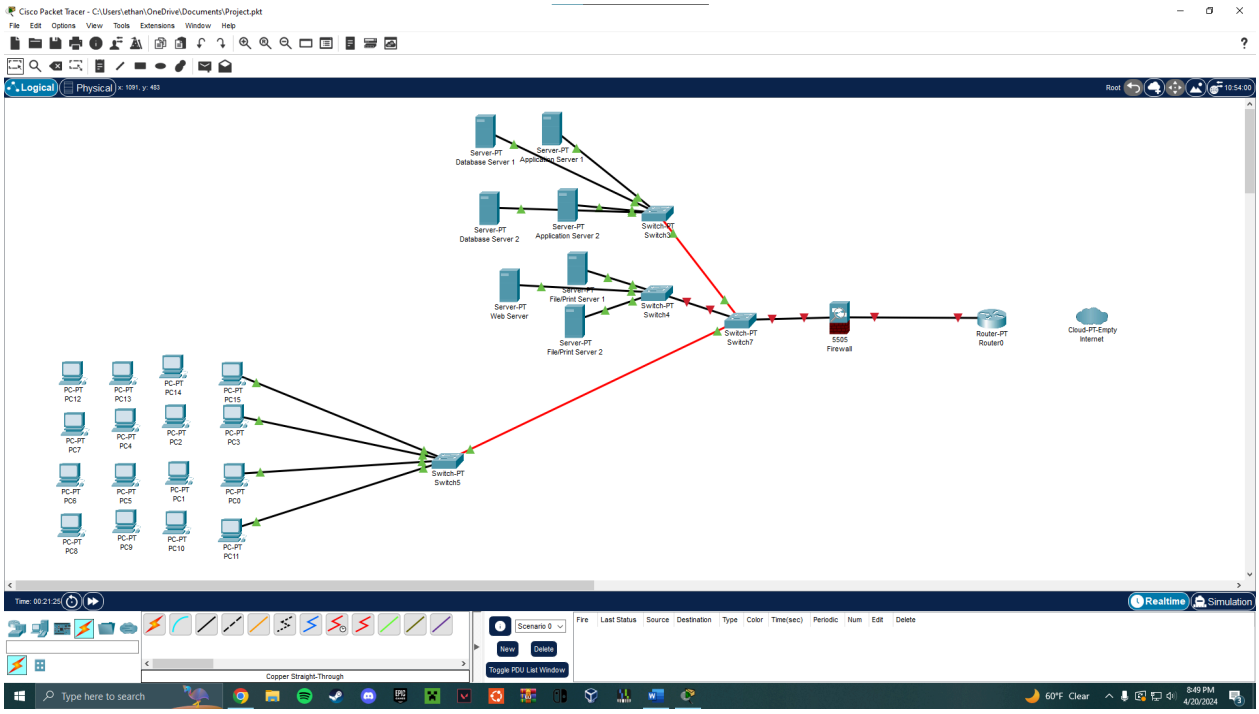
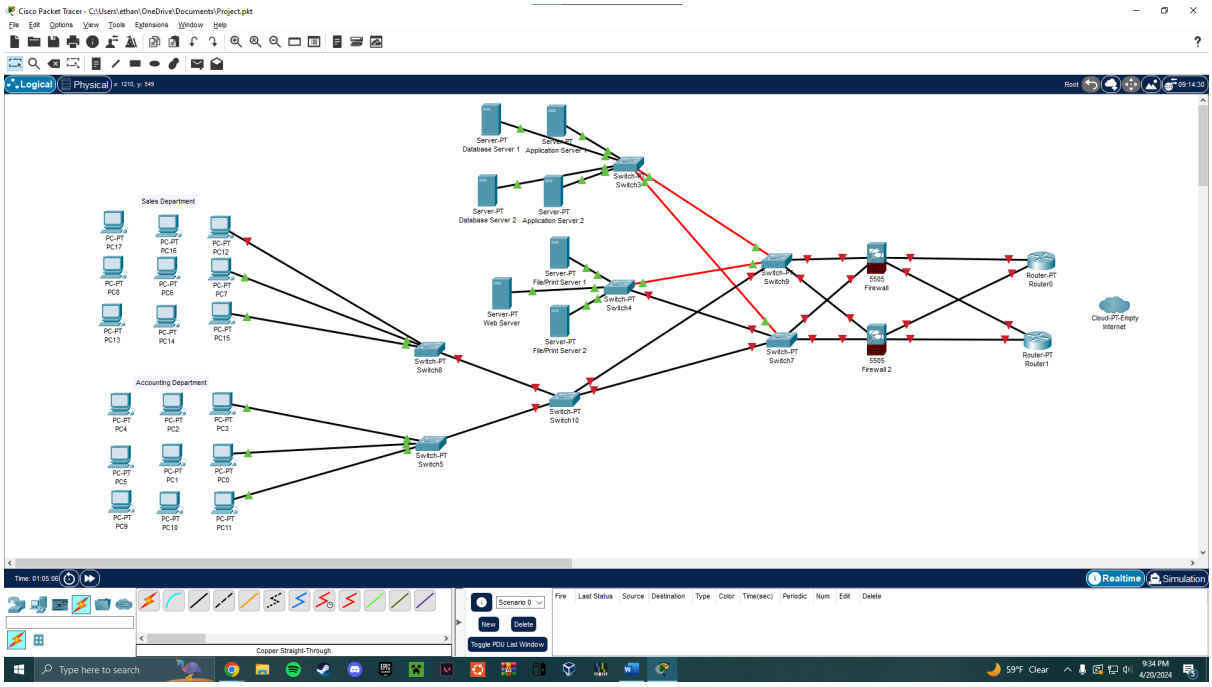
Part 1: Network Design



Above I made a design of the current network that is being used at the Corporation Tech's company. The senior network architect wants me to rebuild their infrastructure and topology to make it more modern, redundant and efficient, and also wants me to add logical separation between departments. Currently, the network has 3 main switches, one with workstations, one with the web/file servers, and one with all the database and application servers. These switches connect to another switch, which goes into a single firewall, into the router, and out to the web. It's quite basic at the moment, which is why the senior architect wants me to redesign it.

My main plan to implement the requests is to have 2 switches connecting all the workstations together. One switch will connect all the computers for the accounting department, and the other one will connect all the computers for the sales department. I also want to add backup switches behind every individual switch in case one fails. There is also a need for redundant communications at the firewall and router level, so I will add an extra firewall and extra router and interconnect them so if one breaks down, the other will take its place.

The network architect also wants me to recommend if they should keep using IPv4, or upgrade to IPv6. Realistically, I think it comes down to how recent their current networking equipment and servers are. If they're old, then the company might have to stick with IPv4, but if it's newer then it's still up for debate. Personally, I would recommend upgrading to IPv6 for the main purpose of future proofing their network. They're probably paying a lot of money to redesign it right now, and it would be better in the long run to upgrade now instead of waiting for when IPv4 becomes outdated and they have to spend more money to update their infrastructure again.



Here is my finished design of what Corporation Techs wanted me to add to their network. It incorporates everything I had in my plan, which was the switches to separate the sales and accounting departments, and the redundant switches, firewall, and router.

Sources:
https://help.ui.com/hc/en-us/articles/360006836773-Addressing-Loops-and-Managing-Redundancy-STP

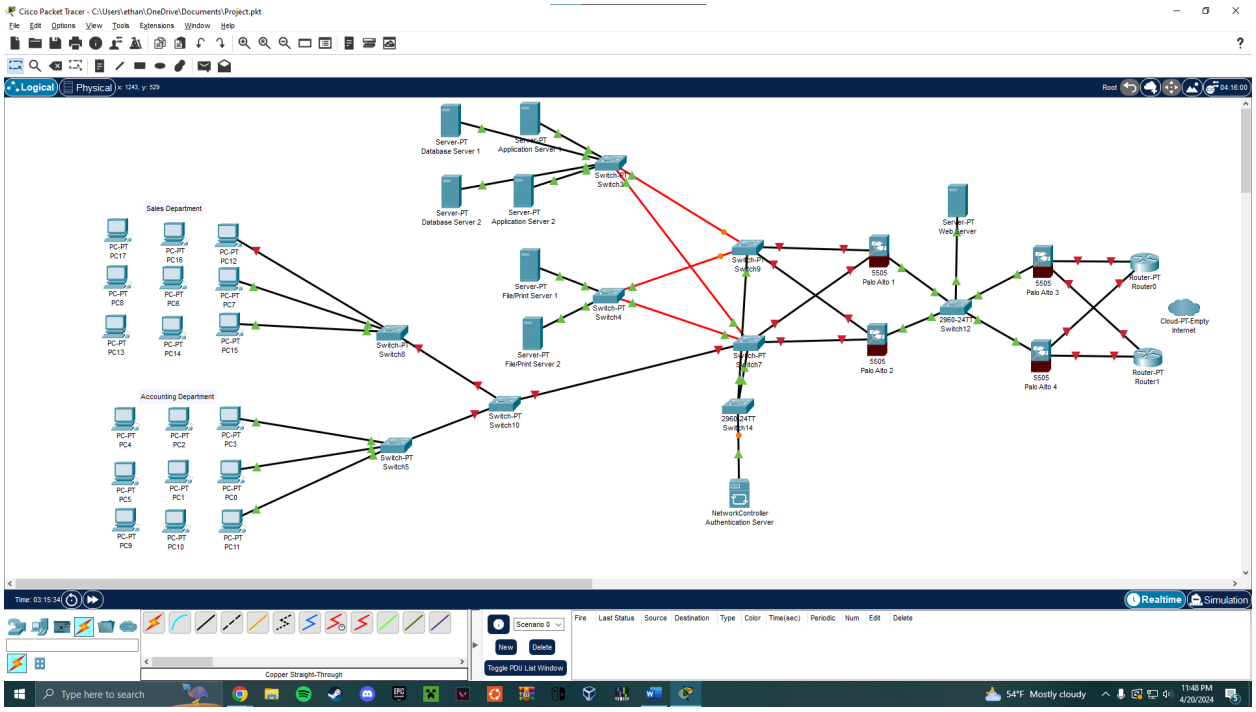
https://www.alliedtelesis.com/us/en/white-paper/easing-enterprise-transition-ipv6#:~:text=The%20Internet%20is%20a%20global%20entity&text=Not%20being%20IPv6%2Dready%20can,to%20be%20accessible%20by%20IPv6.

Part 2: Firewall Selection and Placement

For the 2nd part, the senior network technician wants me to upgrade the firewall and create a demilitarized zone to separate the internal network from the web servers. The DMZ should increase the security of the network by having the web servers behind one firewall, and all the other networking equipment behind another. First I had to research a firewall and the big 3 names I kept seeing were Palo, Fortinet, and Cisco. I thought Cisco would be the most obvious choice to go with, but when I looked into it, it seemed like Palo Alto currently makes the best firewalls on the market. They're easy to manage, flexible, and have a lot of advanced features, so this is the brand I'm going to recommend. The specific firewall I'll pick is the PA-440. It's a next generation firewall that costs around $1,500-$2000 online, which sounds like a good value for a company only running 50 workstations.

To make a strong DMZ for the network, I actually want to use multiple firewalls. One firewall will sit in between the router and web servers, and the other one will be in between the servers and the rest of the internal network. The first firewall will be configured to filter and then send external web traffic to the servers directly behind it. Any traffic that is destined for the main network will be sent through to the second firewall. For this 2nd firewall, it will decide if the traffic is part of a real communication for somebody working in the office, or if it's a malicious attempt to interact with the internal network. It is highly important that this firewall is configured correctly, because if it is not, then it's very likely a hacker will get into the internal network at some point.

For the DMZ to be safe, there needs to be some kind of authentication for the firewall to know who is allowed in and out of the internal network. One method I found for authenticating users is by using multifactor authentication for anybody who's trying to access resources in the internal network. The problem with this method is that it gets complicated to utilize MFA every time you want to access something. Instead my plan for authentication is going to be to use an active directory server that utilizes Kerberos to authenticate devices automatically. The authentication server will be connected to the first two switches of the internal network, and any time a device wants to access an internal server, it will have to prove its identity to the authentication server first and provide that proof to the server it wishes to access.



Above is the updated design of the network. It adds on the authentication server, and a DMZ that houses a switch connecting to the web server. This allows users outside the network to access the web server in a DMZ, securing the network perimeter by avoiding having users connect into the internal network to reach the web server like before.

Sources:
https://www.gartner.com/reviews/market/network-firewalls

https://www.reddit.com/r/networking/comments/xur7sr/what_enterprise_firewall_would_you_go_with_if/
https://www.paloguard.com/Firewall-PA-440.asp
https://en.itpedia.nl/2023/01/28/wat-is-een-demilitarized-zone-dmz/
https://www.redhat.com/en/blog/identity-management-systems-dmz

Part 3: Remote Access and VPNs

For part 3, the senior network architect wants me to find him a VPN and remote service plan so users can access internal resources of the network while they're not in the office. The solution needs to be secure against unauthorized access and not be able to be snooped. In my research, I compared the two best options, which were IPsec and SSL VPNs, and decided that the best option for Corporation Techs is most likely going to be an IPsec VPN.

The SSL/TLS VPN was a good choice, it offered a much easier setup compared to the IPsec, and also used lightweight software so it would've been more compatible with different devices, but the SSL VPN can really only be used for so much. It works at layer 7 of the OSI model, so its best purpose is to help communicate with web applications and other computer programs, but that isn't really what you want for accessing remote network resources. The IPsec VPN works at the network layer of the OSI level and encrypts full IP packets at the network level to ensure security. It is better at connecting networks together because it is encrypting all the traffic, instead of just encrypting specific application data. Yes, it is a little bit more complicated to set up and requires specific user software, but it gives you more options to configure, such as the encryption type and level. The complexity is also somewhat of a benefit, as the simplicity of SSL VPN makes it not effective enough for corporate use.

Some other options for remote access are TeamViewer and Splashtop. Both of these are very similar, and they're applications that run on devices that allow remote access, remote support, and remote control over the internet. These solutions have a cheaper upfront cost and are easier to manage than configuring a whole VPN server, but they do come with disadvantages. Due to the fact that these services are applications, user's are going to be connecting to workstations inside the network and streaming the screens of the computers they're using, which is going to lead to latency and technical issues occasionally. A VPN on the other hand allows you to work locally on your computer, and just download/upload files to the internal servers when you need to. Additionally, while the application route still offers encryption, it won't be as configurable and secure as having a dedicated VPN connection.

In the end, an IPsec VPN setup is going to be the best configuration for the corporation tech's network. The best implementation is to use a VPN gateway, which is a hardware VPN. This device will be able to do all of the traffic encryption and decryption, authenticate clients wishing to connect to the network, log all of the traffic if needed (which it should be), and also route the traffic through the network.

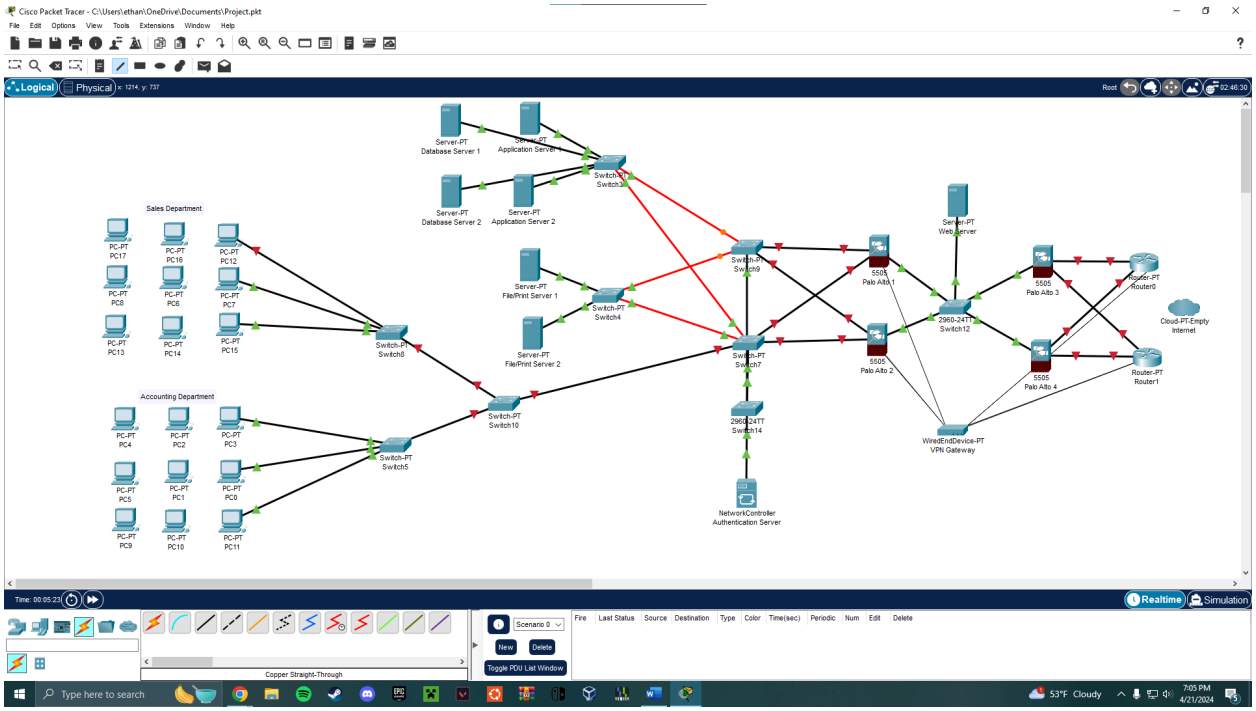
Sources:

https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/#:~:text=The%20IPsec%20protocol%20suite%20operates,of%20directly%20encrypting%20IP%20packets.

https://www.ninjaone.com/blog/secure-remote-access-solutions/

https://www.archonsecure.com/blog/hardware-vpns-are-better-for-remote-access

Part 4: Final Network Design



This is the final network design I created for Corporation Techs. Compared to the original topology, it has several improvements to incorporate new features, enhanced security, and redundancy. The first change I proposed is how to separate all of the workstations into 2 different departments. This one is a simple change, and it just requires adding two new switches for the network. One switch will run the subnet for the accounting department with half of the 50 workstations connected to it, and the other switch will run the subnet for the sales department. With the separation of these two departments, it will be easier to manage the computers when sorting traffic or creating rules for specific users or roles due to the IP ranges being different. It could also increase the potential throughput of the network too because the traffic of 50 workstations will be going through 2 switches now instead of 1.

The second proposal I made was how to manage the creation of a DMZ. My solution for it was to put the web server that outside users access in between 4 firewalls (two are for redundancy). As of right now, when a user goes to access the web server, their traffic enters the internal network where all of the file servers and employees are storing data. This is highly insecure because if a hacker can find a vulnerability in the web server, they can traverse out of that server and potentially start reading confidential data in the company. With the change I'm proposing, the web server will be behind 2 firewalls that allow traffic from the outside through to

the web server, but anything that tries to move past the web server will hit another 2 firewalls that are more strict on what's allowed. Now if somebody hacks their way out of the web server, they can't do much more because they're stuck in the DMZ and the internal network will be protected. The exact firewalls I chose to set up the DMZ are the PA-440, which are made by Palo Alto. This specific firewall is made by one of the best firewall manufacturers on the market right now, and has a good price/performance ratio for the size of this network.

During my changes, I also added a level of redundancy to everything in the network. Previously if just one router, firewall, or central switch goes down, then all the devices on the network will lose connectivity and won't be able to communicate. In my plan, I added a backup router, backup firewalls, and a backup switch to ensure not everything will crash in the event of a hardware failure. The backup devices can actually be used in conjunction with the regular devices, to allow for load balancing for better throughput of data. Now for example, if the network's router completely broke for some reason, the backup router could recognize that and all the data would start going through the redundant router instead, preventing an internet outage. As long as the IT staff can get another router running within a couple days, it will almost guarantee that the whole network will never go down for a power failure. The only equipment I didn't make redundant are the switches for the workstations and internal servers. If one of those switches dies, it will definitely take down the subnet that it's running, but the rest of the network will still be functional. To prepare for the failure of these switches, the best practice would be to have a backup switch with identical configurations ready to be swapped out within minutes of the switch dying. This will also require IT training to prepare for this scenario.

Another change I made was to add an authentication server into the network. Right now, users on the network are trusted to access resources as long as they know the password to get into those resources. Well this is another insecure part of the network because if hackers can get their hands on the passwords, then there is a high risk of internal files becoming compromised. With an authentication server, there will be an added layer of security when accessing internal files on the network. All the computers would have to be set up with this server in mind, and it would involve workstations needing to provide a key to the internal servers to prove their identity, which if confirmed would allow the computer access into the server's files. This can also be combined with the password system to make for 2 factors of authentication, something you know and something you have.

The final change I made to the design was to add a hardware VPN into the network. This VPN would use the IPsec protocols, and its purpose is to allow secure remote access into the network. The VPN would be placed right outside the DMZ, with traffic moving directly from the routers, to the second set of firewalls in the building. This placement will avoid traffic traveling through the demilitarized zone so it can't be captured if a hacker somehow managed to take over the DMZ, but it also still makes sure the traffic does still go through a firewall so it can be filtered like all other packets. The reason I chose to recommend an IPsec VPN over something easier to configure like an SSL/TLS VPN is because the IPsec VPNs are better suited for connecting to corporate networks, and they also encrypt all of the packets that are being sent, whereas SSL VPNs sometimes only encrypt the application data that is being used. A dedicated

hardware VPN gateway also allows for authentication of users, that way nobody who's untrusted can use the internal network. With this setup, employees will be able to remote access the internal network resources like their computer was physically connected to the office.