NetShark Innovators

Network Design Update: Providence Medical Center

NetShark Innovators (Group 5)

Joshua Marzan, Daniel Rivera

Miami Dade College

Terminology Used

- **Internet of Medical Things (IoMT):** imaging devices, monitoring devices, biosensors, infusion pumps that transfer data over the network
- **Electronic Health Records (EHR):** digital version of a patient’s paper chart recorded in real time, offering instant availability to healthcare staff and users
- **Health Insurance Portability and Accountability Act (HIPAA):** national standard implemented in 1996 that protects patient health information from being disclosed without the patient’s knowledge or consent

Introduction

A recent cyber attack affected Providence Medical Centers, and a change is needed to be made.

Our goal is to implement a new network with industry standards pertaining to security, manageability, and overall reliability.

The healthcare industry is driven by:

- The evolution of information systems
- Sensitive patient data
- Research data collected onsite
- The system’s ability to protect stored data

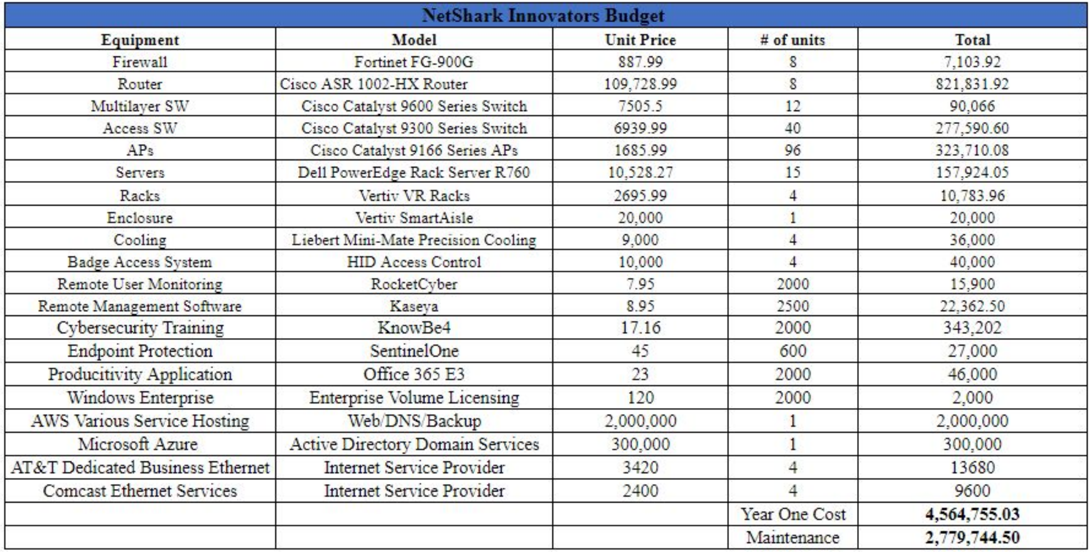
Goals

1. A more educated and aware user base less prone to cyber attacks
2. A secure, reliable, and available network that will meet the needs of medical personnel, staff, and patients.
3. Improved overall customer satisfaction with network performance

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

Budget & Timeline



NetShark Innovators Budget				
Equipment	**Model**	**Unit Price**	**# of units**	**Total**
Firewall	Fortinet FG-900G	887.99	8	7,103.92
Router	Cisco ASR 1002-HX Router	109,728.99	8	821,831.92
Multilayer SW	Cisco Catalyst 9600 Series Switch	7505.5	12	90,066
Access SW	Cisco Catalyst 9300 Series Switch	6939.99	40	277,590.60
APs	Cisco Catalyst 9166 Series APs	1685.99	96	323,710.08
Servers	Dell PowerEdge Rack Server R760	10,528.27	15	157,924.05
Racks	Vertiv VR Racks	2695.99	4	10,783.96
Enclosure	Vertiv SmartAisle	20,000	1	20,000
Cooling	Liebert Mini-Mate Precision Cooling	9,000	4	36,000
Badge Access System	HID Access Control	10,000	4	40,000
Remote User Monitoring	RocketCyber	7.95	2000	15,900
Remote Management Software	Kaseya	8.95	2500	22,362.50
Cybersecurity Training	KnowBe4	17.16	2000	343,202
Endpoint Protection	SentinelOne	45	600	27,000
Producitivity Application	Office 365 E3	23	2000	46,000
Windows Enterprise	Enterprise Volume Licensing	120	2000	2,000
AWS Various Service Hosting	Web/DNS/Backup	2,000,000	1	2,000,000
Microsoft Azure	Active Directory Domain Services	300,000	1	300,000
AT&T Dedicated Business Ethernet	Internet Service Provider	3420	4	13680
Comcast Ethernet Services	Internet Service Provider	2400	4	9600
			Year One Cost	**4,564,755.03**
			Maintenance	**2,779,744.50**

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

Technical Requirements

Scalability: user data, devices on networks, more sites

Availability: network redundancy across all major switches, diesel generators powering server room in case of outages,

Network Performance: 10Gbps bandwidth to allow for video calls, EHR search/transfer, real time image transfer (XRay/MRI), administrative work. 2nd ISP for network redundancy between sites

Security: HIPAA/ePHI framework, best practice for patching

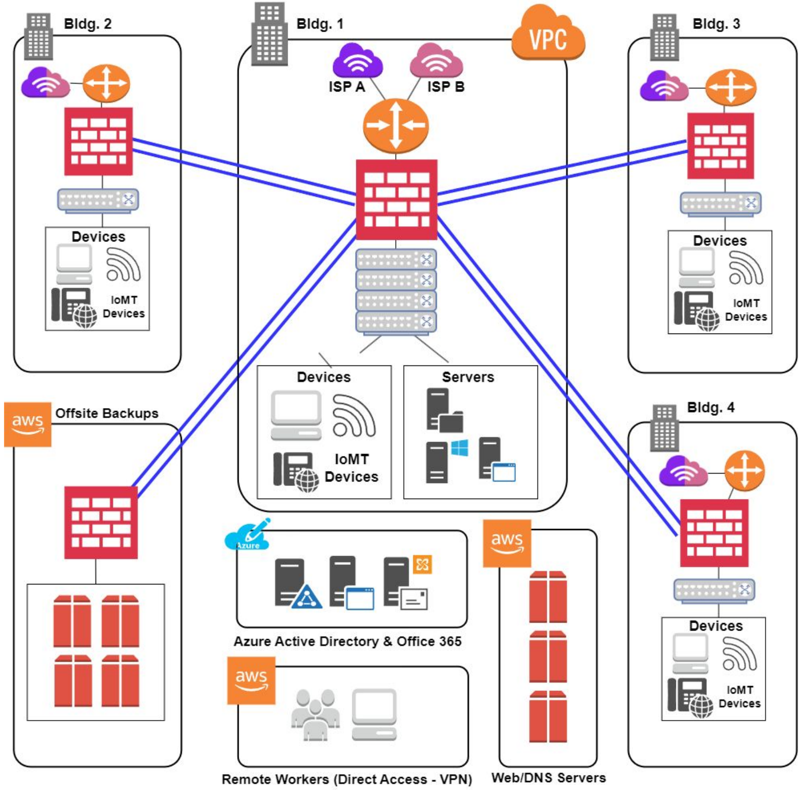
Manageability: track network changes, implementing patching schedule

Group 5 - NetShark Innovators

Joshua Marzan & Daniel Rivera

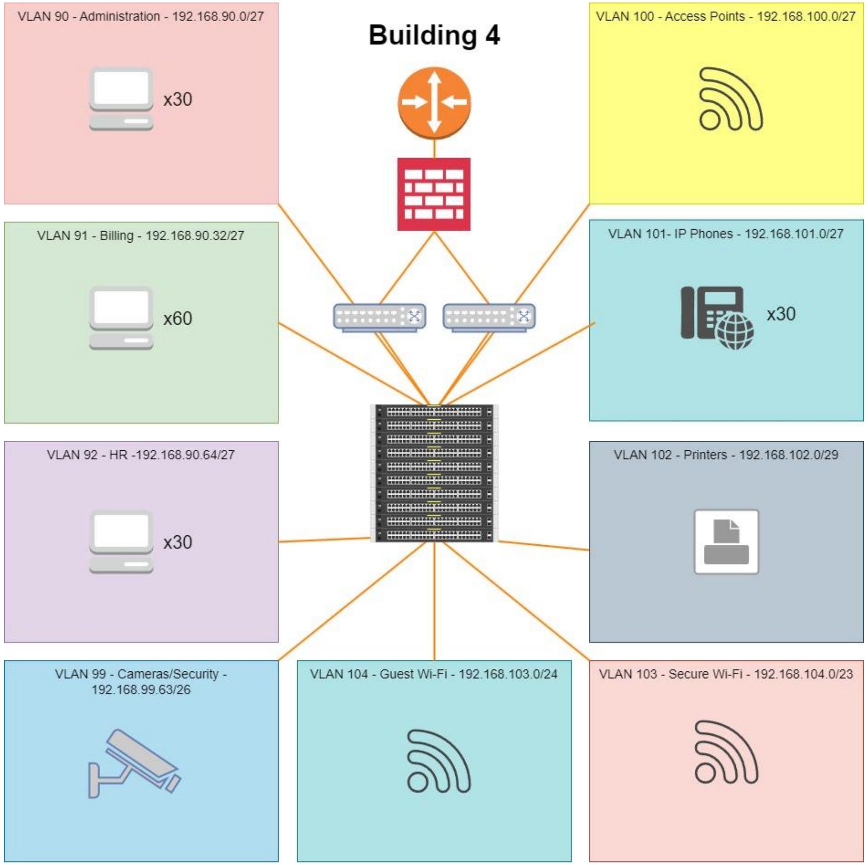
Network Design

- "Hub-and-Spoke" topology
- Site-to-Site implementation via FortiGate Firewalls (2 VPN tunnels)
- VPN used for Remote Users, Web Servers, and Offsite Backup of EHR
- Network devices compartmentalized into VLANs by device group and department



Network Design (cont.)

- Dual ISPs > Router > Firewall > Multilayer Switch > Switch Stack
- VLANs created by device group (surveillance cameras, IoMT devices) or by department (Administration, Billing, HR, etc.)
- All administered through the labeled switch stack, segmented via the switch's console


VLAN 90 - Administration - 192.168.90.0/27
x30
Building 4
VLAN 100 - Access Points - 192.168.100.0/27
VLAN 91 - Billing - 192.168.90.32/27
x60
VLAN 101- IP Phones - 192.168.101.0/27
x30
VLAN 92 - HR -192.168.90.64/27
x30
VLAN 102 - Printers - 192.168.102.0/29
VLAN 99 - Cameras/Security - 192.168.99.63/26
VLAN 104 - Guest Wi-Fi - 192.168.103.0/24
VLAN 103 - Secure Wi-Fi - 192.168.104.0/23

Security Measures

- Two FortiGate 900G firewalls (active/passive) implemented in Building 1
- Data encryption at rest (Volume Encryption), in transit (AES-256), web-application access (TLS through HTTPS), and with remote access (VPN tunnel)
- Strict access control for resources based on user title and department
- Staff training (KnowBe4, HIPAA compliance)
- 3rd party cybersecurity services
  - RocketCyber monitoring
  - Mimecast email protection
  - SentinelOne endpoint protection
  - ManageEngine Endpoint Central RMM