Computer Infrastructure Report

CareConnect

Thomas Juricek, Dylan Street, Peter Bizub

Lewis University

FA25-CPSC-49300: Computer Infrastructure Capstone Project

12/12/2025

Contents

Abstract (Dylan)

Information security and system reliability have become big concerns in the world of healthcare computer infrastructure. When taking an analytical visit to the clinic CareConnect, the infrastructure is outdated, unreliable, and puts them at great risk of violating safety and privacy guidelines which could cause major penalties for the clinic. A plan has been constructed to modernize CareConnect's infrastructure so that it is reliable and secure enough to not cause violations from breaking privacy guidelines. This plan will also include equipment to withstand and protect against outages as well as allowing for scalability in infrastructure. By following our plan, CareConnect can comfortably assume their computer infrastructure won't get them in trouble with privacy and security guidelines, always know they will have patient and company data available from anywhere even in outages, and as they expand, their network will too.

Introduction (Tommy)

CareConnect is a small, but modern healthcare clinic in Romeoville, IL, providing primary care services. They mostly serve a local population in the surrounding suburban area. They mostly specialize in primary care, which consists of routine checks, disease management, vaccinations, and some minor in-office procedures. The CareConnect clinic will usually see a wide range of patients throughout the week, usually ranging from 20-50 patient encounters per day. The clinic is looking to update their IT infrastructure, with the intention of increasing quality of service, and patient safety. Careconnect operates with 25 employees including physicians, nurses, and administrative staff who rely on the network infrastructure to access electronic health records, communicate with patients, and coordinate care. The infrastructure must support approximately 20 active users during business hours (8 AM to 5 PM, Monday through Friday) and 10 to 30 guest Wi-Fi devices. The network will include 20 desktops, 10 laptops, 20 VoIP phones, two printers, three wireless access points, one managed switch, and a next generation firewall. The Romeoville clinic consists of several functional areas, shown in figure 1, such as exam rooms, a reception and waiting area, administrative offices, billing and records, a staff office, an IT room, and a dedicated server room, all of which require reliable internal connectivity. In addition to the main clinic site, the organization maintains connectivity with a Chicago headquarters and a St. Louis branch through IPSec VPN tunnels over each location's local ISP.

CareConnect's current network is facing significant reliability and security challenges. Right now, the network is unsegmented, meaning medical devices, staff workstations, and guest Wi-Fi all share the same unrestricted space. We also lack redundancy and off-site backups, which puts patient data at serious risk during outages or hardware failures. To make matters worse, reliance on end-of-life hardware is creating security gaps that threaten HIPAA compliance. This project will overhaul the infrastructure to prioritize security and stability. We will implement Virtual Local Area Networks (VLANs) to segment traffic, establish off-site backups, and replace outdated equipment. On the operational side, the new network will support essential services, including secure VPNs for clinical staff needing remote access and VoIP for the facility's 20 IP phones. To ensure ongoing security, we will deploy IDS/IPS systems and a SIEM for continuous monitoring, while handling standard connectivity via DHCP, DNS, and NTP. Finally, we will ensure HIPAA compliance through a robust data protection strategy involving both on-site snapshots and off-site backups.

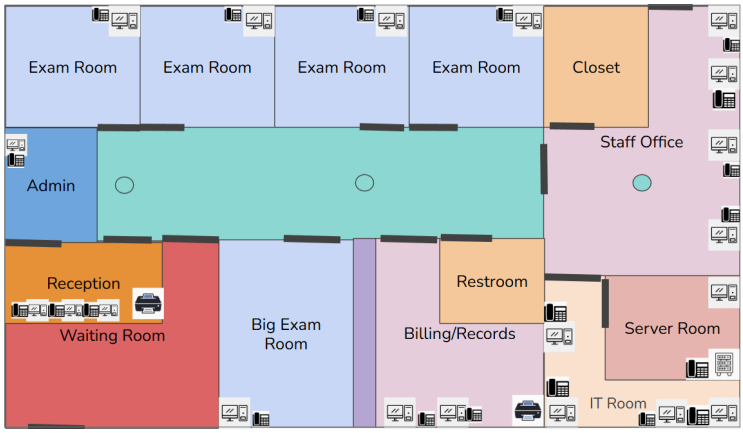

Figure 1. Physical layout of the Romeoville clinic with exam rooms, administrative areas, and dedicated IT and server spaces.

The paper is structured as follows. First, we present a network topology incorporating VLANs and secure off-site backup. Second, we detail security tools and configurations including IDS and IPS, firewall rules, and staff security training. Third, we acknowledge the contributions and cite technical references supporting our design decisions.

Background

Network Layout (Tommy)

Network layout refers to the logical arrangement of devices and connections in the CareConnect IT infrastructure. A good network layout should ensure that data moves quickly and smoothly between devices, support the addition of more devices and users without significant performance loss, maintain fault tolerance by reducing the risk of outages, and remain secure against cyber threats. Just as importantly for CareConnect, the layout must also be cost-effective given the clinic's relatively small size. There are several network layout types commonly used in modern infrastructure design. The topologies considered for the CareConnect network were ring, bus, mesh, and active star [29].

A ring network is designed in a loop where adjacent pairs are directly connected. Data is passed through neighboring devices to reach each node. Traffic is very predictable in a ring topology since data usually travels in one direction. A ring topology is efficient in small environments and can be implemented as a dual-ring to increase resilience. In a bus topology, every device is connected to a main cable called the bus. This is a very simple design, and new devices can be added by connecting to the main cable without reconfiguring the network. On the downside, if the main cable is disconnected or breaks, the entire network goes down, and as more devices are added, performance can quickly degrade due to data congestion. A mesh topology is one in which devices are interconnected so multiple communication paths exist between any two nodes. Because traffic can take many routes, mesh networks are reliable and allow communication even if one link fails, and they perform well due to multiple direct paths between nodes. Unfortunately, a mesh topology can be costly since each node must be connected to others, requiring extensive cable and management. In an active star topology, a managed switch acts as the central device [10], regenerating network signals while controlling traffic between connected nodes, as shown on device B in *Figure 2*. In an active star, the switch can enforce policies, segment traffic, and direct data efficiently, limiting congestion [6]. It is also easily scalable, since a new node can be added simply by connecting it to the core switch. For the CareConnect network, an active star topology will be implemented. The design supports VLAN segmentation, provides predictable performance, and is easy to secure, while remaining cost-effective to implement.

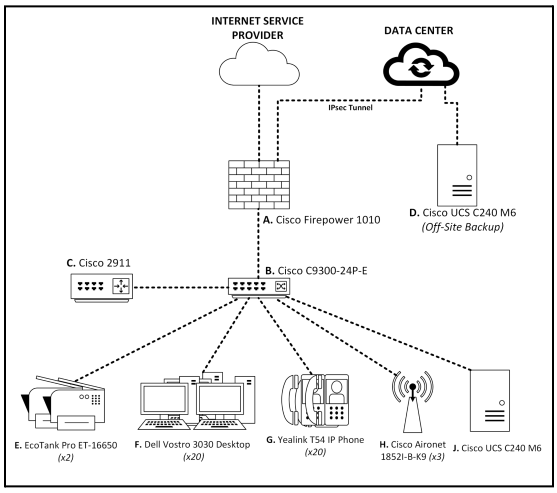

Figure 2. Shows a star topology. The Cisco C9300 acts as the core switch, and everything branches from it.

Perimeter Security and Threat Prevention (Tommy)

A firewall serves as the primary security device at the network perimeter, separating trusted internal clinic systems from external networks and the internet. There are two common types of firewalls: traditional firewalls and next-generation firewalls (NGFW). A traditional firewall inspects inbound and outbound traffic based on access control lists (ACLs) to prevent malware, data exfiltration, and unauthorized access. An NGFW does everything a traditional firewall can, but extends those capabilities by performing deep packet inspection, sandboxing and analyzing suspicious traffic, and using real-time threat intelligence to stop attacks that a traditional firewall may not detect.

CareConnect's current network uses an outdated traditional firewall, which provides poor perimeter security. This leaves patient records and administrative systems exposed to the types of external threats discussed above, threats a modern NGFW is better equipped to prevent. To improve perimeter defense, CareConnect will deploy a Cisco Firepower NGFW at the network edge, as shown in Figure 1 at device A. In addition to perimeter security, the Cisco Firepower can perform DHCP (Dynamic Host Configuration Protocol) which automatically

assigns IP addresses to devices on the network, Network Address Translation (NAT) which allows devices in a private network to access external networks, using a public IP address, and Virtual Private Network (VPN) services, making it a cost-effective solution by combining multiple networking tasks into a single device.

The Cisco Firepower will also host the clinic's Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). An IDS inspects network traffic for signs of malicious activity, while an IPS expands on this by actively blocking or dropping harmful packets in real time [3]. We recommend using Snort, since the Cisco Firepower uses it as its core inspection engine. Snort is an open-source IDS/IPS that uses a large library of signature based rules to identify known threats and can block suspicious behavior based on configuration[8]. The current CareConnect network only uses an IPS at the endpoints, and does not include any network-based IDS/IPS to inspect traffic as it traverses the network, so the addition of a network-based IDS/IPS will be a huge improvement to the CareConnect network.

Secure Remote Connectivity (Tommy)

For a modern day healthcare clinic, one of the notable requirements is to have data be accessible from remote locations, but invisible from the public internet. A VPN will be required to create encrypted tunnels over the open internet,ensuring confidentiality and integrity for data in transit. This is critical for connecting the other CareConnect branches together, as well as having access to the off-site backup servers. Without a VPN, the transmission of Protected Health Information (PHI) between sites would travel in plaintext, or a weaker encryption standard, which is a clear violation of HIPPA [13].

Wireguard and OpenVPN have emerged as popular "state-of-the-art" VPN alternatives to traditional protocols. Wireguard is a modern, high performance, protocol[30] running in operating systems kernel space over UDP. Its lightweight code base allows for fast connection and low latency, which makes it a favorite for software-based servers. Alternatively, OpenVPN relies on the OpenSSL library (SSL/TLS) and it operates in the "user space" [7]. It is highly flexible, and can disguise VPN traffic as standard HTTPS web traffic, allowing users to get access to the internal network in more public places.

However, for CareConnects specific infrastructure, we have decided to use IPsec (Internet Protocol Security) as our standard for Site-to-Site connections.While WireGuard is faster in a pure software environment, it lacks hardware optimization on our chosen equipment. The Cisco Firepower and Catalyst devices are equipped with specialized Application-Specific Integrated Circuits (ASICs) designed to offload AES-256 encryption processing directly to the hardware. This allows IPsec to operate at high speed without putting extra load on the router's main CPU, guaranteeing consistent bandwidth for medical imaging, PHI data transfers, and VoIP calls.The use of IPsec also fits our off-site backup strategy. It provides a persistent, always-on tunnel that ensures automated nightly backups execute without the session timeouts, which are common with software-based VPNs.

Security Visibility (Tommy)

With perimeter security and our IDS/IPS defined, we now turn to the final component of our security: visibility. Because the CareConnect network generates logs from many different sources, such as the IDS/IPS, firewall, core switch, and endpoints, we will need to implement a Security Information and Event Management (SIEM) system. A SIEM is a solution designed to collect and analyze security related data across various sources from our IT infrastructure [31]. Currently, the cybersecurity industry standard is shifting toward using a Security Orchestration, Automation, and Response platform (SOAR) , which not only detects threats but takes action to stop them, like automatically banning an IP address on the firewall with no human intervention.

A full SOAR system is complex and costly for the size of CareConnect, so we have decided to use an on-premise SIEM hosted on the main server. We considered several applications to fill this role, such as LogRhythm, IBM QRadar, and Splunk. LogRhythm has some SOAR features built-in and is more geared toward incident response, but generally has less flexibility and customization compared to others. QRadar is more hardware intensive than the others and requires a dedicated server due to its own Linux distribution and technical dependencies. Splunk is widely considered the most premium option, but it also comes with a higher cost. However,

Splunk has a very good reputation, and its ability to index raw data creates a perfect audit trail. It is also highly flexible, and most devices have a log forwarder designed for it.

We recommend Splunk Enterprise for its superior reliability and audit reporting. To manage costs, CareConnect will utilize a capped license model, restricting ingestion to critical security logs. This strategy secures the Role-Based Access Control (RBAC) and six-year log retention required for HIPAA compliance, ensuring data is preserved without the cost of a full-scale enterprise deployment.

Compliance (Dylan)

The Health Insurance Portability and Accountability Act (HIPAA) sets national standards for protecting Protected Health Information (PHI) [5]. These standards explain that PHI needs to not be shared with anybody other than the patient or intended recipient. While HIPAA does not specify any specific standards directly related to computer infrastructure, it is important to ensure that infrastructure is secure so the clinic does not get penalized for failing to protect PHI. Penalties for improper handling of PHI can range from large fines to a complete clinic shutdown. [9] [17] [25]

The Health Information Technology for Economic and Clinical Health (HITECH) Act is an addition to HIPAA being more specific towards electronic data. There are a few specific standards that are necessary to understand when dealing with CareConnect's computer infrastructure. The first is that data encryption is mandatory when in storage and transfer. Next, CareConnect needs to have breach notification systems in place [22]. It is required that if data is breached in any way, patients need to be notified of the breach along with the affected information. For accessing health information, HITECH requires that patients have 24/7 secure access to their health data. It is also required that both patients and clinical staff need to use safeguards such as multi-factor authentication (MFA) for accessing the Electronic Health Record (EHR) system [2]. Audit logs must be available showing who accesses information and when. It is also required that there needs to be full backups of all health data available if needed. These backup systems follow the same security regulations as any other. The last major standard that CareConnect needs to be aware of is proper disposal of old equipment. It is required that procedures need to be in place when doing so. [25] [26]

Fault Tolerance (Tommy)

Fault tolerance refers to the ability of our infrastructure to continue operating when one or more components fail. The goal is to remove as many single points of failure and ensure high availability of critical services. A common strategy to enable fault tolerance is the use of Redundant Array of Independent Disks (RAID) storage. To decide the best strategy for storage, we looked at several RAID configurations. To start, RAID 0 splits data across several drives for maximum speed, but in this configuration, there is zero redundancy. RAID 1 is creating an exact copy of the drives. Which is good for redundancy, but is less efficient because you need double the drives and only can use half the storage. RAID 5 splits data across all drives, but decreases write speeds and rebuilding a failed drive can take a large amount of time [11]. In RAID 10, just like in RAID 1, you lose 50% of the storage capacity, but you require double the hardware.

For CareConnect, we will use RAID 1, as it provides the highest reliability for a smaller server, and fits CareConnect needs. Fault tolerance can be further reinforced through a well developed DRP (Disaster Recovery Plan) and BCP (Business Continuity Plan), along with documentation of hardware configuration and installation as it is important to ensure plans are aligned with future goals [1].

Along with the usage of RAID, we will use Data Loss Prevention (DLP) to keep information safe, private, and compliant with rules like HIPAA. Data Loss Prevention works by watching sensitive data and making sure it gets into the right hands and is not lost or stolen. It also monitors data on devices, networks, and cloud services and can block and encrypt sensitive information while alerting the IT staff of any problems [27]. Our staff will be trained to make sure Data Loss Prevention will add safeguarded servers, staff laptops, and the VPN to monitor data transfers and prevent data loss during transfers. CareConnect will also enforce access controls to encrypt sensitive files, and restrict data only to authorized staff. They would be alerted in the instance of potential violations and leaks as it is important to quickly assess the legitimacy and potential damage caused.

Privacy-Based Web Security (Peter)

CareConnect will use web filtering to block access to unsafe and inappropriate websites on both staff and guest devices. This will help prevent breaches through malware and phishing. CareConnect requires VPN and Data Loss Prevention (DLP) to ensure sensitive information stays confidential. The star topology network design and VLAN segmentation will limit who can access patient data. Regular staff training and testing will reinforce practice of handling records. Staff are prepared and know about cyber attacks involving social engineering or phishing. Encryption will also be used to prevent unauthorized access to data and devices. The IT room will contain temperature sensors and a motion activated camera to rule out physical tampering. Security measures include 802.X authentication, MFA for remote access, and data encryption [4]. DLP will also be implemented to enforce access controls to encrypt sensitive files, restrict data only to authorized staff, and alert for potential violations and leaks. Staff training will also cover security. IT personnel will be monitoring systems regularly to ensure automatic threat detection software isn't missing anything.

Infrastructure Scalability (Peter)

Infrastructure Scalability allows network growth as CareConnect adds staff, devices, and additional services. Our server rack also has plenty of room for numerous devices to be added. Additionally, our star topology layout supports growth because all our devices are connected to a central switch making it easy to add new equipment and devices without redesigning our entire network layout. We have plenty of ethernet cable length to plug every device in and have extra in case some breaks in the setup process or in the future due to unusual circumstances.

Design

CareConnect WAN (Dylan & Tommy)

CareConnect operates branches in Romeoville, IL, and St. Louis, MO, with Chicago, IL serving as the headquarters. Following best practices to place main equipment in the central city [20], Chicago acts as the hub, hosting all critical services such as EHR, file servers, authentication, and backups. This location houses powerful networking equipment, including a Cisco Firepower 1010 and Cisco Catalyst 9300 for Layer 2 switching and VLAN segmentation across EHR/PHI, staff, and guest networks. Two Cisco UCS 240 M6 servers configured with VMware are used here to host virtualized EHR, file/print, and Active Directory/DNS services. Meanwhile, Romeoville and St. Louis branches each support 15 staff members requiring EHR and file sharing access. These locations utilize a VPN tunnel to connect to Chicago, relying on a local Cisco Firepower 1010 to act as the firewall, NAT gateway, and VPN spoke, alongside a Cisco Catalyst switch for VLAN mirroring and local DHCP services. The branch firewalls (Firepower 1010) connect to Chicago. They use an IPsec VPN, and static routes, shown in figure 3. The reason for using IPsec opposed to OpenVPN or Wireguard is mainly because of the stability and standardization. IPsec is also built into most operating systems, so there is no need for third-party applications. This native support makes it easier for IT to deploy and manage [24]. QoS prioritizes EHR/Voice services, and limits guests. Each site has its own ISP, which terminates at the Firepower 1010. Local breakout for normal web traffic, and business traffic using shared apps will use the VPN.

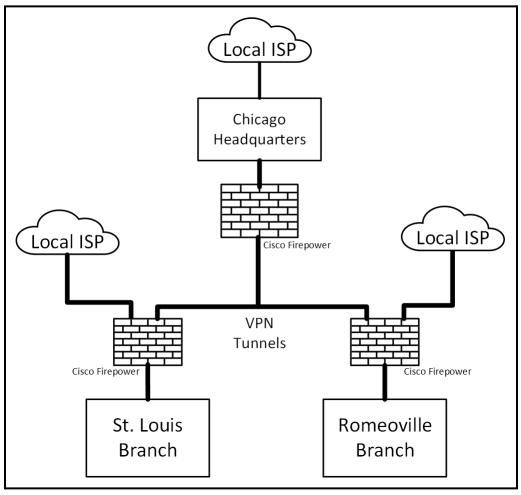

Figure 3. Branch infrastructure topology map, showing all business traffic routed through IPsec VPN tunnels to the Chicago HQ, and each site having its own ISP connection.

The *NIST Cybersecurity Framework* is used as a model for risk management. The framework is a great reference when it comes to protecting and recovering from cyber threats as it includes strategies and techniques to keep up with industry standards. Security measures include Cisco firewalls, VLAN segmentation, 802.X authentication, MFA for remote access, and data encryption [15] [19]. DPL will also be implemented to enforce access controls to encrypt sensitive files, restrict data only to authorized staff, and alert for potential violations and leaks. Staff training will also cover security as human error is the largest cause of cybersecurity breaches [16]. Patients will be encouraged to take free training courses on protecting their own health information as they may not be knowledgeable about such attacks [18]. IT personnel are monitoring systems regularly to ensure automatic threat detection software isn't missing anything [21]. In the worst-case scenario, there exists backup equipment with all data in Chicago. This backup data will need to be used in the cases of data deletion or ransom.

Network Infrastructure Design (Dylan):

Wiring for all equipment will run through the drop ceiling with cat6 ethernet cable. For desktop computers. printers, and phones, these cables will drop down through the ceiling along the wall where they can then be plugged into the hardware. This completely replaces the old network with a new network that will be set up prior to disabling and removing the old network. Drilling holes and wiring will be completed outside of business hours to ensure no physical interruption to staff or patients. At completion, all important data transfers to the new equipment. When data is transferred over, old hard drives must be shredded and taken to Will County's Free Electronic Drop-Off [12]. This allows a smooth transition and eliminates recycling concerns.

As seen in *Figure 1*, new computers will go in place, each with a phone. Three for reception, five total for exam rooms (one in each), one for the admin, two for billing/records, three for clinical staff, four for IT, and one in

the server room. All computers, printers, WAPs and phones will be hardwired directly to the switch in the server room. Clinical and IT staff will also have laptops which will be connected via WiFi through the wireless access points throughout the office (shown as green circles in *Figure 2*). Staff with laptops will also be able to connect to CareConnect's network through the VPN when working remotely.

All switches, firewalls and server equipment will be behind two additional lockable doors from the outside door. To access this equipment, you have to go through a door in the staff room (where clinical staff like doctors and nurses will be doing work from when not seeing patients) to the IT room, then a door into the server room. The IT room will contain temperature sensors and a motion activated camera [23] to support root cause analysis and rule out physical tampering.

Configurations (Thomas)

The network is configured with a Cisco Firepower firewall and a Cisco C9300 24P E core switch. Each VLAN on the core switch including Clinical VLAN 10, Admin VLAN 20, Guest VLAN 30, and Voice VLAN 40 has its own subnet and connects to a dedicated firewall interface. The Firepower outside interface connects to the ISP router which routes traffic to the off site router providing connectivity to the backup server. A dedicated Voice router manages the Call Manager and provides DHCP services for the Voice VLAN. Static routes are configured on both ends to enable communication between the local and off site networks. The Firepower and off-site router use AES encryption and SHA hashing for the IPsec VPN secured with a pre-shared key. Each device has configured default gateway and DNS settings to support.

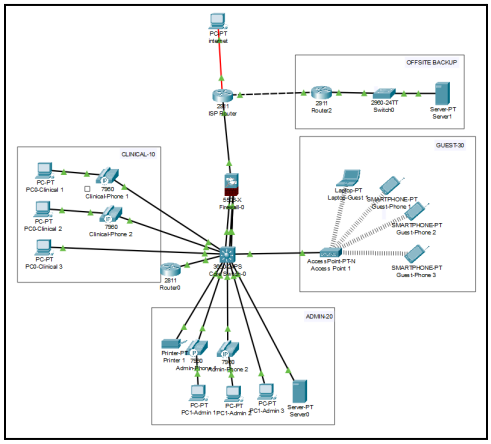

Figure 4. Network simulation in Cisco Packet Tracer

ACLs define permitted traffic between VLANs and enforce the security rules for each subnet, shown in figure 4 Clinical and Admin VLANs are permitted to reach shared internal services and the internet, while the Guest VLAN is restricted to outbound internet-only traffic. The Voice VLAN is limited to SIP, SCCP, RTP, DHCP, and TFTP traffic needed for phone registration and call control, with all other inbound traffic denied. NAT is disabled for VPN bound traffic and enabled for general outbound traffic. Each device has configured default gateway and DNS settings to support internal communication and external access.

Our configured network can be seen in *Figure 4*. There is an admin, guest, and offsite backup VLAN. The moving pink envelopes represent the packets traveling between devices and demonstrates traffic flow across the VLANs. As seen in Figure 4.2 below, an acceptable packet is being allowed to pass through the firewall while an unwanted packet is being blocked.

```
ciscoasa(config)#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-
interval 300
access-list GUEST-IN; 3 elements; name hash: 0x253e2729
access-list GUEST-IN line 1 extended deny ip 10.1.30.0 255.255.255.0 10.1.10.0
255.255.255.0(hitcnt=0) 0x7a699bc6
access-list GUEST-IN line 2 extended deny ip 10.1.30.0 255.255.255.0 10.1.20.0
255.255.255.0(hitcnt=0) 0xd8d41c2e
access-list GUEST-IN line 3 extended permit ip any any(hitcnt=0) 0xaa4cb3dc
access-list INSIDE-OUT; 1 elements; name hash: 0x7ad6ea2c
access-list INSIDE-OUT line 1 extended permit ip any any(hitcnt=0) 0xd94bcb74
access-list ADMIN-OUT; 1 elements; name hash: 0xcaae3b0b
access-list ADMIN-OUT line 1 extended permit ip any any(hitcnt=6) 0xdb32cd2d
access-list GUEST-OUT; 1 elements; name hash: 0xeb5633e4
access-list GUEST-OUT line 1 extended permit ip any any(hitcnt=4) 0x81054806
access-list VPN-ACL; 1 elements; name hash: 0x5312c3d3
access-list VPN-ACL line 1 extended permit ip 10.1.10.0 255.255.255.0 198.51.100.0
255.255.255.0(hitcnt=0) 0xb929ceb7
access-list NO-NAT; 1 elements; name hash: 0x33318001
access-list NO-NAT line 1 extended permit ip 10.1.10.0 255.255.255.0 198.51.100.0
255.255.255.0(hitcnt=0) 0x806aa944
access-list OUTSIDE-IN; 2 elements; name hash: 0x3a6a6345
access-list OUTSIDE-IN line 1 extended deny tcp any any eq www(hitcnt=0) 0x55a91616
access-list OUTSIDE-IN line 2 extended permit ip any any(hitcnt=0) 0x51932244
ciscoasa(config)#
```

Figure 4.1. A screenshot of the firewall's access control lists

Methodology (Tommy)

To build and verify our network design without the need of having access to the expensive physical equipment, we utilized Cisco Packet Tracer. This software acts as a lab where we can drag and drop routers,

switches, firewalls, and other network devices to create a functioning topology. Beyond just mapping out the physical layout of devices, Packet Tracer allows us to configure them using the actual Cisco command-line interface, and run traffic simulations to see how data moves through the systems in real-time. This software gives us a risk-free 'sandbox' environment to test our VLANs, routing protocols, and security rules, ensuring that our configuration is solid before we commit to a final deployment.

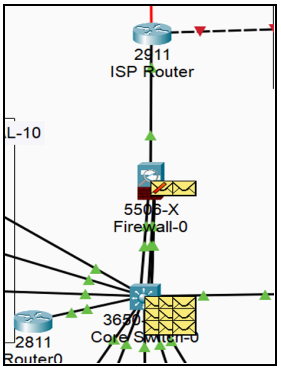

Figure 4.2. Malicious packet stopped by firewall

Evaluation Scope (Tommy)

To evaluate the proposed network, we will focus on testing how traffic moves through the network using Cisco Packet Tracer's Simulation Mode. This tool will be used to follow packets sent through the simulated network and confirm that our design is working. End-to-end connectivity testing will be performed by sending traffic between devices on different VLANs. These tests will examine VLAN separation. Firewall testing involves sending both allowed and blocked traffic toward the firewall to observe how access rules affect packet flow. Switch behavior will be examined by watching the MAC address table while traffic is moving through the network. This will allow us to observe how the switch handles and tracks active devices. Network traffic will also be observed during simulations to look for delays, congestion, or unusual behavior. Wireless testing will include sending traffic over air, and confirming packets reach the wireless devices successfully. Signal range and device connectivity will be observed to evaluate wireless coverage across the network area.

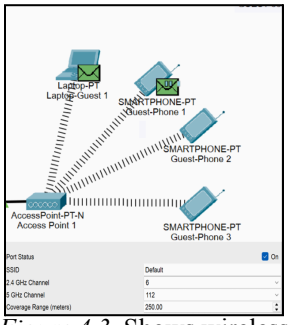

Figure 4.3. Shows wireless connectivity and successful packets.

Experimental Results (Dylan, Peter)

To test packet flow and performance of our topology, we used simulation mode in Cisco Packet Tracer. We did this to ensure that our network functioned correctly and our VLANs can move traffic and communicate with each other. Figure 4 shows our simulated topology and connectivity.Figure 4.2 shows that our firewall is doing its job of blocking unauthorized traffic and letting authorized traffic through. A test was performed where two packets were sent towards the firewall. One packet was blocked while the other packet was allowed through. This shows that our firewall is enforcing access control list rules and blocking unauthorized traffic. The access control list for the firewall can be seen in Figure 4.1.

Figure 4.3 is our wireless network test that shows our wireless connection is working and receiving packets. It also shows that 2.4GHz and 5GHz are active. The coverage range indicates 250 meters demonstrating strong and reliable coverage around the clinic.

We monitored our core switches MAC address table during the simulation on packet tracer. While traffic

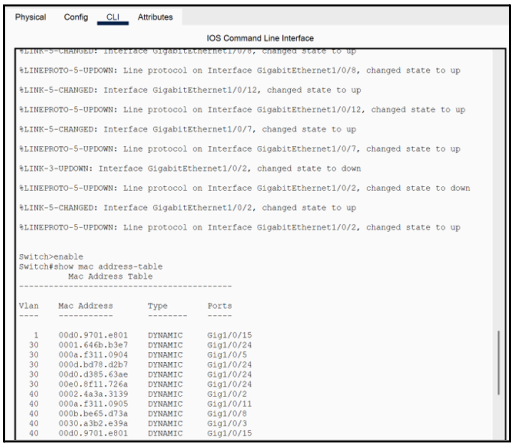

Figure 4.4. A screenshot of the core switches mac address table. New traffic is correctly showing up and the switch is logging it.

was moving, new MAC addresses showed up in the table. Even though they appeared on the same port, it showed the switch was keeping track of the traffic, shown in figure 4.4. Based on the MAC table, this confirms that our core switch was correctly learning devices and understanding traffic.

We also tested and ensured packets could be sent to our offsite backup location which can be seen in Figure 4.5. This means that if there is an emergency, CareConnect should be able to access the data from the offsite backup.

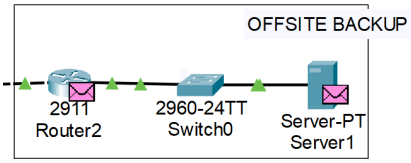

Figure 4.5. Packets reaching the off-site backup location.

General User Training (Thomas, Dylan)

Staff Training will help prevent mistakes and ensure CareConnect's proper operations along with protection from cyberthreats. General training for all employees will consist of teaching on spotting and reporting phishing and social engineering cyber attacks. It will also consist of learning about HIPAA and how to properly handle PHI. MFA will also be utilized, so staff will be debriefed on using this effectively. Clinical staff will be shown how to connect to the VPN properly by IT. All staff will also learn how to avoid unsafe practices such as sharing files over guest WiFi or using weak passwords. Connecting personal devices to the main network is also not allowed and must be connected to the guest network. Staff will also be updated regularly from IT on newest cyberattack trends and defence practices. Staff should also be quizzed on a regular basis to prove understanding of training [14].

IT Administrator Training (Thomas, Dylan)

All equipment is listed in the *Equipment Cost Breakdown* below. The 2D top-down map (*Figure 1*) shows where equipment will go. The physical topology map (*Figure 4*) can be helpful for determining what plugs-in to what, though it is relatively straightforward. Wiring is not shown, but can be routed through the drop-ceiling to each component.

For setting up the firewall, GigabitEthernet port 1/1 plugs-in to the ONT, while any of the remaining ones can plug-in to the core switch. For accessing all configuration settings properly, a license will be required [28]. To add a new port to the firewall, you will need to run the following commands in order: *enable* | *configure terminal* | *interface (interface name)* | *nameif (name based on role)* | *ip address (ip address)* | *security level (value)*. To confirm the correct port was added, use *vlan brief*. To block unwanted sites, this can be done through its *Access Control Policies*. From here, you can create rules by category. These rules will be applied to all devices, so there is no need to worry about trying to create different groups. Downloads are not allowed unless given permission from the IT department. Entertainment, gambling, and social media sites along with sites that are known for phishing and malware will be blocked for obvious reasons. Custom sites can also be added to the filter however, the categories get updates regularly from Cisco and should serve as substantial protection.

To add a workstation to the network, assign it to the appropriate VLAN on the core switch and ensure the switch's port is configured as an access point for that VLAN. The workstation can use DHCP to automatically receive its IP address, subnet mask, default gateway, and DNS from the firewall serving that VLAN. Once connected, the device should be able to communicate with other allowed systems based on the firewall's ACLs. No additional configuration is required other than plugging the workstation into the properly assigned port and confirming it receives the correct network settings.

Setting up a VoIP phone involves connecting it to a switch port that is configured for *both* a data VLAN and a voice VLAN. The switch port must be set as an access port for the user's data VLAN and assigned a voice VLAN using the *switchport voice vlan* command. When the phone powers on, it receives an IP address from the DHCP server for the voice VLAN, along with its Call Manager information from the dedicated router. The phone then downloads its configuration files from the Call Manager, registers to the system, and becomes ready to place and receive calls. If a workstation is connected through the phone, it will receive an IP address from the data VLAN while the phone remains on the voice VLAN, allowing both devices to operate correctly on the same physical port.

For configuring the core switch, make sure it is in configuration mode, create VLANs 10, 20, 30, and 40. Name them according to the device groups for easier identification. From here, ports can be configured to use one of these VLANs depending on the type of device. A full configuration guide can be found here. After making changes, brief them to ensure devices are given the correct VLAN.

Conclusion

CareConnect's current network suffers from several weaknesses, including a lack of network segmentation, no redundancy, and aging equipment. These issues create compliance risks, reliability concerns, and potential data loss. The proposed design addresses these problems by implementing VLAN-based segmentation, a next-generation firewall that will also host a VPN, our IDS/IPS, and handle perimeter security. Along with these, all user devices will be replaced. The proposed design will strengthen security, improve reliability, and help keep the clinic compliant with HIPAA guidelines. Our team recommends that CareConnect moves forward with the new design in phases, to minimize downtime. The new infrastructure should start being implemented as soon as possible, to avoid any further risk.

Appendix

Equipment Cost Breakdown (Dylan):

Category	Device / Item	Qty	Total Initial Cost	Yearly Power	Power Cost
Network	Cisco Firepower 1010	1	$710.77	262.8 kWh	$39.42
	Cisco C9300-24P-E Switch	2	$8,299.98	3,504 kWh	$525.60
	Cisco Aironet 1852I APs	3	$1,185.00	236.4 kWh	$35.46
	Cisco Catalyst 8200 Router	1	$1,302.99	262.8 kWh	$39.42
Server Room	Cisco UCS 240 M6 Server	2	$4,598.00	14,000 kWh	$2,100.00
	APC NetShelter SX 42U Rack	1	$2,723.52	*N/A*	*N/A*
	APC Smart-UPS 1500VA	1	$700.00	228 kWh	$34.20
	APC Rack Air Removal Unit	1	$3,422.28	10,512 kWh	$1,576.80
Endpoints	Dell OptiPlex 3030 Desktop	20	$19,980.00	4,672 kWh	$700.80
	Dell XPS Laptop	10	$14,597.60	730 kWh	$109.50
	Dell 27 Monitor (SE2725HM)	20	$2,799.80	952 kWh	$142.80
	Yealink SIP-T54W VoIP Phone	20	$1,599.80	480 kWh	$72.00
	Epson EcoTank Pro ET-16650	2	$2,319.98	166.4 kWh	$24.96
Misc	Cat6 Cabling (1000ft Spool)	2	$407.98	*N/A*	*N/A*
Fees & Tax	Shipping, Tax	1	$2,669.56	*N/A*	*N/A*
Services	ISP Service	1	*N/A*	*N/A*	$3,147.43
	Backup Server Colocation	1	*N/A*	*N/A*	$4,788.00
Personnel	IT Systems Administrator	4	*N/A*	*N/A*	$400,000.00
TOTALS			***$67,317.26***	***36,006.4 kWh***	***$413,336.39***

Team Contributions

- Tommy
    - Network topology and research
    - Created topology graphics
    - Developing VLAN structure
    - Planning Configurations
    - VPN and off-site backup configuration
    - Simulated network topology in Cisco Packet Tracer
- Peter
    - Responsible for ensuring project requirements were met
    - Ensuring infrastructure is up to HIPAA standards
    - Explained topology & configurations
    - Testing of the topology
- Dylan
    - Researched equipment for physical infrastructure components
    - Calculated electricity usage for equipment and total costs
    - Created a top-down 2D site map
    - Helped plan physical topology of site
    - Edited milestone based off instructor suggestions

References

[1] DiDio, L. (2025, January 23). How to start your healthcare organization's infrastructure modernization journey. HealthTech Magazine. https://healthtechmagazine.net/article/2025/01/how-start-your-healthcare-organizations-infrastructure-modernization-journey

[2] U.S. Department of Health & Human Services. (n.d.). HIPAA security series #4: Security standards-Technical safeguards. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

[3] NetSecCloud. Cisco Firepower IDS vs. IPS: What's the difference? http://netseccloud.com/cisco-firepower-ids-vs-ips-what-s-the-difference

[4] Okta. (2023, September 2). Why multi-factor authentication (MFA) is important. Okta Identity 101. https://www.okta.com/identity-101/why-mfa-is-everywhere/

[5] U.S. Department of Health and Human Services. Summary of the HIPAA privacy rule. HHS.gov https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[6] Sheehan, Jerry. "Star Topology Explained: Network Layout Essentials - SynchroNet." SynchroNet, 9 Mar. 2025, synchronet.net/star-topology/#Why_Its_Popular_in_Modern_Networking Accessed 22 Sept. 2025.

[7] Palo Alto Networks. (n.d.). IPsec vs. OpenVPN. Cyberpedia. https://www.paloaltonetworks.com/cyberpedia/ipsec-vs-openvpn

[8] Roesch, M. (1999). Snort -Lightweight Intrusion Detection for Networks. Retrieved from https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf?

[9] HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information. (2025, January 6), from Federal Register website: https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information?

[10] Absar, N., Jahangir Alam, M., & Ahmed, T. (2014). Performance Study of Star Topology in Small Internetworks. International Journal of Computer Applications, 107(2), 45–53. https://research.ijcaonline.org/volume107/number2/pxc3899961.pdf

[11] Sivakumar, P., & Devi, K. (2015). A review on RAID levels implementation and comparisons. Australian Journal of Basic and Applied Sciences, 9(21), 86–91. https://www.ajbasweb.com/old/ajbas/2015/Special%20ICEAS/86-91.pdf

[12] Will County Land Use Department. (2025, August 6). Electronic Information - Will County Green. Will County Green. https://www.willcountygreen.com/greenguide/electronic.aspx

[13] Ibrahim, R., Ibrahim Khider, Salaheldin Edam, & Mukhtar, T. (2025). Comprehensive Strategies for Enhancing SD‐WAN: Integrating Security, Dynamic Routing and Quality of Service Management. IET Networks, 14(1). https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ntw2.70007

[14] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176. https://www.sciencedirect.com/science/article/abs/pii/S016740481300179X?via%3Dihub

[15] U.S. Department of Health & Human Services. (2023). Health Industry Cybersecurity Practices (HICP): Technical volume 2. HHS 405(d) Program. https://405d.hhs.gov/Documents/tech-vol2-508.pdf

[16] Clearwater Security. (2024, March 15). Effective security measures for healthcare organizations: 6 best practices every healthcare organization should know. Clearwater Security. https://clearwatersecurity.com/blog/6-security-measurement-best-practices-every-healthcare-organization-should-know/

[17] Marron, J. (2024). Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

[18] American Hospital Association. 2023. The importance of cybersecurity in protecting patient safety. American Hospital Association. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

[19] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[20] RunCloud. (2023, June 1). Choosing the ideal server location & does it even matter? RunCloud Blog. https://runcloud.io/blog/ideal-server-location

[21] Centraleyes. (2024, May 6). Manual vs automated risk management: What you need to know. Centraleyes. https://www.centraleyes.com/manual-vs-automated-risk-management/

[22] Burde, H. (2011). The HITECH Act: An overview. AMA Journal of Ethics, 13, 172-176. https://journalofethics.ama-assn.org/article/hitech-act-overview/2011-03

[23] Avelar, V. (n.d.). Practical Options for Deploying Small Server Rooms and Micro Data Centers. Retrieved from https://media.zones.com/images/pdf/White_paper_APC_Practical_options.pdf

[24] Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). Guide to IPSec VPNs (NIST Special Publication 800-77 Revision 1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf

[25] U.S. Department of Health and Human Services. (n.d.). HIPAA for professionals. Retrieved from https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

[26] U.S. Department of Health and Human Services. (n.d.). HITECH Act enforcement interim final rule. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf

[27] Palo Alto Networks. What Is DLP (Data Loss Prevention)? Cyberpedia. https://www.paloaltonetworks.com/cyberpedia/what-is-data-loss-prevention-dlp

[28] Cisco Systems. (2023). Configuring VLANs (Catalyst 9300 Series Switches, IOS XE Release 17.17. Cisco. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-17/configuration_guide/vlan/b_1717_vlan_9300_cg/configuring_vlans.pdf

[29] Jiang, R. (2015). A review of Network Topology. Proceedings of the 2015 4th International Conference on Computer, Mechatronics, Control and Electronic Engineering. https://www.atlantis-press.com/article/25839746.pdf

[30] Master, A., & Garman, C. (2021). A WireGuard Exploration. *CERIAS Technical Reports*. https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1000&context=ceriastr

[31] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21*(14), 4759. https://www.mdpi.com/1424-8220/21/14/4759