I. Network Description

A. Network Topology (presently)

II. Recommendations

a. Justification for each recommendation

b. Methods to measure the success of each enhancement

III. Executive summary

IV. Final network diagram

V. References

1. **Network Description**

The Logical Topology map includes the current fracture elements.

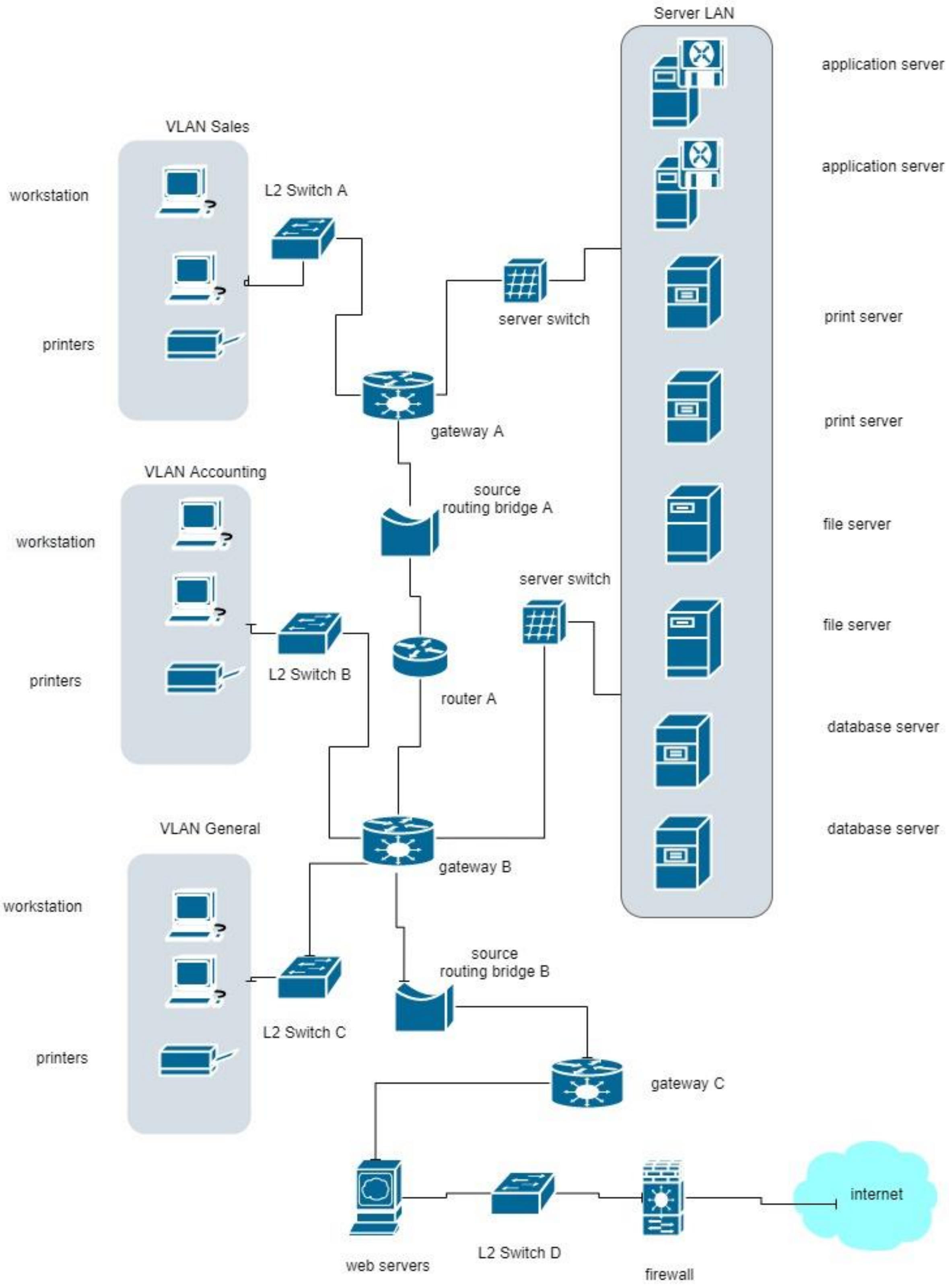
A. Please refer to the **Network Topology** (presently)

B. Network design with the following components: Current infrastructure elements:

1. One web server (accessible by the public) runs Linux/Apache.
2. Two application servers, two database servers, two file servers, and two print servers run MS Windows Server.
3. 50 Workstations run MS Windows.
4. Printers were not on the list but would be present with printer servers
5. Single border firewall
6. Linux and Windows servers use TCP, so there would not need any conversion between the servers. However, gateway B as a security layer could also function as a protocol converter if required.
7. The network runs IPv4.
8. Network not physically connected to other networks.
9. L2 Switch D, gateway C, firewall, and webserver protect Internet connectivity from malicious intrusions.
10. Using intrusion detection system (IDS) and intrusion prevention system (IPS) in the firewall provide a layer of protection.
11. If the webserver is attacked and compromised, Gateway C will provide multilayer security through isolation and separation from the network.
12. The source routing bridge B would enable a layer of protection.

13. **Logical topology separating Accounting and Sales departments providing separation and security**
    a. VLAN Accounting and VLAN Sales are logically apart, thus keeping the Accounting and Sales department separate.
        i. The use of separate L2 Switches A and B add separation and security.
        ii. Gateway A and gateway B add a layer of security and separation.
        iii. Each VLAN would have its printer for logical and physical separation would add another layer of security.
14. **Logical topology with redundant communications**
    a. **Plan for availability 24/7**
    b. One Concentrator amplifies a signal.
    c. One Repeater rebuilds the signals.
    d. Using L2 switches A, B, and C will allow faster ethernet by providing redundancy.
    e. Gateway A and B will provide security by separating the server and LAN switches.
    f. Router A and source routing bridge A would allow redundancy to the network.
    g. Source routing bridge A would allow for blocking to occur for security.

C. **Network Topology** (presently)



D. Recommendations of Enhancements

a. Upgrading to IPv6

The benefits of IPv6 are less management, increased address space, enhanced routing functionality, a better quality of service support (QoS) for all types of applications, better IPSec. These benefits would allow company Tech to grow as its business grows.

As company Tech grows, the company will need more addresses for more network devices. IPv6 with its 128-bit address could support 340 undecillion IP addresses for network devices, thus allowing company Tech many years of growth without fear of running out of IP addresses. As the business grows, the company would experience routing problems, IPv6 would give enhanced routing functionality. IPv6 has better QoS for all types of applications than IPv4. Though IPv4 could have a similar QoS as IPv6 as an add-on. With the increase in business use of the Internet from company Tech, a significant improvement in IPv6 IPSec provides better security than IPv4's IPSec. IPSec in IPv6 protects the data. It uses Authentication Header (AH) and Encapsulating Security Payload (ESP) with cryptographic security services. IPv6 IPSec provides confidentiality, data origin authentication, and Data Integrity. To provide confidentiality, IPSec would encrypt traffic and allow its decryption with the encryption key, an integral part of the IPv6 protocol. The data origin authentication is thru a cryptographic checksum, using a shared encryption key that allows receiver verification of the sender, thus preventing spoofing. Finally, IPv6 uses the cryptographic checksum to check for changes in a packet in transit. In migration to IPv6, the best strategy for company Tech is Tunnelling, which allows gradual transition. This solution enables two IPv6 hosts to tunnel traffic through the IPv4 network as IPv4 phased out. However, this would require configuration overhead.

b. Firewalls Implementation:

Using 4-tier deployment with firewalls to provide security for each subnet, Corporation Tech will have multilayer security between its subnets and the internal LAN and the Internet. The Windows Defender Firewall (WDF) protects the workstations on the lowest risk layer. In the next layer of security, WDF protects the company's servers. Finally, the network firewalls are the outermost and highest risk part of the network. A demilitarized zone (DMZ) will provide layers of security between its internal subnets and outwardly between the internal LAN and the Internet.

i. Workstation Firewalls:

On workstation host software firewall: Native firewall comes with Windows, Windows Defender Firewall (WDF), with Windows 10.

a. The WDF is a native and free security component with Corporation Techs workstations with Windows 10.

b. One advantage of WDF is its ability to adjust its settings based upon the network connection to a known, previously accessed network.

c. The WDF can create a password-protected workgroup that allows file-sharing and printer-sharing between system authorized users.

    i. Adds a layer of security to the VLAN Accounting and VLAN Sales network.

ii. Server Firewalls:

Each Windows Servers has Windows Defender Firewall (WDF) with its server software. WDF with IPSec and its other security advantages native and free with Windows Server 2016 and above. It can create password-protected workgroups.

ii. Network Firewalls:

Please refer to the **Final Network Topology** below for device names.

A border firewall is a firewall between the Internet and the DMZ; Firewall 1 will be a pfSense firewall-router appliance. PfSense firewall-router appliance is an excellent choice with Linux based webserver and would manage access to DMZ. Being an appliance firewall, pfSense does not share resources with other services. This resource priority is essential in the security at the border firewall. Ease of implementation and configuration changes management are two advantages of appliance firewall.

1) Firewall 5 between Gateway A and the L2 Switch A filters for Sales communication.
2) Firewall 4 between Gateway B and the L2 Switch B filters for Accounting Department communication.
3) Firewall 3 between Gateway C and L2 Switch C filters for internal abuses between the general VLAN and VLAN Accounting and VLAN Sales.
4) Firewall 2 between Gateway C and DMZ logically separates and filters the internal LAN and the DMZ.

In the Server LAN, concentrators and repeaters devices are between servers. They renew the strength of the signal by preventing the loss of signal strength.

The Microsoft Security Essentials suite also includes antivirus and anti-malware.

E. De-Militarized Zone with Firewall:

DMZ is an extranet in its interaction with the Internet. External users can access resources hosted in a boundary network with DMZ. It exchanges data with external partners in a safe place with only intended external users who can access it. The DMZ has two firewalls providing security and preventing malicious attacks from reaching the internal LAN.

1) Firewall 1 filters incoming packets from the Internet. This firewall would be a PfSense firewall-router appliance to provide maximum security for the DMZ and internal LAN
2) Firewall 2 filters the packets leaving the DMZ, and entering the internal LAN would also be a PfSense firewall-router appliance to provide logical isolation and security for the internal LAN.
3) Web servers, email servers, and File Transfer Protocol servers are placed in the DMZ to provide security through separation.
4) Each target host on the DMZ network segment has two IP addresses. Internal access of LAN uses a static IP address. A virtual IP address to allow access from the WAN.
5) Requires VPN connection to keep the user from the Internet out and keep external partners out of the private LAN.
6) These servers allow external users to use these services.

7) DMZ protects the rest of the network if an attack succeeds. These servers have limited connectivity to specific hosts on the internal LAN, such as the webserver in DMZ can connect to the Database Server but no other hosts.

F. Network Authentication:

Network authentication is one of three main parts of security to control access to the company's resources. Network authentication is best done with an Authentication Server and not as part of a firewall. Multifactor authentication has three features, Type 1--something you know, Type 2--something you have, and Type 3--something you are or do.

- Type 1 is something you know. An example of Type 1 would be a password.
- Type 2 is something you have. An example of Type 2 would be something like a smart card, RFID, ID badges, or text sent to your preregistered smartphone.
- Type 3 is something you are. An example of Type 3 would be your biometrics such as fingerprints, iris scans, retina scans, facial geometry, or signature dynamics.

G. Virtual Private Network (VPN)

Virtual Private Network (VPN) Server using IPsec is the best solution for Corporation Techs to secure remote access through the Internet to its internal LAN to use its servers and workstations. Internet Protocol Security (IPsec) would provide authentication and encryption of information to prevent snooping between the remote users and the LAN servers. The benefits of VPN using IPsec are as follows.

1. VPN has flexibility that allows integration with existing networks and technologies.

2. VPN has a remote access configuration that grants workers the ability to access and use company resources, such as information on servers and printers, in an efficient and timely manner, thus promoting productivity.
3. VPN has secure mobile connectivity with Wi-Fi and broadband for diverse types of mobile devices increases the accessibility of the user to company resources.
4. VPN has scalabilities that allow for the increase or decrease capacity with ease with fully scalable global architecture. In addition, VPN enables telecommuting to save long-distance costs for telecommuters and traveling workers. VPN provides flexibility and the versability of worker location.
5. VPN has cost-saving because it does not require a dedicated leased line between each endpoint's location.
6. VPN with IPsec authenticates and encrypts packets and provides end-to-end technology that works in the Internet layer of the TCP/IP Model using tunneling protocols. Improve privacy and confidentiality with solid encryption and verified transmission integrity.
7. Tunneling protocol encases the network protocol to travel the Internet through encryption, enabling the original data to go through the Internet securely.

H. Implementation of VPN Server with IPSec

1. The software-based VPN as part of the VPN Server would be in the DMZ.
2. PfSense firewall-router appliance, implemented in Project part 2, will configure the VPN server with IPsec.
    a. Firewall 1 firewall-router would protect VPN servers from Internet-based attacks.

b. Firewall 2 would protect the internal network. In addition, the physical and logical location of the DMZ would provide physical and logical isolation and security for the VPN Server.

c. PfSense configuration would provide the least disruption to the availability of network resources to the users.

3. IPsec protocol secures Internet Protocol (IP) communication through authenticating and encrypting each IP packet in an IP data stream.
   a. IPsec uses authentication header (AH), encapsulation security payload (ESP), and internet key exchange (IKE).
   b. With Tunnelling, the IP packet is encapsulated and given a new header, and the destination host decapsulates the packet. This secure traffic for a remote access VPN connection from a remote host over the Internet.
   c. It supports all OS platforms.
   d. It provides secure, node-on-the-network connectivity.
   e. Offers standard-based solutions, permitting easier interoperability between different devices and vendors.
4. VPN performances are affected by the type, protocol, load, client configuration, bandwidth, topology, encryption level, traffic, client version.
5. VPN stabilities are affected by configuration, location, software version, underlying OS.
6. VPN with dynamic Network Address Translation (NAT) using IKE, ESP, and AH.

These factors make the VPN one of the most efficient and cost-effective ways to provide secure remote connectivity.

b. **Methods to measure the success of each enhancement**

Use GNS3 to build, design, and test a simulated network environment. Appliances with the GNS3 environment will reflect the existing environment can be seen in section **C. Network Topology** (presently) with appropriate switches, gateways, and a firewall. The recommended enhancements are added to the GNS3 topology to reflect the new topology with firewalls, DMZ, and VPN. GNS3 's Virtual PC Simulator (VPCS) evaluates the new network design for the network enhancements success. VPCS has utilities to enable testing of the enhanced network design. Wireshark, included in GNS3, Microsoft Security Essentials, is the best option for Corporation Techs to observe the live network traffic and capture it for analysis. VPCS has Ping for sending ICMP, echo, request, and Traceroute, which trace a network between two points. The VPCS will allow a connectivity test to see if the connectivity is as the IT management team would like.

1. With GNS3, PfSense would set up firewalls, switches, gateways rules to filter traffic and logically separate the subnets, VLAN Accounting, VLAN Sales, VLAN General, and VLAN server, and DMZ.
2. The ping test of GNS3 would evaluate the logical separations between the subnets due to the firewalls, switches, gateways, and DMZ. In addition, the Wireshark would detect communication devices within the network.

To evaluate the Windows Defender Firewall rules on the workstations and servers. Powershell evaluates Windows IIS Server by using the Get-NetFirewallRule command to return information about the WDF.

To evaluate the IPv6 implementation, a ping command on the system's operating system will cause a reply differentiating between a 32-bit or 64-bit OS device.

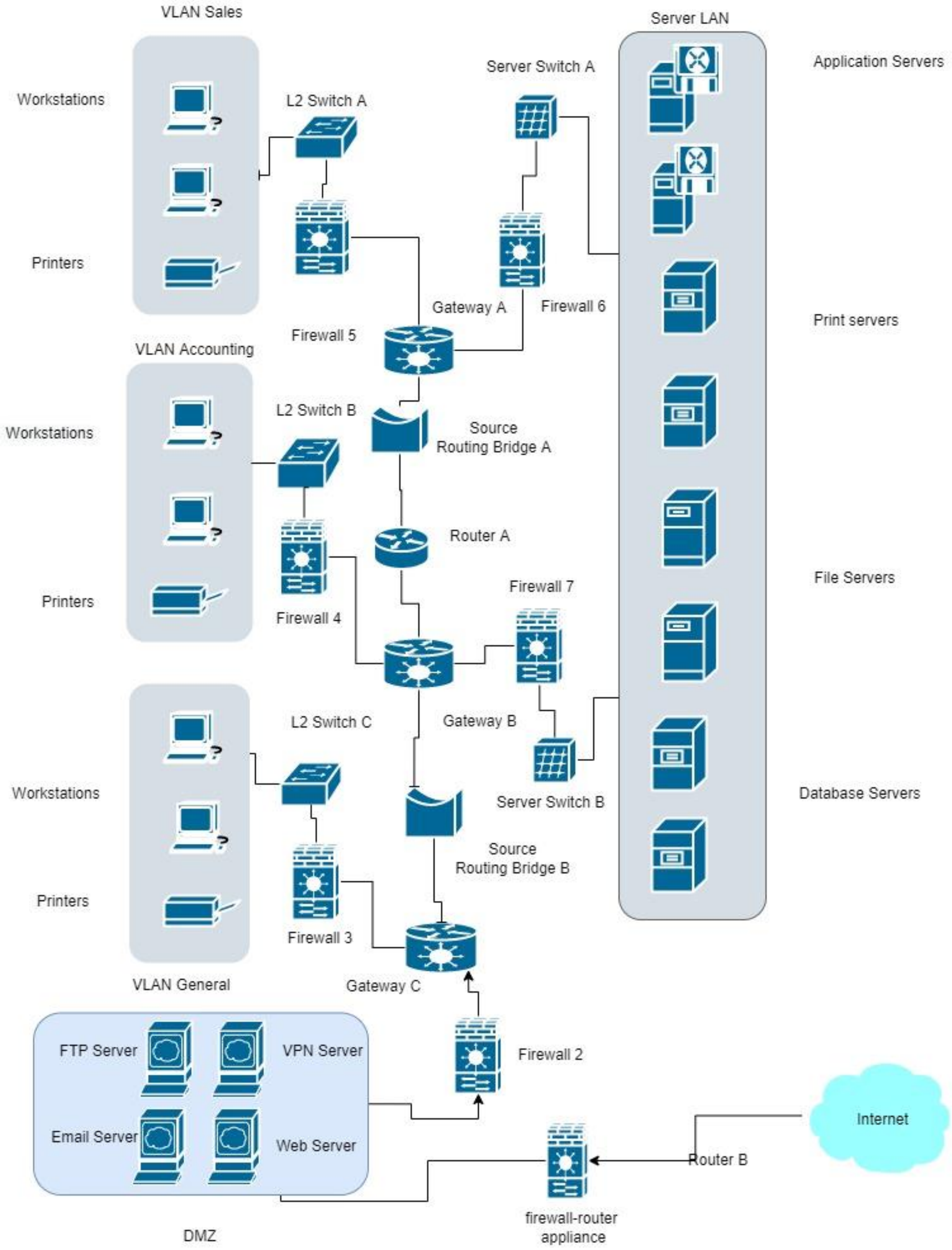
Wireshark implements VPN. Then a penetration test does network scanning with Nessus. Then with Nessus's vulnerability analysis reduced and eliminated network vulnerabilities, thus preventing an attack's weaponization, delivery, and exploitation.

Snort monitored the DMZ and LAN subnetworks for attacks. Kali Linux Test of the monitoring system of Snort and Splunk SIEM.

I. Executive Summary

The enhancements of the network enable growth and security for Corporation Techs. Upgrading to IPv6 allows the company to grow in the future without significant changes in its network. Firewalls logically separate the VLAN Accounting, VLAN Sales, VLAN General, and DMZ provide multilayers of logical security for the subnets and interact with Windows Defender Firewall on the Windows Workstation and Windows Server. DMZ safely hosts resources for external users, websites users. With multifactor authentication protects Company Techs from many attacks. VPN allows flexibility, scalability, administration ease, and reliability with security thru data-origin authentication, data integrity, multifactor authentication, data confidentiality. The enhancements provide growth and protection.

V. Final Network Topology



IV References

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