users and several thousand endpoints/IoMT devices.

Our solution is to develop a secure, redundant, HIPAA-compliant network to support the current IT infrastructure needed to keep operations running.

Approach

Network Segmentation: Users access resources based on dept. or VLAN.
Monitoring: Vigilantly oversee network resources and local backups of ePHI.
Scalability: Allocate additional IP addresses in case of future growth
Redundancy Boost: Integrate multiple switches, routers, and firewalls improve network redundancy.
Infrastructure Upgrade: Establish two Main Distribution Frames (MDFs) in Buildings 1 and 4, connected via CAT 6a cables to respective Intermediate Distribution Frames (IDFs) in each building.

Network Design



Project Timeline

Phase & Description	Start/End	Duration
1. Prev. Network Assessment, Design Proposal, Decommissioning	06/01/2023 - 08/23/2023	84 days
2. Network Infrastructure Upgrades	08/01/2023 - 11/13/2023	105 days
3. VLAN Implementation, Network Segmentation	09/11/2023 - 12/22/2023	103 days
4. Wireless Network Enhancement	12/04/2023 - 03/22/2024	110 days
5. Network Monitoring, Identifying Observability	01/02/2024 - 05/01/2024	121 days
6. Load Testing, DR Exercises Current Network Assessment	04/01/2024 - 07/08/2024	99 days
7. Providing Documentation, Initial Runbooks, User Training	05/08/2024 - 08/30/2024	115 days

Objectives

- HIPAA-Compliant Network Access
- High Availability/Redundant (99.999%)
- Cybersecurity Training for End Users
- Developing a Disaster Recovery Plan
- IT Inventory Management System
- Enhanced Network Architecture for long-term manageability

Security Considerations

Data Encryption: AES-256 (in transit), TLS via HTTPS for web app/ePHI access, volume encryption (at rest)

VPN Connectivity: Site-to-Site VPN tunnels from sites to the central hub (Bldg. 1). Redundancy through multiple VPN tunnels and dual ISPs per site.

Access Control: Implemented per user through logon scripts in Azure AD.

Contact Us

Lead Designer: jmarzan@netshark.com
System Engineer: drivera@netshark.com