INTERCOM PROGRAMMING AND MANUFACTURING COMPANY

(IPMC)

SCHOOL OF CYBERSECURITY | EC-COUNCIL

IPMC

C|CT 2023/2024 ACADEMIC YEAR

COURSE TITLE: **CERTIFIED CYBERSECURITY TECHNICIAN (C|CT)**

COURSE CODE: **212-82**

PROGRAMME: **DIPLOMA IN CYBERSECURITY**

STUDENT NAME: **SARPONG AMOH ALEXANDER**

STUDENT ID:

DATE: **MONDAY, 13TH JAN 2025**

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This project provides Cyber Security Threat Detection, Monitoring and Protection of system in a Nursing Home for old People in my area. This system will establish a well-structured networking tool, cyber security tools and mechanisms to detect, monitor, prevent and protect the Nursing Home from information systems related threats, and creates an internal mechanism to handle all potential cyber related issues in the future.

The current trends in cyber security attacks in industries, and the harm caused have made many organizations to go insolvent, hence the need to implement a strong cyber security threat detection and protection systems in the Nursing Home for old people.

In reference to that, some critical points should be taken into consideration.

- The network should be simple to use, modify and troubleshoot should be adopted.
- A well-planned network should be designed to facilitate the needs and tasks of the Nursing Home for old people.
- High standards quality hardware products should be used in respective of cost due to the nature of the business.
- The network should be governed by policies to maintain its productivity, security, and efficiency.
- In case of data lost, uncontrollable disasters, and hardware failure, a disaster recovery plan should be implemented in order to prepare for such occurrences.

Through the implementation of these adjustments and modifications, the Nursing Home will improve the working environment for its staff, clients, and better secure its information and database, resulting in a more productive and smooth flow of data, increasing the company's efficiency. The Nursing Home will experience almost no point of failure with a well-structured secured network design.

Numerous backup plans have been put in place to maintain a 99.9% uptime protection against a wide range of unpredictable events that might arise on a daily basis and compliance with government policies and requirements for wireless networks. As the Nursing Home begins to grow and expand, it will also be incredibly easy to modify and adapt this well-planned network. This project also talks about the physical layout and logical topologies for the Nursing Home facility for whom we are designing the network. The project proposes a network architecture that performs very well, highly available network without any downtime or failure, adaptable, expandable due to new services emerging, secured and manageable.

2. SCOPE

The project aims to create a well secured data transmission link with a functional network system connecting all departments in the nursing home building with ability to failover. This project's initiation is to give networking and security capabilities for IP-based medical devices, personnel, guests, and nursing home employees. The following are some objectives that shed light on the subject matter:

- Uninterrupted access to high-speed internet.
- Provide improved medical facilities to the old people.
- Organized health records for future reference.
- Continuous communication throughout the nursing home's departments that is network capability for end-to-end connectivity.
- A network that demonstrates a secure network for protecting medical information and staff research projects.
- Providing wireless limited internet access for the staff and visitors of the nursing home.

The project primarily focuses on three (3) functional areas, or system levels.

2.1 Core Layer

This Layer serves as the system's base and it includes cable types such as fiber cables as well as quick connections and core switch. In core layer, packets are neither manipulated nor does it route traffic at LAN level. Fast and reliable data transfer throughout a network is mostly the responsibility of the core layer. This layer's primary goal is to send packets with less delay.

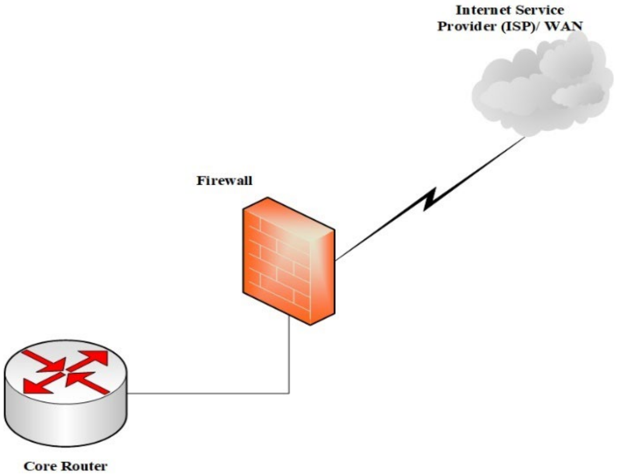


Diagram 1

2.2 Distribution Layer

The Distribution Layer is responsible for directing packets. Furthermore, it provides protocol-based network connectivity. This layer is where network-transmission control, including what enters and exits the network, is first applied. This layer includes the core switch, data center switch, and other departmental switches. This layer ensures that the packets are legitimately directed amid Virtual Local Area Networks (VLANs) and subnets. This layer is often referred to as the work-group layer.

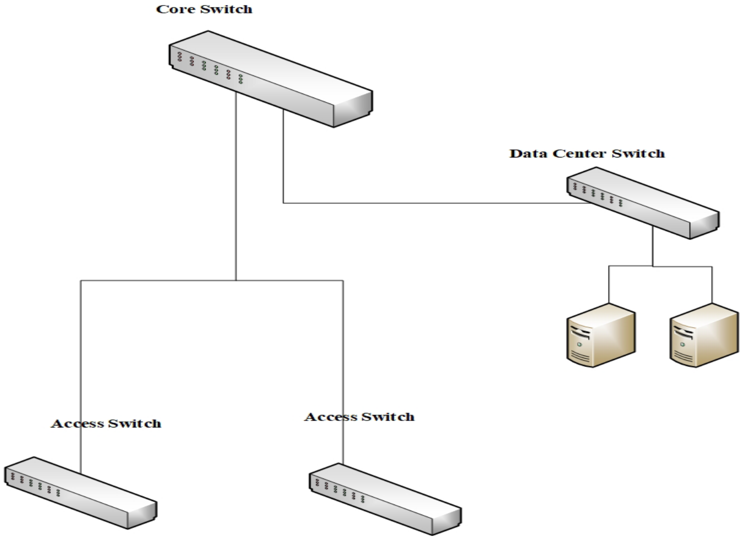


Diagram 2

2.3 Access Layer

The Access Layer contains gadgets that permit work-groups and clients to utilize the role played by the core and distribution layers. Network areas can be expanded or contracted in the access layers by using a standard switch, or repeater. Its primary function is to link end users' devices like computers to the network, this layer is also known as the work area or desktop layer. This layer ensures that data bundles reach the computers of the end users.

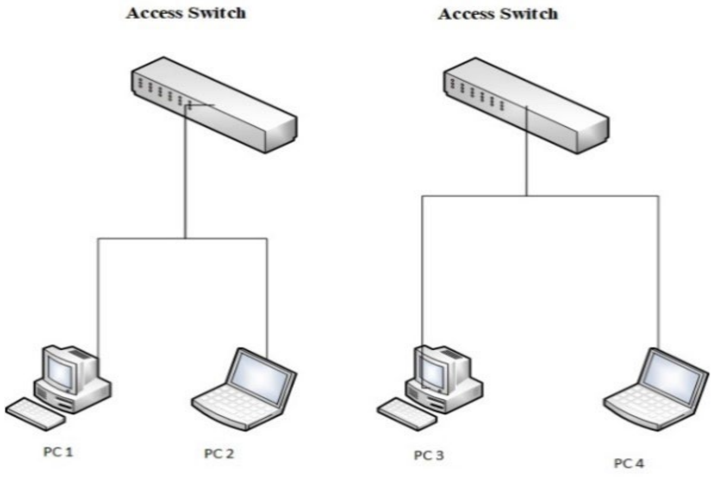


Diagram 3

3. NETWORK REQUIREMENTS

In the Nursing Home for old people, we have desktop computers, laptops, smart devices like phones, tablets and phablets. Some network requirements include Internet Service Providers (ISP), Servers, Firewall, router, switches (Core switch, Data Center switch and access switches), Wireless Access Point (WAP), Disaster Recovery devices and cables. The network will be divided into segments, which is the Data Center (Server room), entrance reception, Managers Office, private meeting room, staff lounge, staff office, Dining room, Accounts Office.

3.1 Internet Service Provider (ISP)

We require a high-speed internet service provider for a project of this size, with over one hundred (100) end users accessing the internet simultaneously. We cannot compromise on internet speed as people lives are at stack. We choose a connection of one Gigabits per second (1Gbs) bandwidth from a reliable ISP.

The reasons include;

- Multiple nursing home staff accessing and using their workstations simultaneously.
- Providing fixed bandwidth for guests and visitors as they might stream videos or access websites while waiting in the waiting area/visitor's area.
- Provide high-speed internet access to the various departments of the nursing home to enable continuous, high-quality video communication.
- Taking future expandability into account.

3.2 Servers

It is the only brain and computing processing device that controls the information flow within a corporate network, making it a crucial component. It is a central system used for storing and managing data of the entire network. It is vital for the Nursing Home to use top-tier servers from a reliable manufacturer with good warranty that can support hardware and medical equipment at any point in time.

Therefore, Dell brand servers is recommended to support the nursing home new network based on their services and high standard products to other manufacturers like IBM and others. The best-chosen model is Dell PowerEdge Server Tower Model T560 (other model includes PowerEdge T150, T350 and T550) based on its ability to handle large amounts of data and complex calculations in conditions of limited rack space, also its efficiency infrastructure, quick task completion, and high reviews. The nursing home will need five (5) servers, four (4) primary servers for E-mail services, Web services, File Server and Active Directory Domain Services (AD DS) or Data-base services and a backup server responsible for reserving or backing up important data, files, folders to prevent loss of data in the situation of hard drive failure, disaster or technical failure. The servers should have identical hardware specifications and will run on Windows Server 2022 operating system for easy workstation, device calibration, security and compliance, improve performance, speed and efficiency, enhanced resource management and optimization tools and its support for remote services. On the other hand, Dell PowerEdge Server Tower Model T560 has a high-power consumption, which may lead to higher energy expenses and production of heat and may not support all operating systems.

Table 1 Server Specification (T560)

<table>
<tr><th>Feature</th><th colspan="2">Technical Specification</th></tr>
<tr><td><b>Processor</b></td><td colspan="2">Up to two 5th Generation Intel® Xeon Scalable processor, with up to 32 cores per processor or
Up to two 4th Generation Intel® Xeon Scalable processor, with up to 32 cores per processor</td></tr>
<tr><td><b>Memory</b></td><td colspan="2">16 DDR5 DIMM slots, supports RDIMM 1 TB max
Speeds up to 4800 MT/s on the 4th Generation Intel® Xeon Scalable processor
Speeds up to 5200 MT/s on the 5th Generation Intel® Xeon Scalable processor
Supports registered ECC DDR5 DIMMs only</td></tr>
<tr><td><b>Driver Bay/ Disk Bay, Internal Storage</b></td><td colspan="2">Up to 24 x 2.5-inch SAS/SATA HDD drives
Max 360 TB</td></tr>
<tr><td><b>Form Factor</b></td><td colspan="2">4.5U tower server</td></tr>
<tr><td><b>Power Supply</b></td><td colspan="2">600 W – 2400 W Platinum 100-240 VAC/240 VDC
700 W – 2800 W Titanium 200-240 VAC/240 VDC
1100 W DC/-48-(-60) V
1400 W Titanium 277 VAC/336 VDC</td></tr>
<tr><td><b>Cooling Options and Fans</b></td><td colspan="2">Air Cooling
Up to Eight (8) Standard (STD) fans or High performance (HPR) fans</td></tr>
<tr><td><b>GPU Options</b></td><td colspan="2">Up to 2 x 300 W DW or 6 x 75 W SW</td></tr>
<tr><td><b>Ports</b></td><td>Front Ports
1 x USB 2.0
1 x USB 3.0
1 x iDRAC Direct (Micro-AB USB) port

Internal Ports
1 x USB 3.0 (optional)</td><td>Rear Ports
1 x USB 2.0
1 x USB 3.0
1 x Serial port (optional)
1 x Dedicated iDRAC (RJ45) port
1 x VGA port
2 x Ethernet ports</td></tr>
<tr><td><b>Expansion Slots (PCIe)</b></td><td colspan="2">Up to six PCIe slots:
Slot 1: x16 Gen5 Full height, Full length
Slot 2: x16 Gen5 Full height, Full length
Slot 3: x16 Gen4 Full height, Half length
Slot 4: x16 Gen4 Full height, Half length
Slot 5: x16 (x8 lanes) Gen4 Full height, Half length
Slot 6: x16 Gen4 Full height, Half length</td></tr>
</table>

Operating Systems supported and Hypervisors	Canonical Ubuntu Server LTS Microsoft Windows Server with Hyper-V Red Hat Enterprise Linux SUSE Linux Enterprise Server VMware ESXi
Storage Controllers and RAID Supported	Internal PERC: fPERC H965i, fPERC H755N, fPERC H755, fPERC H355, fPERC HBA355i, HBA465i fPERC Internal Boot: Boot Optimized Storage Subsystem (BOSS-N1): HWRAID 2 x M.2 NVMe SSD drives, or USB External HBA (non-RAID): PERC HBA355e Software RAID: S160 (for NVMe drives only)
Embedded NIC and Network Options	2 x 1GbE LOM on Planar 1 x OCP x8 card 3.0 Note: The system allows both LOM on planar and OCP card to be installed on the system.
Warranty	1 – 3 years

3.3 Router

In our network, we have a core router at the core layer. We need to handle the bandwidth of 1Gbs temporarily. The core router should be of the best features and technical specifications. To handle this bandwidth, we are choosing Cisco 8818 Route Processor because of its, inbuilt firewall feature, encryption, and Intrusion detection service (IDS) and can accommodate an upgraded bandwidth of 518 Tbps. Its networking infrastructure is superior that integrates all network devices and operating standards together. However, it involves an intricate setup and configuration, which can take a lot of effort and specialized knowledge, also it may have limited support options, which might take troubleshooting and problem-solving challenging.

Table 2 Router Specification

Feature	**Technical Specification**
Processors	2 route processors, Intel 8-core @ 2.7 GHz
System Memory	64GB DRAM
Bandwidth	259.2 Tbps/518 Tbps
Ports/Timing	48 QSFP28 100 GbE with MACSec 36 QSFP56-DD 400 GbE Class C, SyncE, 1588 TOD, 1PPS, 10MHz, GNSS
Power Supply	18 high-voltage power supplies or 24 48V DC power supplies
Management Ports	1 (RJ45)+2 SFP+ (1/10G)
SSD Storage	256GB
USB Ports	1 – USB 2.0, 1 – USB 3.0
Slots	18 slots system
Warranty	1 -3 years

3.4 Firewall

Is a network security system configured to prevent unauthorized access to or from a private network. A firewall typically establishes a barrier between a trusted network (private network) and an untrusted network (public network), such as the Internet. Firewall prevents unauthorized users from accessing private network connected to the internet, specifically intranet. Every packet entering or departing the network must go through the firewall. It monitors, controls and verifies each data packet and prevents access should it fails to meet security requirements configured by the network administrator. Firewall can be implemented at the hardware-based and software-based level. Packet filtering firewall and web application firewall is recommended for the nursing home. Packet filtering firewall will examine and manage the data packets as well streamline the network traffic flow while the web application firewall will allow specific web applications to be used by the staffs of the nursing home. The Cisco 8818 router is also capable of filtering the data packets and restricts web applications according to the protocols configured by the network administrator. The hardware firewall recommended for the nursing home is Netgate 1541 1U Base pfSense Security Gateway. The reason for choosing this particular hardware firewall is due to:

- Its high performance and reliability
- Its security features that is AES-NI encryption acceleration, Intrusion Detection and Prevention (IDP), VPN support (OpenVPN, IPsec, PPTP).
- It manageable and ease to use that is user friendly interface.
- Its scalability and future-proofing that is its upgradeable hardware components, expandable storage and networking options, and support for emerging technologies (IoT).
- It has a large pf sense community and its compliance with major regulatory requirements (e.g., HIPAA, PCI-DSS)

Nevertheless, it may be incompatible with some peripherals or hardware components which may have interoperability issues with devices or systems that do not use pfSense.

Table 3 Firewall Specification

Feature	**Technical Specification**
CPU	Intel "Xeon-DE" D-1541, 2.1 GHz FCBGA 1667 supported SoC
CPU Cores	Eight Cores, 45W
Networking	Dual LAN via Intel® i350-AM2 1 Gigabit Ethernet Dual LAN via SoC 10GBase-T Virtual Machine Device Queues reduce I/O overhead Supports 10GBASE-T, 100BASE-TX, and 1000BASE-T, RJ45 output 1x Realtek RTL8201N PHY (dedicated IPMI)
Storage	500 GB M.2 SSD
Memory	16 GB ECC DDR4 RDIMM (expandable to 32 GB)
Expansion	1x PCI-E 3.0 x 16 slot 1x M.2 PCI-E 3.0 x4 (SATA support) M Key 2242/2280 6x SATA3 (6 Gbps) ports via SoC
Other Ports	1x BMC integrated ASPEED AST2400 1x IPMI Port 1x VGA Port 1x Fast UART 16550 Serial Port (header)
USB Ports	2x USB 3.0 ports
Power Consumption	20 W (idle)
Warranty	Standard 1-year hardware warranty Optional extended warranty and support packages

3.5 Core Switch

Core switch comes in the distribution layer. It is also referred to as Backbone Switch or Tandem Switch. The principal purpose of the core switch in a network is to increase the speed of delivery data packets in the center of the network. A core switch is positioned at the top of a network's structure. It handles bigger and more data, and offers improved dependability compared to other switches. The core switch acts as the main artery of a network.

In the network design, a managed switch is advised for each switch-using layer. The reason being that it allows for configuration customization, supports spanning Tree Protocol, Virtual Local Area Networks (VLANs), bandwidth rate limitation, port mirroring, Simple Network Management Protocol (SNMP), and is designed for scalable network systems. Cisco Catalyst 9600 Series Switch is recommended. The reason being that,

- It has very less rate of failure.
- It has very high scalability.
- It is ungradable.

Notwithstanding, it may lack some of the security features and capabilities found in other switches available on the market, also the Cisco IOS operating system may have vulnerabilities that can be exploited by attackers.

Table 4 Core Switch Specification

Feature	Technical Specification
Software Requirement	Cisco IOS XE Software Release 16.11.1 and above
Ports and Line cards supported	48-port RJ45 Copper - 10GE/5GE/2.5GE/1GE/100Mbps/10Mbps
Rack Units (RU)	8
Total number of slots	6
Line Card slots	4
Supervisor Engine slots	2
Supervisor Engines Supported	C9600-SUP-1, C9600X-SUP-2
Maximum bandwidth scalability per Line Card slot	6.4 Tbps (3.2Tbps full-duplex) with C9600X-SUP-2 2.4 Tbps (1.2Tbps full-duplex) with C9600-SUP-1
Supervisor Engine Redundancy Dedicated Supervisor Engine slot numbers	Yes 3 and 4
Input Voltage	AC: 90V to 264V, 47 to 63 Hz DC: -40V to -72V
Operating Temperature	-5° to 45° C (23° to 113° F) up to 6000 feet (1828.8 meter) -5° to 40° C (23° to 104° F) up to 10,000 feet (3048 meter)
Warranty	Cisco warranty support is limited to 5 years from the announcement of discontinuance.

3.6 Data Center Switch

As data center networking infrastructure becomes more disaggregated, a new class of switches called data center switches is emerging. Data center class switches are made to support data and storage for applications that are vital to the organization, in contrast to standard three-tier hierarchical networks. It swiftly manages massive volumes of data traffic, guaranteeing speedy data response and transfer while enhancing the system's overall effectiveness and performance. For this reason, I suggest the Cisco Nexus 9800 Series Data Center Switch.

- It supports higher-power optics and higher-capacity Application-Specific Integrated Circuits (ASICs) allowing the chassis to support port speeds exceeding 400G in the future.
- It supports a fully shared buffer-memory architecture that allows the switch to absorb bursts up to the available shared memory size. It also supports hybrid High Bandwidth Memory (HBM), which dynamically handles even larger flows that

could cause temporary congestion using Storage Area Network (SAN) and LAN ethernet protocols.

- They have high fault-tolerance rate, therefore, improving uptime for mission-critical applications.
- They have the capacity to manage traffic flows from all directions.
- It enhances power efficiency by minimizing the number of power conversions within the chassis.

The switch might not be scalable enough to accommodate complicated or very big data centers.

Table 5 **Data Center Switch Specification**

Feature	**Technical Specification**
Bandwidth	14.4Tbps
Performance	9.374 Bpps
Packet Buffer	324MB + 24GB
Number of Power-supply Trays	3
Total number of ports	36
MACsec	Yes (all ports)
Number of Supervisor slots	2
Number of line-card slots	8

3.7 Access Switches

It appears at the Access layer of a network. It brings the distribution network inside the building. It is the most widely used gigabit Ethernet switch which communicates directly with the public internet. These switches establish connection with end devices like computers, laptops and other medical devices with wired medium. In our network infrastructure, two (2) access switches will be used for the nursing home to connect networking devices. Cisco Catalyst 4503 E-Series Switch is recommended due to its,

- Number of ports (Maximum of 48 ports)
- High performance
- Great efficiency

It's possible that the Cisco Catalyst 4503 E-Series Switch is approaching end-of-life (EOL), which might affect its maintenance and support choices.

Table 6 Access Switch Specifications

Feature	Technical Specification
Total number of slots	3
Line card slots	2
Supervisor engine slots numbers	1
Supervisor Engines Supported	Supervisor II-Plus Supervisor II-Plus-TS Supervisor II-Plus10GE Supervisor IV Supervisor V Supervisor V-10GE Supervisor 6-E
Bandwidth Per Line Card Slot using Supervisor 6-E	Up top 24 Gbps on all slots4
Number of Power Supply Bays	2
Minimum Number of Power Supplies	1
Switched 10/100 Fast Ethernet (RJ-45)	48
Power Supplies Supported	● 1000W AC ● 1400W AC ● 1300W ACV ● 2800W ACV ● 4200W ACV 1400W DC (triple input) 1400W-DC-P External AC Power Shelf

3.8 Wireless Access Point (WAP)

Wireless Access Point are basically networking hardware device which allow wireless devices to connect to a network with either the help of wireless fidelity (WIFI) or Bluetooth medium. Two (2) WAP will be installed at each floor to provide maximum internet connectivity to staff, clients, wireless medical devices, smart phones, smart mobile tablets, laptops and other internet of thing's devices. Cisco Catalyst Wireless 9163E Access Point will best suit.

- It caters for a wide range and more spectrum of use.
- It helps ensure uninterrupted wireless access in even the most challenging outdoor environments.
- It provides the flexibility to expand your 6-GHz wireless coverage according to your specific needs.
- It allows room for expansion, multiple device connectivity with ease, and simple troubleshooting.

The access point's range and coverage may be limited, requiring more devices to be deployed to achieve desired coverage, compared to newer Wi-Fi 6E access points, the 9163E may have lower data transfer rates.

Table 7 WAP Specifications

Software	Cisco IOS® XE Software Release 17.12.3 or later
Supported Wireless LAN Controllers	Cisco Catalyst 9800 Series Wireless Controllers (physical or virtual)
System Memory	2048 MB DRAM 1024 MB flash
Security	WPA2-Personal (802.11i) WPA2-Enterprise with 802.1X WPA3-Personal, WPA3-Enterprise WPA3-Enhanced Open (OWE) Advanced Encryption Standard (AES)
Available Transmit Power Settings	802.3at Power over Ethernet Plus (PoE+), 802.3af Power over Ethernet (PoE) 2.4 GHz • 23 dBm (200 mW) • -4 dBm (0.39 mW) 5 GHz • 23 dBm (200 mW) • -4 dBm (0.39 mW) 6 GHz • 23 dBm (200 mW) • -4 dBm (0.39 mW) **Note:** In countries where use of the 6-GHz band is not allowed or there is no current software support, the 6-GHz radio will be disabled. The radio may be enabled with future software, once the product is certified to operate at 6 GHz for that country.
Extensible Authentication Protocol (EAP) types	EAP-Transport Layer Security (TLS) • EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol (MSCHAP) v2 • Protected EAP (PEAP) v0 or EAP-MSCHAP v2 • EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) • PEAP v1 or EAP-Generic Token Card (GTC) • EAP-Subscriber Identity Module (SIM)
Warranty	Limited 1-year hardware warranty (WARR-CW-1YR-LTD)

3.9 Cables

One of the crucial parts of the network infrastructure is cabling the entire network to connect network devices. It is pretty much unless without connecting one component of a network to the other, consequently I recommend CAT 6 graded Shielded Twisted Pair (STP) cables to connect network to router, router to switch, switch to server, switch to end devices. I recommend STP cables because of its capabilities to cancel interferences. Having shielded cabling will cut out interference of all other radio frequencies and disturbances throughout the nursing home environment. STP cables reduce electromagnetic and radio frequency interference, as well also protect against cross-talk. Specifically, I recommended CAT 6 grade cables, because of its maximum transmission speed of 1000mbps/100 meters. Additionally, the network requires over 5,500 feet total cable that will permit little to no interference, and need to have the durability to withstand the test of time of data flow and ever-changing environmental conditions.

CAT 6 cables may not support high-speed protocols like 10GbE or 40GbE. It can be more difficult to install due to their thicker gauge and tighter bend radius requirements.

3.10 Workstations

The Nursing Home has the need for workstations for the various wired connections and users. I decided to choose Hewlett-Packard (HP) workstations for the network environment based on its Intel vPro technology for remote management, manageability integration kit for easy deployment, sure start for secure boot protection, BIOSphere for firmware protection, also due to its reliability and superior tech support. The model I have decided to go with is the HP Envy x360.

Some users may find pre-installed software (bloatware) that can slow down the laptop. HP's customer support may not be as comprehensive or responsive as some other manufacturers.

Table 8 Workstation Specifications

Feature	Technical Specification
Processor, Graphics & Memory	Intel® Core™ Ultra 7 155U (up to 4.8 GHz, 12 MB L3 cache, 12 cores, 14 threads) + Intel® Graphics + 32 GB(Onboard)
Operating System	Windows 10 or Windows 11 Pro/Home
Storage	512 GB PCIe® NVMe™ TLC M.2 SSD (4x4 SSD) 1 TB PCIe® NVMe™ M.2 SSD 1 TB PCIe® NVMe™ M.2 SSD (4x4 SSD)
Wireless Technology	Intel® Wi-Fi 7 BE200 (2x2) and Bluetooth® 5.4 wireless card
Battery	4-cell, 55 Wh Li-ion polymer Supports battery fast charge: approximately 50% in 30 minutes
External I/O Ports	2 Thunderbolt™ 4 with USB Type-C® 40Gbps signaling rate (USB Power Delivery, DisplayPort™ 2.1, HP Sleep and Charge); 1 USB Type-A 10Gbps signaling rate (HP Sleep and Charge); 1 USB Type-A 10Gbps signaling rate; 1 HDMI 2.1; 1 headphone/microphone combo
Warranty	1-year limited hardware warranty support

Another important workstation for the nursing home staffs are tablets. These tablet devices will be used to show medication requirements, doses and the recording of patients taking their medication. I recommend Samsung Galaxy Tab S10 Ultra due to its timely security patches and feature enhancements, global service centers and online resources ensure prompt support. The Galaxy Tab S10 Ultra does not support fast charging, which can make it take longer to recharge the battery and the storage and RAM are not easily upgradable, which may limit its future-proofing.

Table 9 Specifications

Feature	Technical Specification
Operating System	Android 14, One UI 6.1
CPU	Octa-core (1x3.4 GHz Cortex-X4 & 3x2.8 GHz Cortex-X4 & 4x2.0 GHz Cortex-A720)
Memory	256GB 12GB RAM, 512GB 12GB RAM, 1TB 16GB RAM, microSDXC (dedicated slot)
WAN Bluetooth USB	Wi-Fi 802.11 a/b/g/n/ac/6e/7, tri-band, Wi-Fi Direct 5.3, A2DP, LE USB Type-C 3.2, magnetic connector
Body	Glass front, aluminum frame, aluminum back
Battery	Up to 16 hours

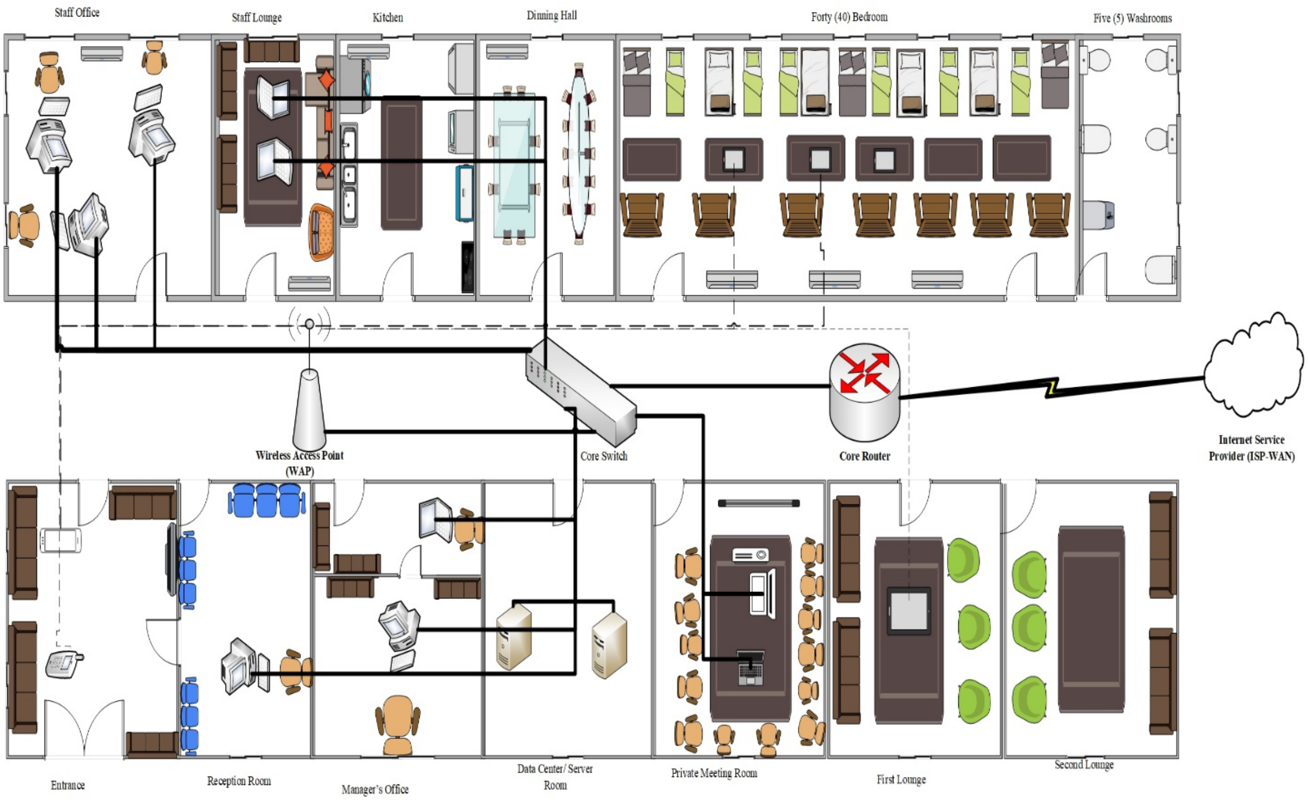
3.11 Disaster Recovery Devices

The final hardware device the nursing home should be concern and consider purchasing for the network infrastructure is disaster recovery devices. All the workstations, servers and important devices within the network infrastructure will need a backup battery to support the systems for a short period of time in case of events like power flicker or outages. The CyberPower Cp600LCD 340W backup utilities will best be suitable due to its long battery life. Similarly, considering the situation of power failure which could be a life-threatening condition, I suggest the purchase of a backup generator capable of powering the nursing home facility for a long time. It allows a large window of time for fixing of power. Elite 100 kW Generator by Guardian is a reliable, quick, efficient, and well supported electrical product that will keep the nursing home facility fully functional during power crisis.

The Cp600LCD can generate a significant amount of noise, particularly during high-load conditions. It can also generate a significant amount of heat, particularly during high-load conditions, which can reduce its lifespan.

The Elite 100 kW generator can pose an electrical shock hazard if not installed or maintained properly and also requires regular maintenance to ensure optimal performance which is costly.

4. EXISTING NETWORK TOPOLOGY DIAGRAM



The nursing home is a one storey building with an entrance, reception room, managers office, data center (Server room), private meeting room, first lounge, second lounge and a kitchen at the first floor. The second floor has the staff office with three (3) staffs, staff lounge, dining hall, forty bedrooms and five walk-in washrooms. The wired users are made up of the reception, manager's office, data center, private meeting room, staff office, staff lounge.

Currently, the nursing home facilities do not meet the requirement of a modern network standards. Due to the tremendous risk involved with the nursing home needs for connectivity and maintenance. The current network that the nursing home has implemented will cut off and completely renovated. The project prepares a new layout of logical and physical topologies that will fulfill the nursing home needs of 99.9% connection uptime, full scale office range, security, and back-up capability.

The network starts off with two servers that will be located within the data center. Both servers will run at all times, one as primary server and the other as a backup. The second server which acts as a backup will thoroughly copy everything within the network. The second server will also be available to kick in and take over should the first server ever fails for any reason.

With this network setup, the nursing home will have a star topology with easy failure justification, troubleshooting, and efficiency.

5. SECURITY ISSUES IN EXISTING NETWORK INFRASTRUCTURE

5.1 Absence of a firewall

The existing network infrastructure has no firewall which poses serious security issues in the network architecture. Without a firewall, inbound and outbound traffics is allowed in the network design making it vulnerable to unrestricted access to data. Furthermore, the network may be exposed to external attackers for potential exploitation.

5.2 No Information Technology (IT) Department

The existing infrastructure does not have any IT Department for monitoring and logging of the network. There should be an IT department that should monitor open ports that can be exploited.

5.3 Lack of Segmentation and VLAN Technology

VLANs are technologies in network infrastructure that are used to segments and improve networked organization, enhances security by isolating devices, reduce broadcast traffic and improve network performance.

5.4 No Managed Access Switches

The existing architecture uses only one switch which is the core switch. This might significantly impact the network performance and functionality. It can reduce connectivity; limit scalability that is restrict network growth due to lack of ports.

5.5 Insufficient Servers

Servers are crucial in network architecture, but the current infrastructure uses only one server, which is vulnerable to crashes, reduced processing power, and poor responsiveness.

5.6 Data Security (Insufficient Encryption)

Insufficient encryption poses a serious security risk, affecting data confidentiality and integrity. Insufficient encryption significantly compromises data security and can have far-reaching consequences. Organizations must prioritize implementing robust encryption measures to protect sensitive data, maintain compliance, and safeguard their reputation.

5.7 Poor Physical Security

In the existing infrastructure there is no surveillance and monitoring in sensitive areas like the server room, data center and the whole nursing home.

5.8 Insufficient Wireless Access Point (WAP)

Inadequate Wireless Access Points (WAPs) can negatively impact network performance and user experience. Some effects of inadequate WAP includes poor coverage and weak signal strength as well as dropped connections, reduced network capacity and bandwidth, slow data transfer rates, increased latency and lag, difficulty supporting multiple devices, security risks due to unsecured connections.

6. SECURITY ISSUES WITH MITIGATION PLAN

Addressing these security issues requires a systematic approach, including regular audits, employee training, implementation of security best practices, and a robust incident response plan. Each identified issue should be prioritized based on risk and potential impact on the organization.

6.1 Presence of Firewall

Firewall plays an important role in a network architecture for network security. The new proposed network topology will include a hardware firewall or an inbuilt firewall of the core router (Cisco 8818 Route Processor) which will block unauthorized incoming and outgoing traffic, detect and block malware, viruses, and other malicious activities, safeguard sensitive data from unauthorized access. In the new proposed network topology, there will be regularly update of firewall software and firmware, monitoring of firewall logs for security incidents, and conducting of regular security audits. The Firewall will be configured to allow only necessary traffic and will implement policies for employees and guests.

6.2 IT Department

In the new network topology proposal, there will be an IT Department for supporting and enabling an organizations operations, strategy and growth. The IT department will be responsible for designing, implementing, maintaining the network architecture and computer systems as well as peripherals, ensuring data integrity, security and availability, testing and maintaining software applications, protecting the nursing home data (medical records of old people) and systems from cyber threat, managing IT services including incident responses, managing user accounts, permissions, and access.

6.3 Introduction of Segmentation and VLAN Technology

Network segmentation and VLANs are essential components in modern network design enhancing security, scalability, and manageability. In the new proposed topology, the network will be segmented physically, logically that is the use of VLANs and subnets according to Departments and locations in the building as well as functions (whether being a staff of guests). It limits attack surfaces and reduces lateral movement, reduces broadcast traffic and improves network efficiency, simplifies network expansion and management. It isolates sensitive data from other network segments.

5.4 Managed Access Switches

Access Switches are important in a network architecture for linking devices such as computers, printers and other IP devices to a network, segmenting traffic into smaller, more manageable VLANs, supply power to devices (Power over Ethernet) that is eliminating the need for separate power sources, enhance security by implementing security feature like port-based access control, MAC address filtering and 802.1X authentication, and also optimizes network performance through features like quality of service (QoS). The new proposed network topology will include two managed access switches.

5.5 Additional Servers

In the new proposed network, five servers were recommended to be used as compared to existing network infrastructure which has only two servers. The recommended multiple servers will isolate sensitive data or applications on separate servers to enhance security, reduce individual server load by distributing workload across multiple servers, enable testing, development, and staging environments, facilitate faster recovery in case of data loss or disaster and ensure continuous operations should even one server fails.

5.6 Data Security (Insufficient Encryption)

Data security is very importance in an active network for protection of digital data from unauthorized access, use, disclosure, disruption, modification, or destruction from malware, phishing, insider threat, ransomware and others. The nursing home needs more encryption of data both in transit and at rest, security audits and usage of secured protocols like HTTPS, SSH and others. Role-based access control (RBAC) will be implemented to limit access to sensitive data to authorized personnel only. Sensitive data at rest and in transit will be encrypted using advanced encryption protocols like Advanced Encryption Standard (AES) and others.

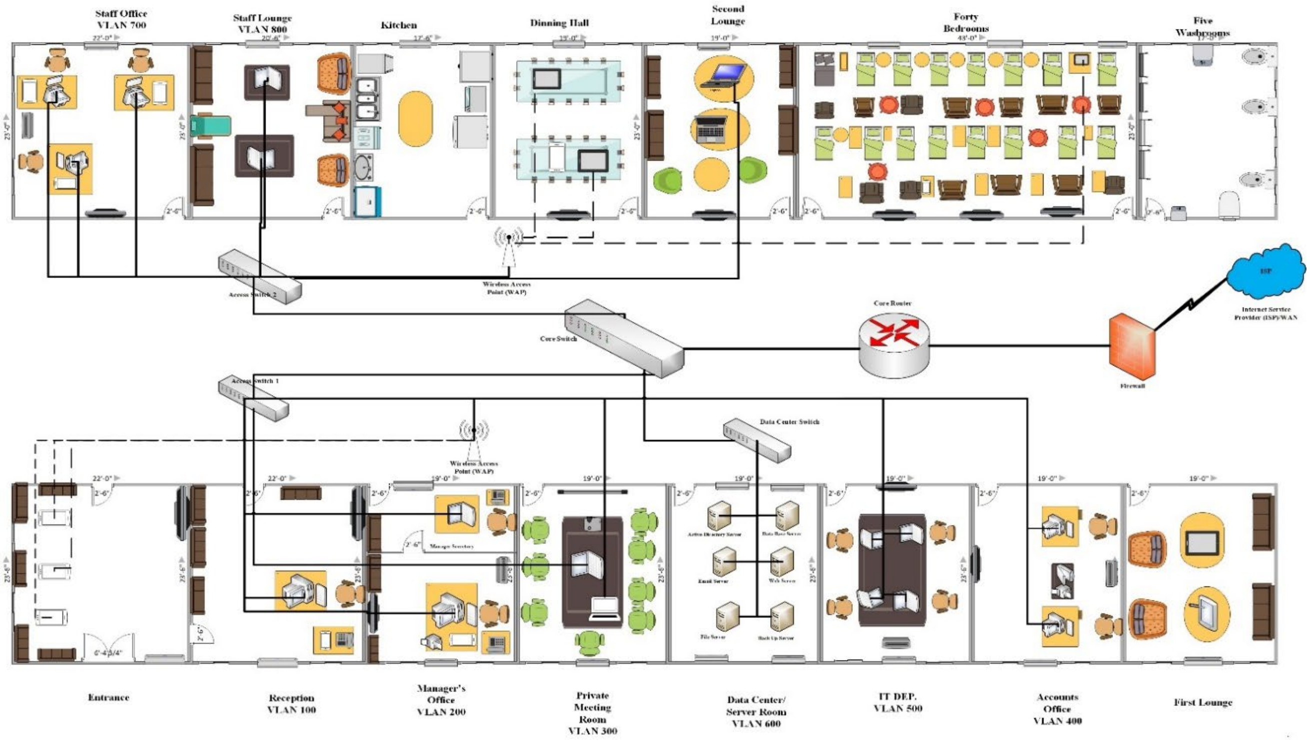
5.7 Poor Physical Security

Physical security is one of the most important security features to consider in a sensitive environment like health environment that keeps records of people in a network architecture. Some physical security measures that should be considered includes perimeter fencing, gates and access controls especially in the data center, surveillance cameras, motion detectors, alarm systems and secure doors and windows. Some technologies include biometric authentication (e.g., facial recognition, fingerprint scanning), smart cards and access control systems and Physical Security Information Management (PSIM) systems.

5.8 Insufficient Wireless Access Point (WAP)

Extra WAP should be procured in the new proposed topology to provide convenient wireless connectivity in the forty bedrooms and provide same for visitors. Additional one of the WAP should be procured for each floor to have one WAP to improved mobility and flexibility, increased security, enhanced productivity, reduced cabling costs and have a simplified network management. The WAP should have security features like WPA3 encryption, 802.1X authentication, MAC address filtering and SSID hiding to enhance its security.

7. PROPOSED/NEW PROTOTYPE NETWORK TOPOLOGY



Authentication Method

Active Directory

The user authentication method used is Active Directory. The project employs Active Directory to manage the systems and users of the network. Active Directory (AD) is a directory service developed by Microsoft that provides a centralized repository for storing information about objects on a network, such as users, groups, computers, and printers. It provides a centralized authentication and authorization to network resources. It uses user name and password-based authentication that requires users to create account with passwords that use a combination of numbers, letters, and symbols to reduce the risk of guessing by hackers.

Other user authentication methods include;

Token-based Authentication; A unique token is created for the users. The users must save this token in order to continue using the system. Tokens come in two varieties: logical tokens, which are wholly software-based, and physical tokens, like the USB token.

However, this might provide an operational problem with regard to the token distribution and control procedure.

Biometric Authentication: The technique used for validation is a print of a finger, face recognition, or an iris scan, where it is the biometric structure of a user that is identified. It verifies users using biological features like facial, fingerprint and voice recognition.

The nursing home network will be monitored using a software firewall aside the hardware firewall for real-time threat detection, vulnerability assessment, and compliance monitoring. I commend Wazuh Application Firewall which has network and application layer protection, real-time traffic analysis and filtering, intrusion detection and prevention systems (IDPS), web application firewall (WAF) capabilities, integration with Security Information and Event Management (SIEM) systems and supports multiple operating systems (Windows, Linux, macOS).

How to remove vulnerability;

- Configure Wazuh to regularly scan the systems for vulnerabilities using scanners like OpenVAS or Nessus.
- Set up alerts and notifications to inform you of newly detected vulnerabilities.
- Wazuh will display a list of identified vulnerabilities, including their severity level and affected systems.
- Filter the list of vulnerabilities by severity level (e.g., Critical, High, Medium, Low).
- Select a vulnerability to remediate.
- Wazuh will provide recommendations for remediation, such as updating software or firmware, applying patches or hotfixes, configuring system settings or policies.
- Implement the recommended remediation steps.
- After implementing the remediation steps, use Wazuh to verify that the vulnerability has been successfully removed.

Terminal Access Controller Access Control System plus (TACACS+)

The project employs the Authentication, Authorization and Accounting (AAA) protocol to manage networking devices and amend identification of confidential code in a unify server remotely. In TACACS+, AAA services are rendered separately and distinguish authentication and authorization operations while both functions are combined in RADIUS. TACACS+ has the ability to combine with its own data storage or work in harmony with other services, Transmission Control Protocol (TCP) is used for transportation, while all the packets are encrypted except the header whereas in RADIUS only the confidential code is encrypted. In the health care system, AAA protocols seem to be the best, but TACASC+ is favorable since it uses TCP for transport that assures a reliable communication between server and the client compared to UDP. TACACS+ allows network administrators to define commands which users can use and above all during transportation data cannot be sniffed from packet due to its encryption.

Data Storage

The following needs to be considered when selecting a data storage for a nursing home, which includes security and compliance that is ensuring the solution and requirements meets HIPAA and other regulatory requirements, scalability that is choosing a solution that can grow with your healthcare facility's needs, ease of use, a user-friendly interface to minimize training and support needs.

Preferably, Network-Attached Storage (NAS) is best suitable option for the nursing home's data storage needs which is an on-premise method of storage. NAS is a device used exclusively as a single centralized storage location for multiple devices on a network. NAS device connects directly to a switch or a router on an existing network via ethernet and contains multiple drives arranged in a Redundant Arrays of Independent Disks (RAID) configuration for redundancy. Once connected, NAS allows data to be accessed as a shared folder by other computers and devices on the network. It uses file-sharing protocols to enable data retrieval and storage, making it easy for authorized users to access files from various devices, including computers and mobile devices. The reason being that

- NAS provides a centralized storage solution, making it easy to manage and access files from multiple devices.
- NAS enables easy file sharing among staff members, reducing the need for email attachments or manual file transfers.

- NAS devices often come with built-in security features, such as encryption, access controls, and backup capabilities.
- NAS devices can be easily scaled up or down as the nursing home's storage needs change.

Specifically, I recommend HPE 3PAR 9450 device, due to its,

- It can handle over two (2) million Input/output operations per second (IOPS) making it suitable for demanding workloads.
- Scalable architecture that can grow with the nursing home needs.
- Support for thin provisioning, which enables you to allocate storage capacity on demand, reducing waste and improving efficiency.
- Support for data encryption, which helps protect your data from unauthorized access.
- Its support of multiple protocols, including Fibre Channel, Internet Small Computer Systems Interface (iSCSI), and NFS.

Table 10 Specification of HPE 3PAR 9450

Feature	**Technical Specification**
Storage Controller	3PAR 9000 10-core 2.4 GHz Controller Node Maximum
Capacity	6000 TiB Maximum
Drive description	SFF SAS
Cache	896 GiB Maximum
Maximum Drives per enclosure	24
Host Interface	32 Gb/sec Fibre Channel (10) Ports per controller 16 Gb/sec Fibre Channel (80) Ports 10 GbE iSCSI/FCoE (40) Ports 10 Gb Ethernet (24) Ports Maximum supported
Compatible Operating Systems	Microsoft Windows Server 2008 Microsoft Windows Server 2008 R2 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Microsoft Windows Hyper-V HP-UX SUSE Linux Enterprise Server (SLES) Red Hat Enterprise Linux (RHEL) VMware ESX and ESXi Oracle Solaris Oracle UEK

	Oracle Linux Citrix XenServer IBM AIX HPE OpenVMS Apple OS X HPE OpenVMS is a registered release only. For the latest information on supported operating systems refer to Single Point of Connectivity Knowledge for HPE Storage Products (SPOCK)
Availability features	Redundant power supplies and fans A minimum of dual redundant controllers, with up to two controllers for added redundancy RAID 1, RAID 5 and RAID 6 for data protection.

Data Protection Issues in the Nursing Home Environment

The new nursing home is likely to face several issues of data protection, which includes;

External Threat; Is a potential risk to nursing home's assets, data, or systems that invents from outside the nursing home environment. It can come from various sources, including hackers, malware, phishing and others. It can have severe consequences like data breaches, financial loss, reputation damage and system interruption.

Data Corruption; It can arise from failure of hardware, errors or bugs in software, accidental deletion or modification of data by authorized persons.

Difficulty recovering or inability to recover data in the event of a disaster.

Internal Threat; This includes authorized users unintentionally or intentionally compromising data security or stealing sensitive data.

Data Compliance; This includes failure to comply with data protection regulations such as GDPR or HIPAA, ensuring compliance with local rules and regulations regarding the processing and storage of data.

To ensure information security in the nursing home, the nursing home should implement robust security measures including,

Physical Security Measures; This includes implementing access controls such as locks, biometric scanners and smart cards to restrict access to sensitive areas in the facility. Similarly, installing security cameras and monitoring systems to detect and deter access.

Network Security Measures: This involves implementation of firewalls to control incoming and outgoing network traffic, IDS and IPS to detect and prevent unauthorized access and malicious activities, VPN to encrypt and secure remote access to the network and transmission of data to outside the nursing home environment, use of secure communication protocols.

Incident Response and Disaster Recovery; This is related to developing incident response plans to ensure prompt and effective response to security incidents, and developing disaster recovery plans to ensure continuity in the event of disaster and conducting regular testing and exercise to ensure incident response and recovery plans are effective and up-to-date, regular security audits and vulnerability assessments.

Data Security Measures; This includes encrypting sensitive data to prevent unauthorized access, implementing access controls, such as strong passwords, two-factor authentication and permissions, to restrict access to sensitive data.

Virtual Private Network (VPN) Technology

In order for the Government Health Service to access the medical records of the old people in the nursing home, VPN technology needs to be employed. The records need to be reliably transmitted and secured. VPN technology is a technology that creates a secure and encrypted connection in open and public network between clients and VPN servers using cryptography. This connection allows you to access the internet securely and privately. It uses a set of cryptographic systems which are message digest algorithm, digital signature, digital certificates, asymmetric encryption, and symmetric encryption. VPN IPsec is the tunneling protocol use to provide protection and data privacy.

Techniques of VPN Connection

VPN connections are separated into two categories: Customer Edge (CE) and Provider Edge (PE), sometimes referred to as Network-based VPN. In PE-base VPN, gargets implement the tunneling process called encapsulation and decapsulation while the CE, gargets have no VPN role to play, also on the other hand, in CE, gargets execute all VPN roles of tunnel encapsulation at the customer end while the PE gargets is indisputable to the VPN tunnel and has no role to play in VPN tunneling. The main aim of adopting a VPN technology is due to data security.

VPN Environment

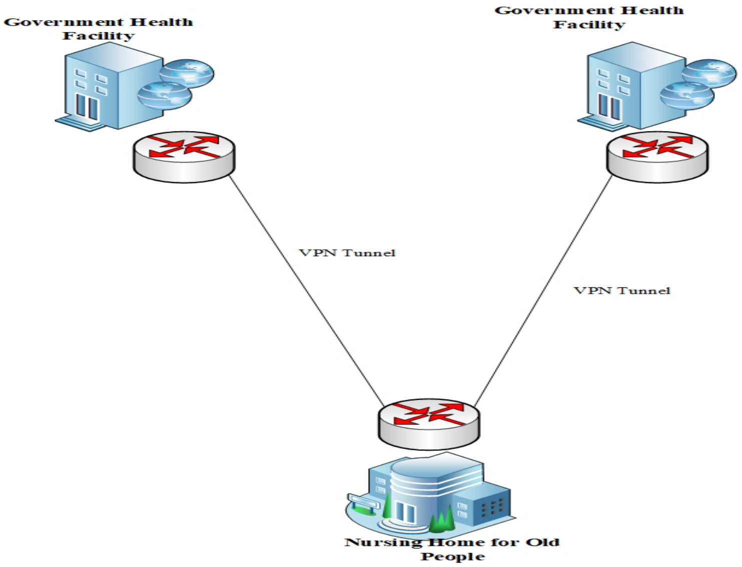

Government Health Facility
Government Health Facility
VPN Tunnel
VPN Tunnel
Nursing Home for Old People

Diagram 4

Internet Protocol Security (IPsec)

It is a tunneling protocol that was introduced by the Internet Engineering Task Force (IETF) to regulate encryption, confidentiality, data originality, and authentication to strengthen integrity at the network layer (layer 3) of the OSI model. It creates end-to-end traffic while guaranteeing the anonymity of data packets, meaning that information like the IP address and payload cannot be intercepted while in transit. The main goal of the IPsec is secure data transmission via unsecure media. A collection of protocols is integrated by IPsec to work as a suite, with each protocol affecting data security. Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulating Security Payload (ESP) are the elements that make up IPsec. IPsec have two forms of operation to establish a secure communication route between communication networks which are tunnel and transport. In Tunnel mode, a new IP header is added to the packet for forwarding as the entire passenger IP packet will be contained and encrypted prior to transportation which is Router-based, whereas in Transport mode, it provides end-to-end communication between IP hosts or devices like routers, VPN users, or firewalls and is computer-based.

Generic Routing Encapsulation (GRE)

GRE is an exclusive layer 3 protocol that enables different protocols to be swallowed in IP tunnels and can engulf any network layer protocol. Although IPsec may be used with GRE tunnels to encode and make it more dependable and secure, GRE is a virtual end-to-end connection that lacks protection and flexibility since packets are not coded during transmission.

Protocols that do not support IPsec may be executed using a GRE tunnel. Before the encapsulation process starts, all data traffic traveling between the sites is encased in a GRE packet. The GRE first encapsulates the private IP packets using the tunneling protocol, and it has the ability to engulf numerous protocols over backbone single protocols. VPN over WAN is made possible using GRE tunneling, which is also inexpensive and easy to set up.

Encapsulating Security Payload (ESP)

ESP is one of the IPsec protocols that uses encryption and encapsulation to protect the confidentiality of data. Prior to transportation, ESP adds extra ESP header and trailer fields to the packet and encrypts the original data. Both tunnel and transit modes are compatible with AH and ESP. The ESP standard format published by IETF 2406 includes the payload data, authentication data, next header, and pad length.

Internet Key Exchange (IKE)

It is a tool for communicating with different protocols. To protect all data and data integrity, many internet protocols require security checks. Security frameworks like Internet Security Association and Key Management Protocol (ISAKMP) are implemented by it. Security Association (SA) is the fundamental of IPsec by setting arrangement of principles encoding tools. It is a data formation which is utilized to store and secure all the privacy variables between devices. IKE is divided into two stages: phase 1 involves setting up IKE SA to create a secure authenticated communication link by generating a shared secret key for encryption, and phase 2 involves IPsec SA, which clarifies and secures data flow between peers and configures access lists to allow.

IP Addressing System/Scheme

The following information is in regards to the nursing home new network infrastructure IP addressing system. The project suggests the use of IPv4 Class C IP address scheme, 192.168.1.0 (a private IP) due to the fact that a Class C contains enough hosts for all the connected clients in the nursing home. A Class C IP address will only allow a maximum of 254 total available hosts for the network. The nursing home will use this Class C and internal NAT subnetting to communicate the network designated IPs to the global network IP, 90.44.22.5. The private address is free and cannot be route over the internet. To be able to route private IP address over the internet, Network Address Translation (NAT) must be implemented on the private address utilizing public IP address. The Internet service provider (ISP) will provide two or more public IP addresses for translation over the internet.

IP: Class C - 192.168.1.1
Subnet Mask: 255.255.255.0
Total Available Hosts: 254
Network Address/ Base Network: 192.168.1.0
Range: 192.168.1.1 - 192.168.1.254
Broadcast: 192.168.1.255

Table 11 **IP Addressing Scheme**

Department	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address	Subnet Mask	VLAN ID
Reception	192.168.1.0/29	192.168.1.1	192.168.1.6	192.168.1.7	255.255.255.248	VLAN 100
Managers Office	192.168.1.8/29	192.168.1.9	192.168.1.15	192.168.1.16	255.255.255.248	VLAN 200
Private Meeting Room	192.168.1.17/29	192.168.1.18	192.168.1.23	192.168.1.24	255.255.255.248	VLAN 300
Accounts	192.168.1.25/29	192.168.1.26	192.168.1.31	192.168.1.32	255.255.255.248	VLAN 400
IT Department	192.168.1.33/29	192.168.1.34	192.168.1.39	192.168.1.40	255.255.255.248	VLAN 500

Data Center	192.168.1.41/29	192.168.1.42	192.168.1.47	192.168.1.48	255.255.255.248	VLAN 600
Staff Office	192.168.1.49/29	192.168.1.50	192.168.1.55	192.168.1.56	255.255.255.248	VLAN 700
Staff Lounge	192.168.1.57/29	192.168.1.58	192.168.1.63	192.168.1.64	255.255.255.248	VLAN 800

The IP address must be sub-netted for efficient use of IP addresses, improved network organization and management, enhanced network security, better network performance. It is done using the Variable Length Subnet Masking (VLSM). The IP addressing scheme comprises of eight (8) subnets for the eight VLANs. I selected /29 subnet which gives 6 usable hosts and the intention for selecting /29 is that you won't need to redo the network when the number of users per department increases in the future, the network will always accommodate such increases.

8. SECURITY AND NETWORK POLICIES

The Nursing Home network will adhere to the following guidelines and policies to maintain uniform integrity in the workplace.

- **E-mail Policy**

The aim of the email policy is to avoid damaging the nursing home reputation. The public will often interpret emails sent by the nursing home as official statements of the nursing home policies. The policy applies to all staffs, vendors and agents operating on behalf of the nursing home.

Policies

Prohibited Use: The nursing home email system is prohibited to create or disseminate any disruptive or offensive communications including remarks that are offensive about national origin, gender, age, sexual orientation, sexual orientation, pornography, religious beliefs and practices, or political views. Staff should notify their supervisor right once if they receive any emails from staff members that include this information.

Personal Use: Using a reasonable amount of the nursing home resources for personal emails is acceptable, but non-work-related emails shall be saved in a separate folder from work related email. Sending of chain letters or joke emails from the email account is prohibited. Virus or other malware warnings and mass mailings from the nursing home shall be approved by InfoSec of the IT Department before sending. These restrictions also apply to the forwarding of mail received by a staff.

Monitoring: The staffs shall have no expectation of privacy in anything they store, send or receive on the email system. InfoSec may monitor messages without prior notice, but is not obliged to monitor content in email messages.

Automatic Forwarding: Staff must be cautious when sending an email from the nursing home facility to an outside network. Upon approval by the InfoSec of the IT Department or Manager, emails will not be forwarded to an external destination. No email containing sensitive information will be sent unless it is absolutely necessary for the operation of the business and is encrypted in compliance with the Acceptable Encryption Policy.

Implementation

Any staff who violates this policy might face disciplinary action, which could include termination of appointment.

❖ Internet Equipment Policy

This policy outlines requirements for all equipment owned and/or operated by the nursing home. It is also intended to reduce the risk of the facility losing intellectual property, sensitive or company-confidential data, or harming its reputation due to unauthorized use of facility resources.

The requirements the policy outlines include:

- ✓ Ownership responsibility
- ✓ Secure configurations requirements

- ✓ Operational requirements
- ✓ Change control requirements

Every device/gargets such as routers, switches, hosts owned and/or operated by the nursing home, registered in the Domain Name System (DNS), must follow this policy. The policy also covers any host garget outsourced or hosted at external/third party service providers, if that garget is located in the domain or appears to be owned by the nursing home. All new gargets which fall under this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from the Information Security (InfoSec) of the IT Department. All existing and future gargets deployed on the nursing home untrusted networks must comply with the policy.

Policies

Ownership Responsibilities

- ✓ Equipment must be documented in the wide enterprise management system which should include host name and location, hardware and operating system/version, main functions and applications, password groups for privileged password.
- ✓ Password groups must be maintained in accordance with the corporate wide password management system/process.
- ✓ Immediate access to equipment and system logs must be granted to members of Infosec in the IT Department or manager of the facility upon demand, per the Audit Policy.
- ✓ Network interfaces must have appropriate Domain Name Server records.

InfoSec of the IT Department shall conduct periodic equipment audits in accordance with the Audit Policy to ensure adherence to this policy.

General Configuration Requirement

- ✓ InfoSec must approve hardware, operating system, services and applications as part of the pre-deployment review stage.
- ✓ All patches/hot-fixes recommended by the equipment vendor and InfoSec must be installed.
- ✓ Services and applications not serving business requirements must be disabled.

- ✓ Services and applications not for general access must be restricted by access control lists.
- ✓ Insecure services or protocols (as determined by InfoSec) must be replaced with more secure equivalents whenever such exist.
- ✓ Security-related events must be logged and audit trails saved to InfoSec-approved logs. Security related events include (but are not limited to) the following: user login failures, failure to obtain privileged access, access policy violations.

New Installations and Change Management Procedures

- ✓ Configuration changes must comply with the Corporate Change Management (CM) Procedures.
- ✓ InfoSec must perform system/application audits prior to the deployment of new services.

Equipment Outsourced to External Service Providers

Contracts with external service providers and security associates should specify who is responsible for the security of the equipment deployed, and growth protocols should be defined.

Implementation

Any staff found who violates this policy may be subjected to disciplinary action, including termination of appointment. External service providers who violate this policy may be subject to financial penalties, including termination of contract.

- ❖ **Computer Network and Internet Access Policy**

The computer network is the property of the Nursing home and may be used only for legitimate business purposes that is assisting staffs in the performance of their jobs. All staffs have a responsibility to use the computer and internet in a professional, lawful and ethical way. Abuse of the network or internet may result in disciplinary action, including possible termination of appointment.

The Company's computer network may not be used for the dissemination, viewing, or storage of commercial or personal advertisements, solicitations, promotions, destructive code (such as viruses or self-replicating programs), political content, pornographic text or images, or any other unauthorized materials without the Company's prior written consent. Using the company's Internet connection to play games or download entertainment applications, such as screen savers, is prohibited for employees. Furthermore, it is prohibited to display, store, or transmit any content that is defamatory, obscene, threatening, sexually explicit, harassing, embarrassment, fraudulent, or otherwise improper or illegal across the computer network. Furthermore, the supervisor should be informed right once by anybody who receives such documents.

Users using a computer connected to the company's network must use an authorized Internet firewall or other security equipment to access the Internet in order to maintain security and prevent the spread of viruses. Unless the computer you are using is not linked to the company's network, it is highly forbidden to go beyond the security of the company's computer network by going straight to the Internet via a modem or another method.

The Nursing Home has the right to deploy software that makes it possible to identify and prevent access to Internet sites containing sexually explicit or other information deemed improper in the workplace.

Guidelines on Anti-Virus Procedures

- ✓ Always run the corporate standard. Download and run the current version; download and install anti-virus software updates as available.
- ✓ Do not open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- ✓ Delete spam, chain, and other junk emails without forwarding it.
- ✓ Never download files from unknown or suspicious sources.
- ✓ Always scan a flash drive/ floppy diskette from an unknown source for viruses before using.
- ✓ Back-up critical data and system configurations on a regular basis and store the data

in a safe place.

❖ Wireless Policy

All wireless infrastructure devices that are part of the nursing home network or that are located on the nursing home property and offer wireless access to endpoint devices, such as laptops, desktop computers, mobile phones, and personal digital assistants (PDAs), are governed by this policy. Any wireless communication device that can send packet data falls under this category.

General Network Access Requirements

All wireless infrastructure devices that reside at the nursing home site and connect to the network, or provide access to information classified as confidential, highly confidential, or restricted must:

- ✓ Be installed, supported, and maintained by an approved support team.
- ✓ Use the nursing home approved authentication protocols and infrastructure.
- ✓ Use the nursing home approved encryption protocols.
- ✓ Maintain a MAC address that can be registered and tracked.
- ✓ Not interfere with wireless access deployments maintained by other support organizations.

Implementation

A staff found to have violated this policy may be subject to disciplinary actions, including termination of appointment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment.

❖ Wireless Network Security

Wireless networks need more collaboration and coordination to optimize the technology's advantages for the staff of the nursing home, and wireless communication raises security concerns for the facility. This document sets forth the policies for using wireless technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless radio frequency spectrum in a distributed environment.

This policy applies to all wireless network devices utilizing the nursing home IP space and all users of such devices, and governs all wireless connections to the facility network backbone, frequency allocation, network assignment, registration in the Domain Name System, and services provided over wireless connections to the facility network backbone.

Policies

- ✓ Wireless access points shall require user authentication at the access point before granting access to Internet services.
- ✓ Wireless equipment and users must follow all network connection policies set forth.
- ✓ Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited.
- ✓ Wireless access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks.
- ✓ Wireless passwords and data must be encrypted.
- ✓ Wireless networks must be designed and deployed to avoid physical and logical interference between components of different network segments and other equipment.
- ✓ The IT Department will attempt to resolve any interference or security incidents by coordinating with the registered Point of Contact (POC) for the wireless network.
- ✓ Any wireless network that poses a security threat may be disconnected from the facility's backbone network.

❖ User Account Access

This policy outlines individual responsibilities concerning the legal and ethical use of the nursing home systems, network resources and electronic information. Information technology resources include computer hardware, software, data and physical and network infrastructure, as well as personally owned devices connecting to these resources, fall within the intent of this policy.

Access

- ✓ Manager of the nursing home can only make accounts
- ✓ No staff should create, modify, execute or retransmit any computer program or instructions to gain unauthorized access to the nursing home database.
- ✓ Personal devices should not be used to spy on activities of others.
- ✓ Attempts to degrade the performance of the nursing home technology systems is prohibited.
- ✓ Staffs are to refrain from controlling systems, overloading networks with excessive data, disk space and other information technology resources.

Password Requirements

This covers any employee who has or is in charge of an account or type of access that supports or necessitates a password on any system that is located at an XYZ Hospital facility, has network access, or houses any confidential XYZ Hospital data.

Guidelines for Strong Password

- ✓ Password must contain upper- and lower-case characters.
- ✓ Password must be at least fourteen characters long.
- ✓ Passwords must contain a combination of numbers, letters and symbols
- ✓ Passwords must not be a dictionary word.
- ✓ Passwords must be changed every 90 days.
- ✓ Passwords cannot be based on personal information, names of family, or username.
- ✓ Passwords are not to be written down, stored on-line or shared with anyone.
- ✓ Passwords are not to be sent out through email messages or via phone or instant messaging.

Network Access

Personal devices are not allowed to interfere with the nursing home services, functions, or responsibilities in order to maintain the technology's availability, functionality, and security.

Staffs are prohibited from extending network access beyond what the nursing home offers, as well as from using any technology that circumvent network access or exit controls.

- ❖ **Hardware Firewall**

Every hardware equipment must be utilized in accordance with the relevant contracts, agreements, notices, and licenses. In addition to filtering traffic to reduce risks and losses related to security threats to the nursing home network and information systems, firewalls are used to provide a secure environment for the nursing home computer and network resources.

Firewalls Security Services

- ✓ The Administrator should only update the firewall and apply patches and other security enhancements and stay current on new vulnerabilities and incidents.
- ✓ Firewall must be configured to detect emergencies, such as system unusable messages.
- ✓ There should be access control between the internal network and un-trusted networks.
- ✓ Firewall must block unauthorized traffic while maintaining security that doesn't impact authorized users excessively.
- ✓ Firewall must detect alerts, critical conditions and error messages.
- ✓ Firewall must hide system names, network topology, network device types, and internal user ID's from the Internet.
- ✓ Firewall must provide stronger authentication than standard applications.
- ✓ Firewall must log and detect failed and multiple unsuccessful login attempts.
- ✓ Firewall must log conspicuous traffic to and from the nursing home internal network.

- ❖ **Encryption**

The purpose of this policy is to ensure that encryption keys are securely managed. It's essential that encryption keys are created, stored, used and destroyed in the appropriate manner in all situations so that critical and confidential information are protected from unauthorized persons. These keys should be accorded the highest levels of security available and that staff and manager are aware of their responsibilities.

This affects all users of computer systems and networks responsible for the management and use of encryption keys.

Use of Encryption

Encryption must be used to encode data where the risk of loss through theft or interception is high, where there is the potential for a major security breach should that data get into the hands of unauthorized persons and where the loss of the data would have a major impact on the nursing home business.

❖ Log Tracking

Network and system logs related to personally identifiable medical information must be retained for five (5) years, payment card, debit or credit transactions, must be retained for a year. All other network and system logs will be retained for ninety (90) days, which include, server operating system logs, email records, internet usage monitoring software logs, remote access logs, network edge routers, database transactional, firewall logs, IDS software logs, software security monitoring/violation logs.

❖ Reporting of Incidents

Analysis of trends and types of security incidents and breaches is crucial to the integrity of nursing home data management and computer security. All security incidents and breaches must be reported to the IT Department for investigation and analysis.

Policies

- ✓ Each department must have a designated Departmental Head or Coordinator (HoD). The role of the HoD is to communicate and coordinate access to administrative systems for staffs in their department.
- ✓ To request new user-ids or authorization for departmental employees to access On-line Administrative Systems files, the HoD should complete and sign the Request for On-line user-id and Administrative System Access form and mail to the manager.
- ✓ Authorized file access can be granted only by the Manager of the nursing home. The manager will contact the HoD to discuss specific access and update authority to be granted users.

❖ Physical Security

Physical security is a key component of a well-rounded security operation. A compact physical security foundation protects and preserves information, physical assets, and human assets by reducing the exposure to various physical threats that can produce a disruption or denial of computer service. The Manager is responsible for ensuring that corporate information assets under their control are properly protected through the implementation of cost-effective physical security measures.

Policies

- ✓ The staff in charge of a computer facility that operates any platform computer system is responsible for providing adequate physical protection of computer equipment and data media.
- ✓ All the staff of the nursing home are responsible for securing their access unit from unauthorized use. Whenever a user is away from his or her access unit during the day, he or she must protect the XYZ Hospital information assets by either logging off of the computer, or activating a password protected screen saver.
- ✓ At the end of the workday, each staff is required to log off of his or her access unit.
- ✓ The nursing home offices and building shall have normal physical security controls in place. Areas should be designed having limited accessibility with personnel access controlled by a biometric hand scanner.

❖ Violations and Enforcement

Staffs who violate any of these policies may be denied access to facilities, IT resources and may be subject to other penalties and disciplinary action, within the nursing home. Violations may be handled through the nursing home disciplinary procedures applicable to the relevant staff.

Additionally, facilities may temporarily suspend, block or restrict access to an account, independent of such procedures, when it reasonably necessary to do so in order to protect the integrity, security, or functionality of facilities or other IT resources or to protect the nursing home from liability. The nursing home may also refer suspected violations of applicable law to appropriate law enforcement agencies.

- ❖ **Disaster Recovery Policies**

The following established policies and procedures for the creation and implementation of an agency disaster recovery plan are under the purview of the nursing home for old people. The nursing home is responsible for the development and testing of a disaster recovery plan for the facility's IT systems.

Information Technology Policies

For all vital data processing applications and the auxiliary tasks that support them, disaster recovery planning and the capacity to execute a recovery are crucial.

The aim of this policy is to enhance the operational capabilities of all information technology resources, that is hardware, software and personnel that support the critical missions of the state in the event of a natural or tragedy caused by humans.

This policy applies to the data center.

Policies

- ✓ Backups will be updated on a daily basis by Differential backup.
- ✓ In the event of a natural disaster, such as a hurricane, floods, wild fires, should there be a server damage, or servers cannot be access by the IT Department or Manager, backups will be used for access to the same material that would be backed up.
- ✓ Managers should be contacted and advised immediately in case of a disaster and status.
- ✓ Accessing backups and putting them into action as quickly as feasible while staying within the Recovery Time Objective time are the necessary steps.
- ✓ All data, operating systems, and utility files including all patches, fixes and updates must be adequately and systematically backed up.
- ✓ Records must be maintained as to what is back up and where was it done.
- ✓ Software licensing should be backed up.
- ✓ The backup media must be precisely labeled and accurate records must be

maintained of back-ups done and to which back-up set they belong.

- ✓ Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away, to escape any damage from a disaster at the main site.
- ✓ In case of security breach or malicious code is places on hardware immediate shut down of infected server is to take place. Backup will replace the primary server before server shut down for no down time.
- ✓ Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency.
- ✓ Possible capture of malicious code will be sent to government agencies for inspection.
- ✓ UPS will be placed on all machines using building power. In case of power outage the UPS will provide sufficient power for the time the generator will start working.
- ✓ UPS will be tested every 4 months. This will ensure all UPS are working. Tests need to be documented every time test is issued.
- ✓ Shut down of servers will include full wipe of all files and a clean install will be necessary.

Implementation:

The nursing home will be required to submit annual disaster recovery plans along with documentation of all test exercises.

9. SECURITY AND VULNERABILITY ASSESSMENT

The project used a manual scan for the assessment using Network Mapper (NMAP) in order to examine the Common Vulnerability and Exposure (CVE) and Common Vulnerability Scoring System (CVSS) to enable us to gather the risk score.

Information of the systems

Target System: Metasploitable, IP Address 10.10.1.129

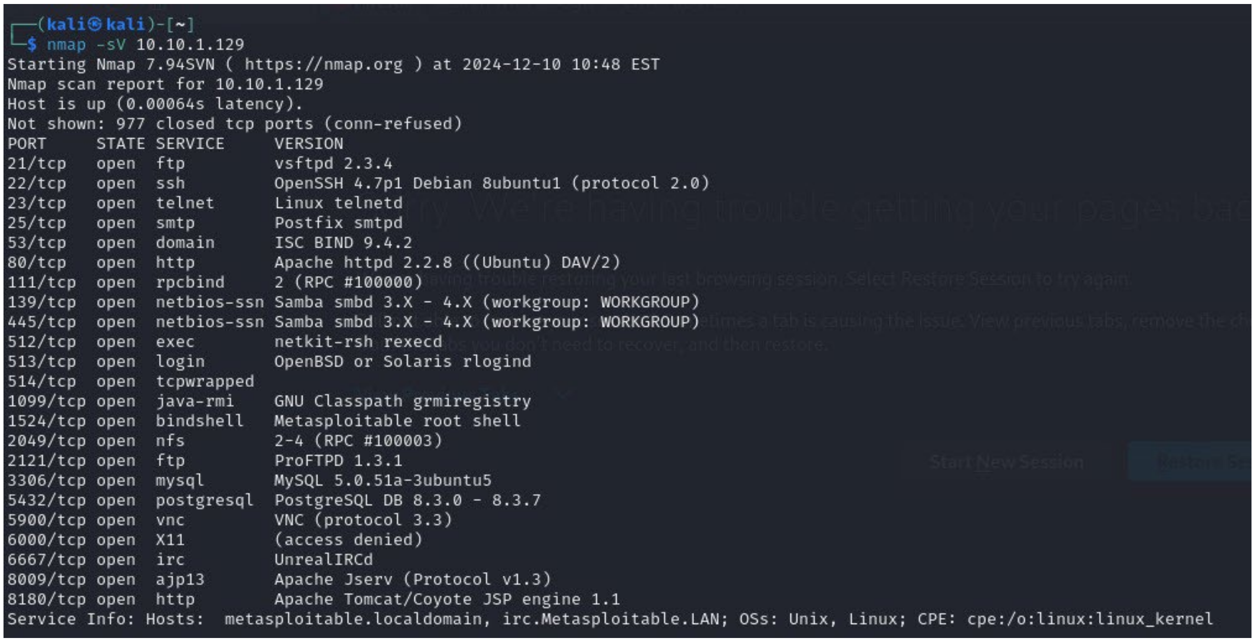
Attacker System: KALI (v6.11.2), IP Address 10.10.1.38

Performing the Vulnerability Scan

- Lauch both systems that is the Kali and Metasploitable
- Test the TCP/IP Connectivity by pinging each system using the IP Addresses.
- Scan the targeted system for vulnerabilities using NMAP tool in KALI

Note: The vulnerability report should include info of open ports, service and version.

kali@kali:~$ nmap -sV 10.10.1.129



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.1.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-10 10:48 EST
Nmap scan report for 10.10.1.129
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- In analysis of the various vulnerabilities, we first of all take the first vulnerability that is **ftp vsftpd 2.3.4** running on **port 21** and find the CVE ID at **https://cve.mitre.org**

The CVE ID is

CVE-2011-2523 vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

The primary purpose of the CVE program is to identify, describe, and catalog cybersecurity flaws disclosed publicly.

The National Vulnerability Database (NVD) is tasked with enriching each CVE once it has been published to the CVE List. **https://nvd.nist.gov/general/cve-process**

Findings

Backdoor Command Execution

https://www.cve.org/CVERecord?id=CVE-2011-2523

Description:

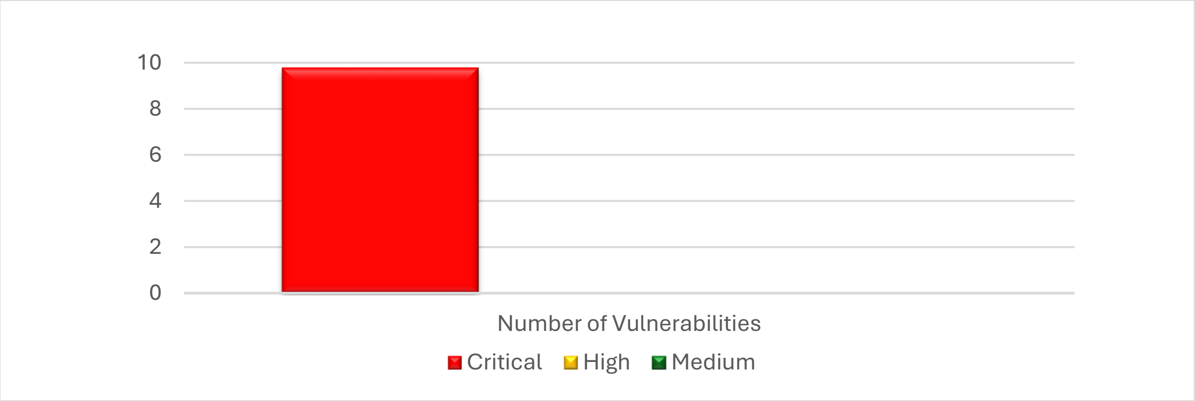
The vulnerability **vsftpd 2.3.4** downloaded between 2011/06/30 and 2011/07/03 contains a backdoor which opens a shell on port 6200/tcp.

Publish Date: 2019-11-27 **Updated:** 2021-04-12

Finding the Risk Score

- Looking for the risk score from **https://www.cvedetails.com** to determine the severity of the vulnerability when attackers potentially take an advantage to exploit. **https://www.cvedetails.com/** is a vulnerability intelligence solution that provides CVE security vulnerability database, exploits, advisories, product and CVE Risk Scores.

Table to indicate the severity of the vulnerability.



Total Findings	Critical	High	Medium
1	1	0	0

The **CVSS Scores** for CVE-2011-2523 is 9.8 and 10 which indicates **Critical**

https://www.cvedetails.com/cve/CVE-2011-2523/

Recommendations

The System Administrators are strongly advised to update to the latest version VSFTPD 3.0.5-13 to protect their servers from exploitation.

10. CONCLUSION

In conclusion, this research work implemented VPN security which is a fundamental network necessity where confidentiality, integrity and high availability are essential. In the health industry, where patients require a high level of privacy and confidentiality of their medical records, it is particularly pertinent and appropriate. The designed network used IPsec VPN and GRE to meet up the security measures as demanded by the client, VPN appears to have nice security features for organization network however is still susceptible to attacks even the most secured network on earth is vulnerable to attacks, a combination of IPsec VPN + GRE will offer a better defense to attacks. Fault tolerance is another crucial component that will guarantee high availability and robustness of a network which is highly needed in a healthcare sector due to emergency that arises at any given time, for a high-quality health service to be sustained the network link must be robust and highly available. Therefore, with the present development we can now concluded that the deliverable presented to the client was successful.

REFERENCES

1. Marwa, A., Malika, B. and Nacira, G. (2013). “Contribution to Enhance IPSec Security by a Safe and Efficient Internet Key Exchange Protocol.” In: *IEEE International Conference Proceedings on World Congress Computer and Information Technology (WCCIT)*, 22nd-24th June, pp. 1-5.

2. Cisco (2007). Available at IPSec Negotiation/IKE Protocols - Configuration Examples and TechNotes – Cisco.

3. Bruno, A. and Jordan S. (2011). *CCDA 640-864 Official Cert Guide*, Cisco Systems.

4. Baghaei, N. and Hunt, R. (2004). “Security Performance of Loaded IEEE 803.11B Wireless Networks.” *Computers Communications* 27 (2004) 1746-1756.

5. Bottino, L. J. (2006). “Security Measures in Secured Computer Communications Architecture.” In: *IEEE/AIAA 25th Digital Avionics Systems Conference*, pp. 1-18.

6. Amadasun, K., Short, M. and Crosbie, T. (2020). “Telecommunication Infrastructure Sharing: A Remedy for the Reduction of Network Operator Costs and Environmental Pollution?” In: *Proceedings of the 20th IEEE International Conference on Environment and Electrical Engineering (EEEIC 2020)*, Madrid, Spain, June 2020.

7. Irving, P. (2010). *Computer Networks* (3rded.), Lexden Publishing Limited.

8. Balchunas, A. (2007). “Static vs. Dynamic Routing.” Available online at: *http://www.routeralley.com/ra/docs /static_dynamic_routing.pdf.*

9. Hassan, H., Eltoweissy, M., and Youssef, M. (2009). “Cell Net: A Bottom-Up Approach to Network Design.” In: *Proceedings of the 3rd International Conference on New Technologies, Mobility, and Security*, pp. 433-438.

10. Manghui, T., Liangliang, X. and Dianxiang, X. (2013). “Maximizing the Availability of Replicated Services in Widely Distribution System Considering Network Availability”. In: *IEEE International Conference proceedings on Software Security and Reliability (SERE) 2013 Gaithersburg*, MD 18th–20th June, pp. 178–187.

11. Chen, F., Wu, K., Chen, W. and Zhang, Q. (2013). “The Research and Implementation of the VPN Gateway Based on SSL.” In: *IEEE International Conference Proceedings on Computational and Information Sciences (ICCIS)*, Shiyang, China, 21st-23rd June, pp. 1376-1379.

12. Rossberg, M. and Schaefer, G. (2011). “A Survey on Automatic Configuration of Virtual Private Networks.” *Computer Networks* 55 (8) 1684-1699.

13. Zaharuddin, M. H. M., Rahman, R. A., and Kassim, M (2010). “Technical Comparison Analysis of Encryption Algorithm on Site-to-Site IPSec VPN.” In: *IEEE International Conference proceedings on Computer Application and Industrial Electronics (ICCAIE)*, Kuala Lumpur, Malaysia 5th-8th Dec., pp. 641 -645.

14. Dhall, H., Dhall, D., Batra, A. S. and Rani, P. (2010). “Implementation of IPSec Protocol.” In: *IEEE International Conference Proceedings on Advance Computing and Communication Technologies (ACCT)*, Rohtak Haryana, India, 7th-8th Jan, pp. 176-181.

15. Jaha, A., Ben-shatwan, F. and Ashibani, M. (2008). “Proper Virtual Private Network (VPN) Solution.” In: *IEEE International Conference proceedings on Next Generation Mobile Applications, Services and Technology (NGMAST)*, Cardiff, UK, 16th–19th Sept., pp. 309-314.

16. Gong, G., Qiang, S. and Wang, J. (2009). “Information Security Measures and Regulation Research.” In: *IEEE International Conference Proceedings on Management Science and Engineering (ICMSE)*, Moscow 14th–16th Sept, pp. 2184-2189.

17. Andrew, T. and Maarten, V. (2007). *Distributed Systems Principles and Paradigms*. Pearson Prentice Hall Inc.

18. https://www.cisco.com/site/us/en/products/networking/sdwan-routers/index.html

19. https://cve.mitre.org

20. https://nvd.nist.gov/general/cve-process

21. https://www.cve.org/CVERecord?id=CVE-2011-2523

22. https://www.cvedetails.com/cve/CVE-2011-2523/

23. https://www.cvedetails.com/

24.https://buy.hpe.com/us/en/storage/disk-storage-systems/3par-storeserv-storage/3par-storeserv-storage/hpe-3par-9450-upgrade-node-with-all%E2%80%91inclusive-single%E2%80%91system-software/p/q0e94a