Final Network Design

David Allen

IST Department, Thomas Nelson Community College

ITN 263: Internet/Intranet Firewalls and E-Commerce Security

Dr. Michael D. Mann

05/01/2023

Final Network Design

Executive Summary

This paper will introduce and discuss the evolution of the core network. This network goes through multiple changes and will include a variety of firewall and remote access technologies. Topics discussed in this paper include addressing scheme and network authentication.

The original topology mentioned includes various devices ranging from Linux and Microsoft servers to Microsoft workstations. The original topology is a star topology. This will be redesigned to further improve redundancy of the network.

The redesigned topology is a dual star topology. This will improve the lack of redundancy of the original network design.

The network needs either an IPv4 or IPv6 addressing scheme. This network will run on IPv4. IPv6 is proved to not be necessary because of the many issues it can have from both a technological and business perspective.

After part one, the network then goes through another redesign. This time the network becomes a two-tiered collapsed core design. This will improve redundancy from the first redesign.

Many different firewalls are present on this network. Some firewalls are hardware-based to protect the internal network. Other firewall solutions include software firewalls installed on all Microsoft workstations. This will help add another level of protection by including a hardware-based and software-based solution.

The network also implements a DMZ. This is a n-tiered network design so that vendors can have access to the extranet for network resources while preventing access to the internal network. The web server is also protected by a firewall to filter web requests and prevent internal access.

The network also has a secure method for authenticating users. Authentication will be accomplished using two-factor authentication for the most security. Secure protocols, such as TLS and IPSec, will also be used in the process of network authentication.

VPN and remote access technologies will be used on the network. The first choice is an IPSec VPN. This type of VPN operates at the network layer and utilizes the IPSec protocol suite to provide secure remote access.

There's also a second popular choice when it comes to VPNs. The second choice would be an SSL/TLS VPN. This kind of VPN operates at the application layer and provides remote access via a web browser.

Between both given options, the IPSec VPN would be the best option. This is based on factors such as software requirements and layers that it operates on. Some best practices are mentioned, such as VPN placement on the network.

Overall, this paper discusses the various changes needed in order to secure the network. This includes changes to the topology, which includes firewall placement and the use of a DMZ. VPN and remote access technologies are also discussed, including which technology is the best and how it helps provide the most secure access to those who need internal network resources.

Original Topology

The original design of the network was a star topology. This topology has the benefits of robustness, easy troubleshooting, easy set up, and easy management (GeeksforGeeks, 2022). For robustness, if a link fails on the network, the rest of the network is not affected (GeeksforGeeks, 2022). It's easy to troubleshoot because of the layout of the design (GeeksforGeeks, 2022). Each device is connected to a central point on the network, which can be a hub, like in this diagram (GeeksforGeeks, 2022). Hubs make it easy to set up and add on to the network because the number of devices is the same as the number of ports and cables needed on the network (GeeksforGeeks, 2022).

This topology does have drawbacks. One of the drawbacks is the central point of failure (GeeksforGeeks, 2022). The network relies on the central hub (GeeksforGeeks, 2022). If the hub encounters any problems, there's a possibility of the whole network being down (GeeksforGeeks, 2022). Performance of the network is also based on the central point (GeeksforGeeks, 2022). More issues could arise if performance isn't fully optimized based on specifications (GeeksforGeeks, 2022).

The network also has a single border firewall that faces the Internet. A border firewall can filter the traffic that enters or leaves the internal network (Stewart & Kinsey, 2020, p. 141). This can prevent hackers from gaining any valuable information from scans on the network (Stewart & Kinsey, 2020, p. 142). This, in turn, will lower the amount of vulnerabilities that can be discovered in the network, lowering the chances of an attack to harden network security (Stewart & Kinsey, 2020, p. 142).

Redesigned Network

The original network needed a redesign to improve redundancy. The redesigned network is a dual star topology (Davis, n.d.). The dual star topology is also used by Sun Microsystem in their ATCA network (Sun Microsystems, 2009). When using two hubs instead of one, having multiple links will strengthen the network's fault tolerance (Sun Microsystems, 2009). In the original design, there was only a single hub. If that goes down, then the entire network goes down. Using two hubs ensures high availability with built-in redundancy of the hub (Sun Microsystems, 2009).

Addressing Scheme

The network needs to have either an IPv4 or IPv6 addressing scheme. In this case, IPv4 will be used. Reasons to keep IPv4 over IPv6 include the maturity of IPv4, bugs, vendor support, lack of skill from employees, and adoption cost (Kaur et al., 2013). First, IPv6 is a lot newer compared to IPv4 (Kaur et al., 2013). This makes IPv4 the mature version over IPv6 with less bugs and less risk (Kaur et al., 2013). Not all vendors support IPv6 (Kaur et al., 2013). This makes it harder for other organizations to transition if vendors aren't supporting IPv6, so they stick with IPv4 (Kaur et al., 2013). Some organizations might lack IPv6 skills (Kaur et al., 2013). Training employees can be a lot of work that employers would rather not spend extra time on, so they keep IPv4 because of this lack of skill from employees (Kaur et al., 2013). Another reason not to switch from IPv4 to IPv6 is the adoption cost (Kaur et al., 2013). Transitioning to IPv6 is too expensive for some organizations (Kaur et al., 2013). On top of the cost to transition alone, training employees would also be necessary, which is just too much for many organizations (Kaur et al., 2013).

Topology Changes

In the next redesign, the network topology is a two-tier collapsed core design. In a collapsed core design, the core and distribution layers are combined into one layer with an access layer underneath (Study CCNA, 2022). The collapsed core layer controls the flow of network traffic to the access layer using the multilayer switches (Study CCNA, 2022). All of the end devices, like workstations and servers, are in the access layer (Study CCNA, 2022). This network design is simple and makes device management and configuration a lot easier (Study CCNA, 2022).

Firewall Selection and Placement

Firewalls on the network include the internal network firewall, web firewall, workstation firewalls, and a DMZ firewall. A multi-homed firewall is used to protect the internal network from threats on the Internet or extranet (Stewart & Kinsey, 2020, p. 141). This firewall filter traffic that enters or leaves the network and protects against hacker scans (Stewart & Kinsey, 2020, pp. 137-142).

The web firewall helps protect the web server. It acts as a proxy between the internal network and web server on its own subnet, which acts as its own DMZ (Stewart & Kinsey, 2020, p. 59). Web requests can come from the multi-homed firewall, which will then be forwarded to the web firewall with its own configurations (Stewart & Kinsey, 2020, p. 59). These requests will then be evaluated and decide on whether or not to let the traffic access the web server (Stewart & Kinsey, 2020, p. 59).

Since the network contains many subnets, protection is also needed there as well. This can be done using packet filtering (Stewart & Kinsey, 2020, p. 183). Packet filtering can accomplish many things, such as blocking or allowing IP addresses, ports, and protocols (Stewart

& Kinsey, 2020, p. 183). The packet filtering mechanics will be done using the multilayer switches in the collapsed core layer (Stewart & Kinsey, 2020, p. 183).

Workstations also need protection on the network, and they already run Microsoft Windows. The best choice here would be to run Windows Defender Firewall with Advanced Security on all workstation computers. Windows Defender is a host software firewall option for devices that run the Microsoft Windows operating system which has a lot of benefits and works with many network configurations (Stewart & Kinsey, 2020, p. 158). Using a host firewall enforces a defense in-depth approach by adding layers the attacker must go through (Microsoft, 2023). Using Windows Defender makes management easy while decreasing the chances of an attack on a computer by reducing attack surfaces (Microsoft, 2023). There's also no need for extra hardware or software because this comes with the operating system (Microsoft, 2023). Host software firewall solutions, like Windows Defender, extends the value of other assets (Microsoft, 2023).

DMZ Design

To increase the security of the network's perimeter, a demilitarized zone (DMZ) is needed. This can give vendors access to necessary resources over an extranet. An extranet is a boundary network that hosts resources for a limited and controlled group of external users, like vendors, business partners, and others associated with the company (Stewart & Kinsey, 2020, p. 93). This also can keep users on the Internet out of the internal network (Stewart & Kinsey, 2020, p. 93).

A common DMZ design is an N-Tiered deployment (Stewart & Kinsey, 2020, p. 94). A series of subnets is created and separated by a firewall, the extranet for the third diagram (Stewart & Kinsey, 2020, p. 94). The extranet will act like a buffer network between the Internet

and internal network (Stewart & Kinsey, 2020, p. 94). The purpose of this design is to keep users on the Internet out of the private LAN and only give access to those who need a limited number of resources on the extranet located in the DMZ (Stewart & Kinsey, 2020, p. 93).

Network Authentication

The proof of a user's identity before granting them access to confidential information is known as authentication (Stewart & Kinsey, 2020, p. 7). A username and password system is a common method to authenticate users on a network, but isn't good enough by itself to provide the best security (Stewart & Kinsey, 2020, p. 7). To improve upon this, it's a great idea to use two-factor authentication to maintain confidentiality and protect the integrity of information (N-able, 2019). Two-factor authentication requires the user to have something on top of the username and password (N-able, 2019). It can be a code sent to an email or through a text messaging system on someone's phone, which is actually one of the most common ways two-factor authentication is implemented since hacker would need the code, username, and password to get into the account (N-able, 2019).

Something else to consider when implementing authentication are authentication protocols. One protocol to use is Transport Layer Security (TLS) (N-able, 2019). TLS uses certificates to authenticate users before they connect to the web server using mutual identification (N-able, 2019). It's built-in to many web browsers that are used today, easy to implement, and doesn't require special software (N-able, 2019). Traffic is encrypted to also prevent eavesdropping (N-able, 2019). The most current version of TLS is version 1.3, which improves upon the vulnerabilities that existed with version 1.2, which included both triple handshake and Heartbleed attacks (Dowling et al., 2021).

IPSec is another important authentication protocol that should be used. A lot of networks, including this one, use IPv4 (Stewart & Kinsey, 2020, p. 103). By default, IPv4 uses plaintext, which is a security issue because encryption must be used when it is necessary (Stewart & Kinsey, 2020, p. 103). IPv4 uses IPSec to encrypt data, compared to IPv6 that uses encryption by default, so it also further proves that there's no reason to jump over to IPv6 yet (Stewart & Kinsey, 2020, p. 103). It was mentioned earlier that workstation computers will run Microsoft Windows Defender Firewall with Advanced Security. Windows Defender is actually integrated with IPSec, which makes the enforcement of authentication simple because of its scalability and tiered access to enforce data integrity and confidentiality (Microsoft, 2023).

IPSec VPNs

For secure remote access, two types of VPNs are considered, Internet Protocol Security (IPSec) and SSL/TLS (Secure Sockets Layer/Transport Layer Security). IPSec encrypts traffic at layer three, the Network Layer of the OSI model (Cloudflare, 2023). It also encrypts traffic from layers four through seven, which includes application traffic (Stewart & Kinsey, 2020, p. 313). Three major parts of IPSec are the Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) (Stewart & Kinsey, 2020, p. 312). The AH protects integrity for packet headers, data, and user authentication (Stewart & Kinsey, 2020, p. 313). This also includes relay and access protection (Stewart & Kinsey, 2020, p. 313). ESP was used with the AH in its earliest versions to only provide protection for packet payload data, but newer versions of ESP now include encryption and integrity protection capabilities (Stewart & Kinsey, 2020, p. 313).

IPSec VPNs need separate software installed on a computer in order for it to work (N-able, 2019). VPNs also require a password for protection (N-able, 2019). Since a password is

required, two-factor authentication can be implemented with the VPN (N-able, 2019). This will make it harder for a hacker to gain access to the VPN because of the multiple layers of security they have to go through (N-able, 2019).

IPSec supports two modes for securing data, transport mode and tunnel mode (N-able, 2019). When the payload of an IP packet is encrypted, transport mode is used between hosts (N-able, 2019). When the entire packet is encrypted and gets encapsulated in a new IP packet with a new header, tunnel mode is used between gateways (N-able, 2019).

SSL/TLS VPNs

Next, an SSL/TLS VPN is an option for secure remote access. Later replaced by TLS, SSL is a protocol that encrypts Hyper Text Transfer Protocol (HTTP) traffic (Cloudflare, 2023). SSL operates at seventh layer of the OSI model, the Application Layer (Cloudflare, 2023). An SSL VPN doesn't have any problems working with Network Address Translation because it operates at the Application Layer (NAT) (Stewart & Kinsey, 2020, p. 318).

SSL is supported through a web browser on most devices (Cloudflare, 2023). There isn't any special software required to use an SSL/TLS VPN, making configuration easy and it doesn't require an IT team to set up (N-able, 2019). Specific access is only granted to those who need to get their job done on an SSL/TLS VPN (N-able, 2019). Depending on how complex the network is and the number of employees, this can be a benefit or a drawback (Stewart & Kinsey, 2020, p. 318).

Two modes are offered on an SSL/TLS VPN, portal mode and tunnel mode (N-able, 2019). Portal mode is useful for web-based programs, which includes email, file sharing, and other browser applications (N-able, 2019). To access any application on the network, tunnel

mode would be used (N-able, 2019). Offline programs can also be accessed, even though browser-based applications are becoming the new standard in the industry (N-able, 2019).

VPN Recommendation and Best Practices

Security and convenience are factors to consider when choosing between either an IPSec or SSL/TLS VPN (N-able, 2019). I would recommend the IPSec VPN over the SSL/TLS VPN. IPSec has better security than an SSL/TLS VPN would (N-able, 2019). Software with specific configurations would be required for a hacker to know to even get access to the VPN (N-able, 2019). IPSec encrypts IP packets at the at the Network Layer and application traffic at higher layers of the OSI model (Stewart & Kinsey, 2020, p. 313). Using two-factor authentication on top of an IPSec VPN provides a very secure remote access solution (N-able, 2019).

Some best practices to follow to further protect a VPN involve passwords, software, firewalls, hardware, services, and protocols (Stewart & Kinsey, 2020, p. 347). Any default passwords should be changed to a stronger, but also memorable, password (Stewart & Kinsey, 2020, p. 347). Antivirus software should be installed, along with its correct definitions (Stewart & Kinsey, 2020, p. 347). Operating systems and applications should remain updated always (Stewart & Kinsey, 2020, p. 347)**.** Firewalls, either built-in or standalone, should be used when necessary (Stewart & Kinsey, 2020, p. 347). Wireless interfaces should be disconnected when connecting to a wired interface, this also applies the other way around (Stewart & Kinsey, 2020, p. 347). When using a VPN, it should only be used for work purposes with any unneeded services or protocols disabled (Stewart & Kinsey, 2020, p. 347). VPN servers should use strong authentication and encryption, while also being protected behind a firewall, in a DMZ for example, for extra protection from Internet attacks (Stewart & Kinsey, 2020, p. 347).

References

Cloudflare. (2023). *IPsec VPNs vs. SSL VPNs*. https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/

Davis, L. (n.d.). *Dictionary of electronic and engineering terms, network Topologies*. Interfacebus. https://www.interfacebus.com/Glossary-of-Terms-Network-Topologies.html

Dowling, B., Fischlin, M., Gunther, F., & Steblia, D. (2021, July 30). *A cryptographic analysis of the TLS 1.3 handshake protocol*. SpringerLink. https://link.springer.com/article/10.1007/s00145-021-09384-1#Sec1

GeeksforGeeks. (2022, November 9). *Types of network topology*. https://www.geeksforgeeks.org/types-of-network-topology/?ref=lbp

Kaur, A., Singh, H., & Tan, F. (2013). *Why isn't digital infrastructure being updated?: The case of IPv6*. https://ap-st01.ext.exlibrisgroup.com/61RMIT_INST/upload/1676463678849/acis2013_384.pdf?Expires=1676463799&Signature=nT6AHv-mIBuVSc0LsHzNut37L7VRpaoduk6YJ13EwR9Rt6E~GeivheVdnQyt4PusFYimZhPYXnYXm~yhwBxYUvq9qvZGROM1zr0~qM-UFhbSWdzy18a-SDoXLq5hsoc76UEV11~bS4aAaBis81VxbubOQciFYgyTqnkhXl9zBcfTqWUVx1RyirjHcI7Mz48Wc-RfKs6TudO0m91ZFBLurVeD2xw58NdUkrVNydeS57wAdzZDX3cKCqtudjUMYBwjR9Kcr1yRRyRJfZ9k5bTcgVAkyEsUX61gzyCwY6O0qXaa2s43C~VQ0FmMEFAWqZ3k2XE-PPQH7P6thIH65O4wRw__&Key-Pair-Id=APKAJ72OZCZ36VGVASIA

Microsoft. (2023, February 24). *Windows defender firewall with advanced security*. Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security

N-able. (2019, April 15). *IPsec vs. SSL: What's the difference?* https://www.n-able.com/blog/ipsec-vs-ssl

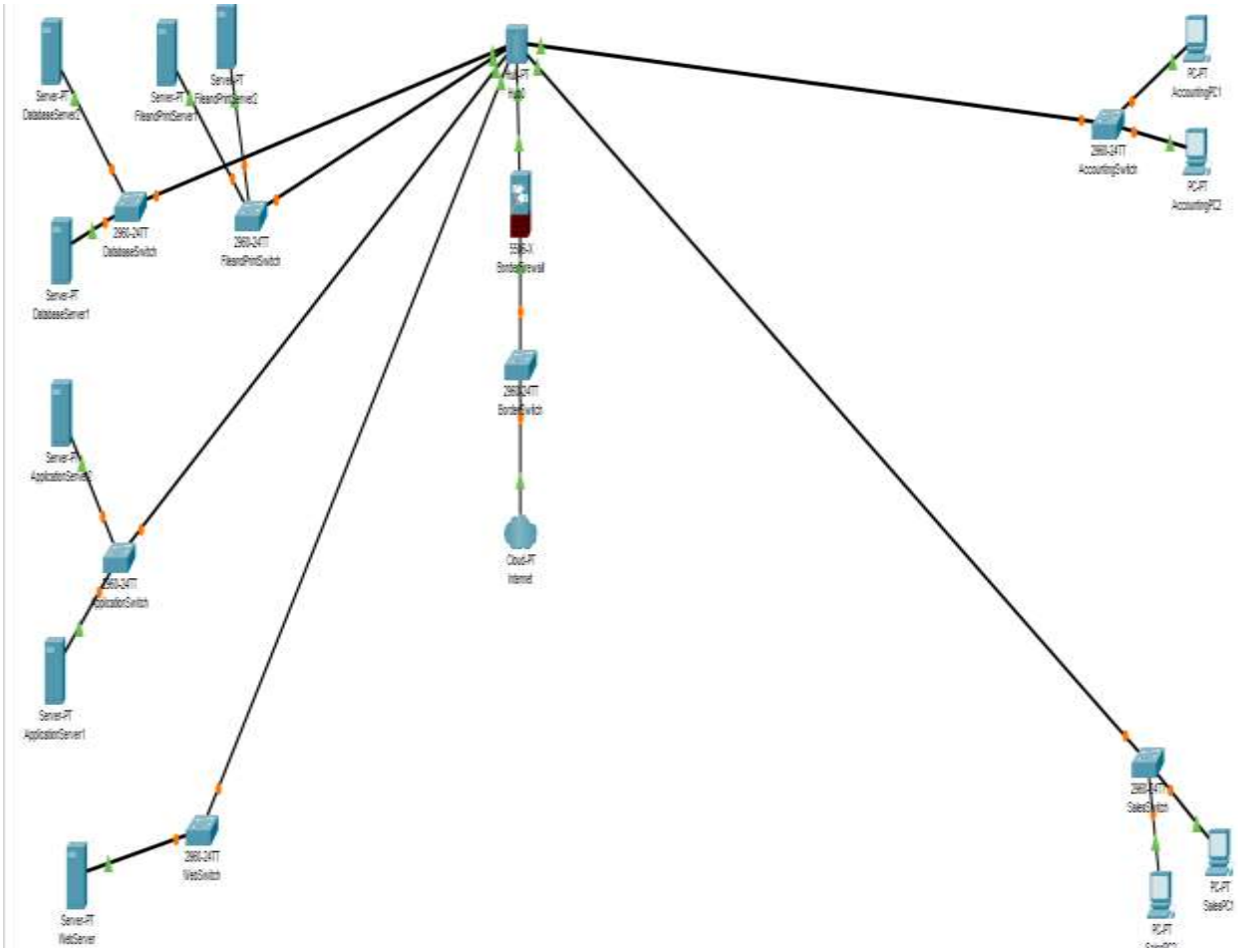
N-able. (2019, April 24). *Understanding network authentication methods*. https://www.n-able.com/blog/network-authentication-methods

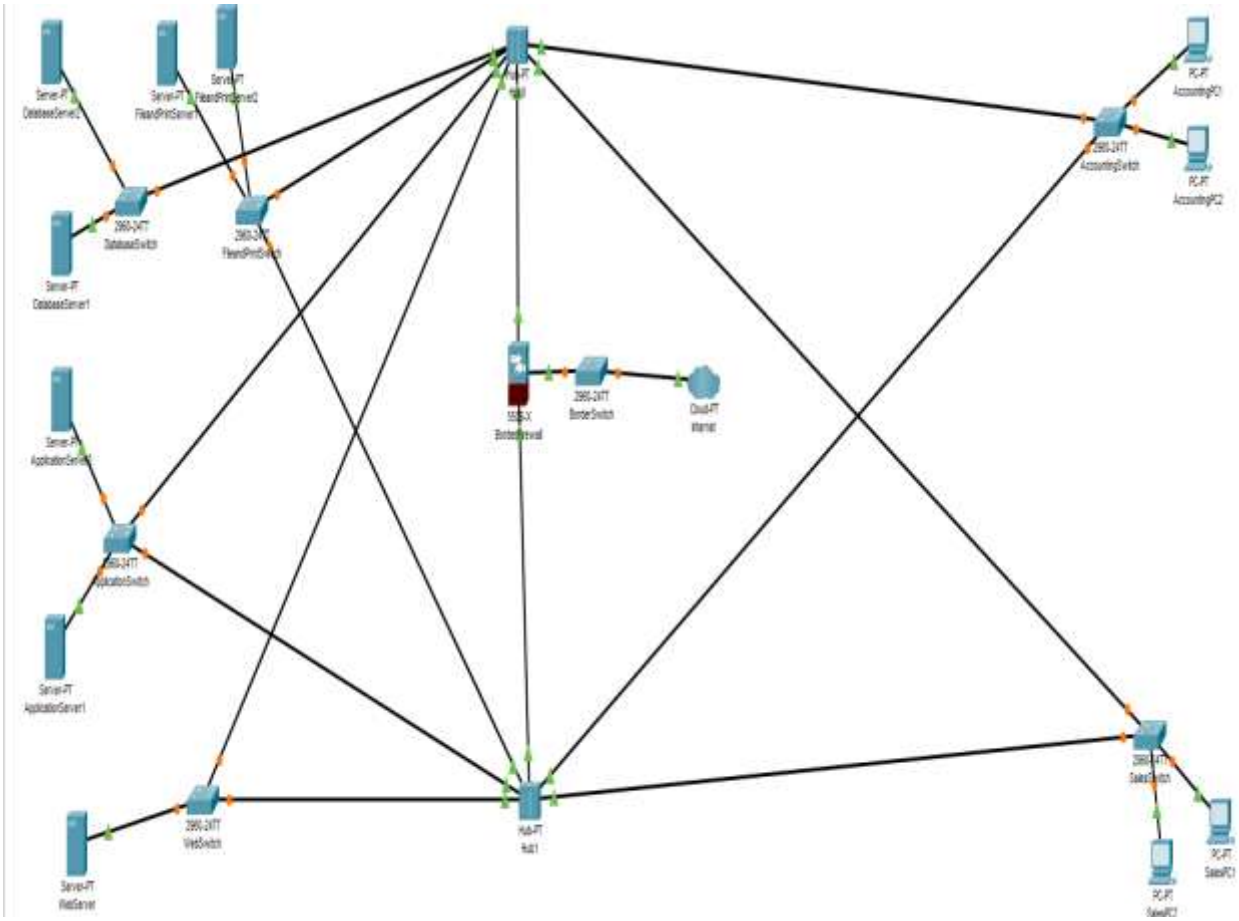
Stewart, J. M., & Kinsey, D. (2020). *Network security, firewalls, and VPNs* (3rd ed.). Jones & Bartlett Learning.

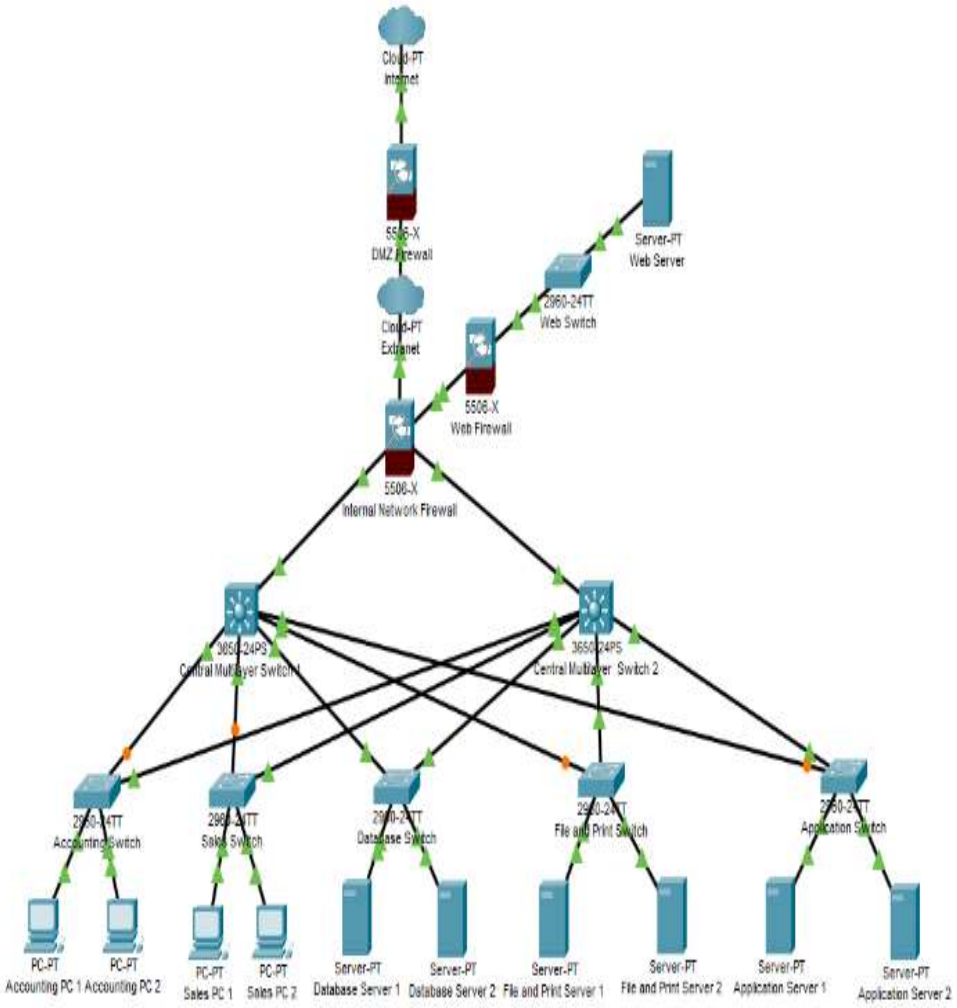
Study CCNA. (2022, December 27). *Collapsed core and three-tier network architectures*. https://study-ccna.com/collapsed-core-and-three-tier-architectures/

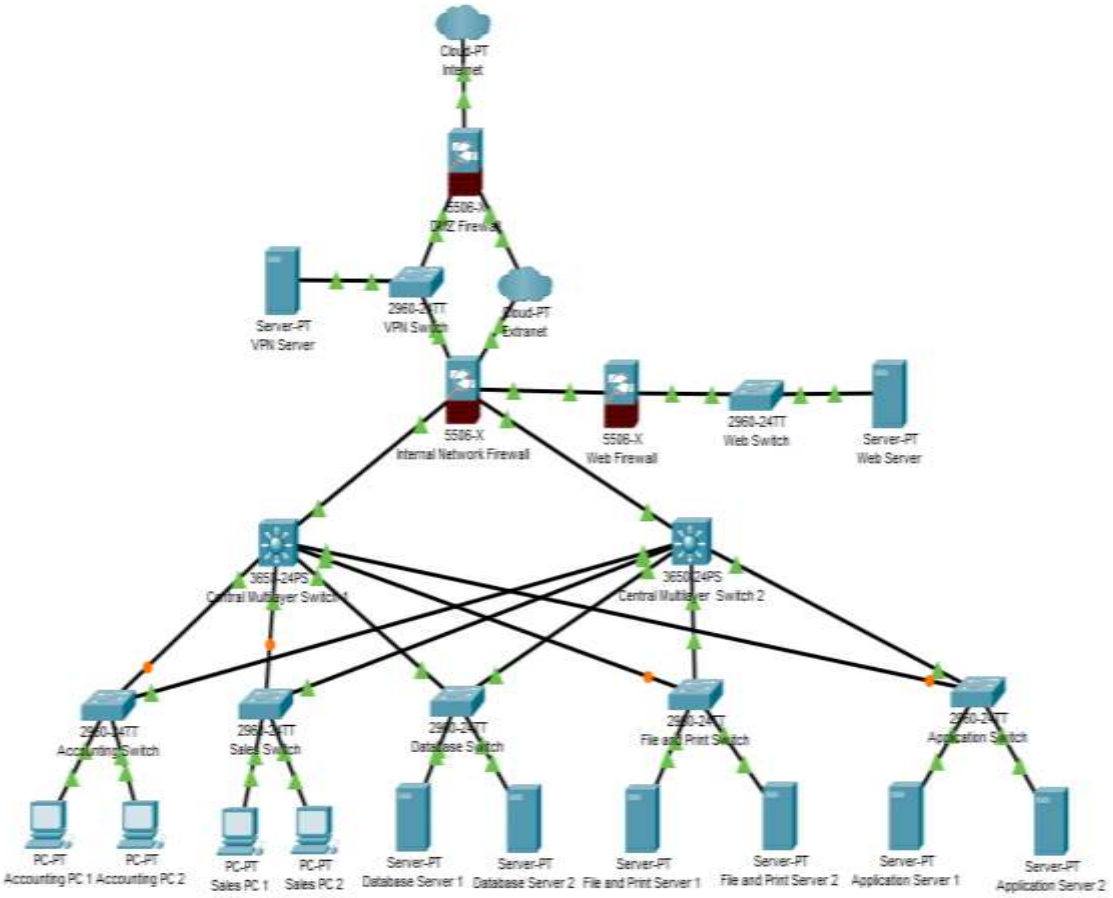
Sun Microsystems. (2009). *Designing a fault-tolerant network*. https://docs.oracle.com/cd/E19859-01/820-7346-10/guide.html#50581505_41253

Appendix A: Network Diagrams






Cloud-PT
Internet
5506-X
DMZ Firewall
Server-PT
Web Server
2960-24TT
Web Switch
Cloud-PT
Extranet
5506-X
Web Firewall
5506-X
Internal Network Firewall
3650-24PS
Central Multilayer Switch 1
3650-24PS
Central Multilayer Switch 2
2960-24TT
Accounting Switch
2960-24TT
Sales Switch
2960-24TT
Database Switch
2960-24TT
File and Print Switch
2960-24TT
Application Switch
PC-PT
Accounting PC 1
PC-PT
Accounting PC 2
PC-PT
Sales PC 1
PC-PT
Sales PC 2
Server-PT
Database Server 1
Server-PT
Database Server 2
Server-PT
File and Print Server 1
Server-PT
File and Print Server 2
Server-PT
Application Server 1
Server-PT
Application Server 2


Cloud-PT
Internet
5506-X
DMZ Firewall
Server-PT
VPN Server
2960-24TT
VPN Switch
Cloud-PT
Extranet
5506-X
Internal Network Firewall
5506-X
Web Firewall
2960-24TT
Web Switch
Server-PT
Web Server
3650-24PS
Central Multilayer Switch 1
3650-24PS
Central Multilayer Switch 2
2960-24TT
Accounting Switch
2960-24TT
Sales Switch
2960-24TT
Database Switch
2960-24TT
File and Print Switch
2960-24TT
Application Switch
PC-PT
Accounting PC 1
PC-PT
Accounting PC 2
PC-PT
Sales PC 1
PC-PT
Sales PC 2
Server-PT
Database Server 1
Server-PT
Database Server 2
Server-PT
File and Print Server 1
Server-PT
File and Print Server 2
Server-PT
Application Server 1
Server-PT
Application Server 2