Project Part 2

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. On the lowest risk layer, the Windows Defender Firewall (WDF) protects the workstations. In the next layer of security, WDF protects the servers of the company. 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.

A. 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. In addition, WDF adds a layer of security to the VLAN Accounting and VLAN Sales network.

B. Server Firewalls:

Each Windows Servers has Windows Defender Firewall (WDF) with its server software.

a. WDF has IPSec and its other security advantages.

b. It is native and free with Windows Server 2016 and above.

c. It can create password-protected workgroups.

C. Network Firewalls:

Please refer to the **Network of Corporation Techs** below for device names.

1. A border firewall, Firewall 1, is part of the DMZ.
    a. Please see **DMZ Firewall Implementation** for more DMZ information.
2. Firewalls separate the VLAN Accounting and VLAN Sales and provide another layer of security for the VLAN subnets.
    a. Firewall 5 between Gateway A and the L2 Switch A that filters for Sales communication.
    b. Firewall 4 between Gateway B and the L2 Switch B that filters for Accounting Department communication.
    c. Firewall 3 between Gateway C and L2 Switch C filters for internal abuses between the general VLAN and VLAN Accounting and VLAN Sales.
    d. Firewall 2 between Gateway C and DMZ logically separates and filters the internal LAN and the DMZ.
    e. Within the LAN, Microsoft Security Essentials is the best option for Corporation Techs. It would interact seamlessly with Windows Defender Firewall on the Windows Workstation and Windows Server.
    f. The Microsoft Security Essentials suite also includes antivirus and anti-malware.

g. Logging many internal hosts, the external hosts, and firewall activities would provide information about internal attacks between departments and external attacks from the Internet to the intranet.

D. De-Militarized Zone Implementation 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 hosts resource servers for a limited and controlled group of external users, partners, suppliers, distributors, contractors, websites. 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.

a. Please refer to **DMZ Of Corporation Techs** for device names
b. Firewall 1 filters incoming packets from the Internet using PfSense firewall-router appliance would provide maximum security for the DMZ, and internal LAN. Ease of implementation and configuration changes management is an advantage of appliance firewall.
    1. PfSense firewall-router appliance is an excellent choice with Linux based webserver. Using an appliance firewall, pfSense does not have to share resources with other services. This resource priority is essential in the security at the border firewall.
    2. PfSense would be an excellent bastion host because it is pre-hardened.

3. PfSense would configure to log sessions between hosts and ports, both valid and invalid.

c. Firewall 2 filters the packets leaving the DMZ and entering the internal LAN would also be a PfSense software firewall host to provide logical isolation and security for the internal LAN.
    1. PfSense would log sessions between hosts and DMZ.

d. Web servers, email servers, and File Transfer Protocol servers are in the DMZ to provide security through isolation and separation.
    1. 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.
    2. Requires VPN connection to keep the user from the Internet out and keep external partners out of the private LAN.
    3. These servers allow external users to use these services.
    4. 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.

E. Network Authentication:

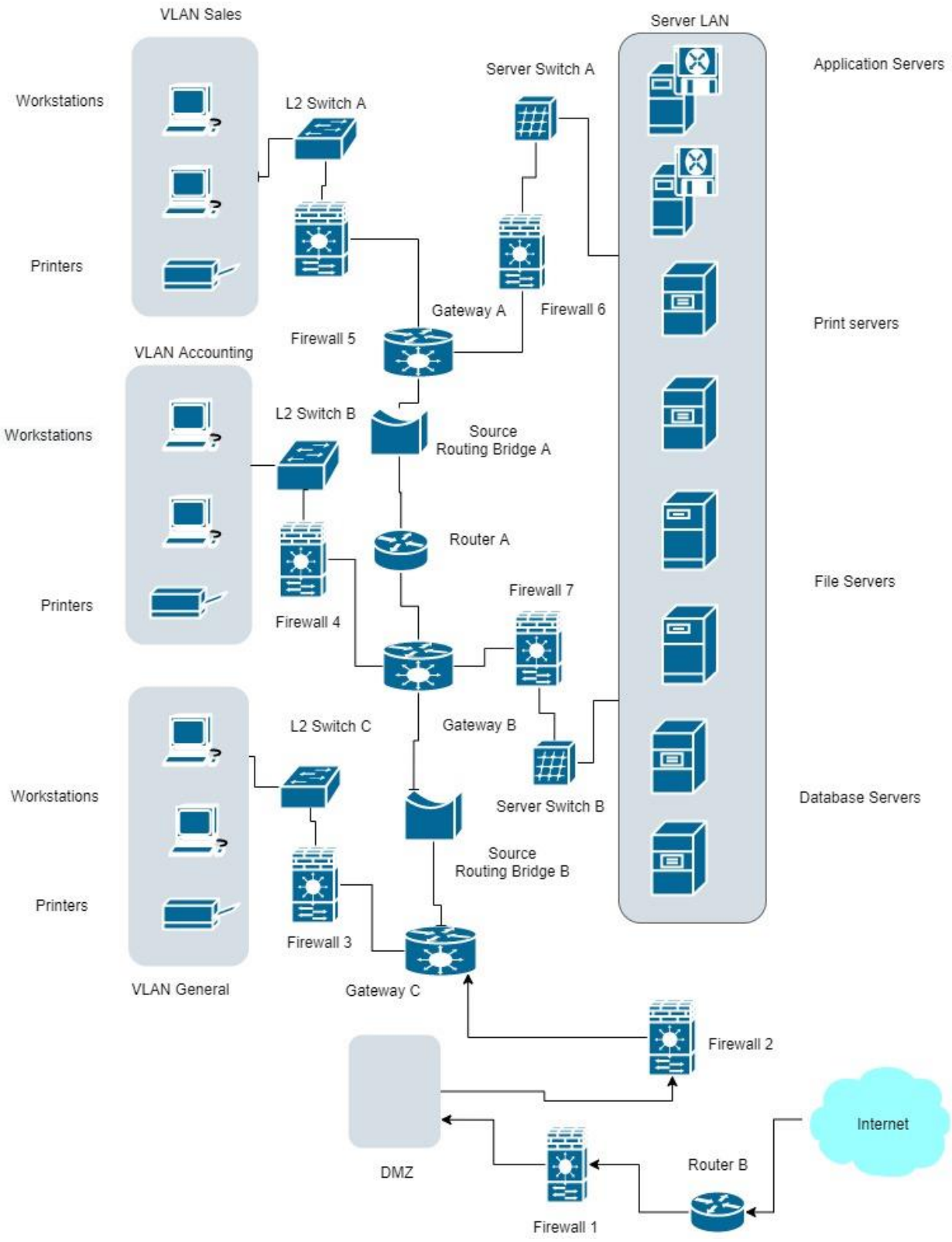
Network authentication is one of three main parts of security to control access to the company's resources and should use an Authentication Server and not be part of a firewall. Multifactor authentication provides more protection to the internal LAN than

single-factor authentication. Multifactor authentication has three features, Type 1--something you know, Type 2--something you have, and Type 3--something you are or do.

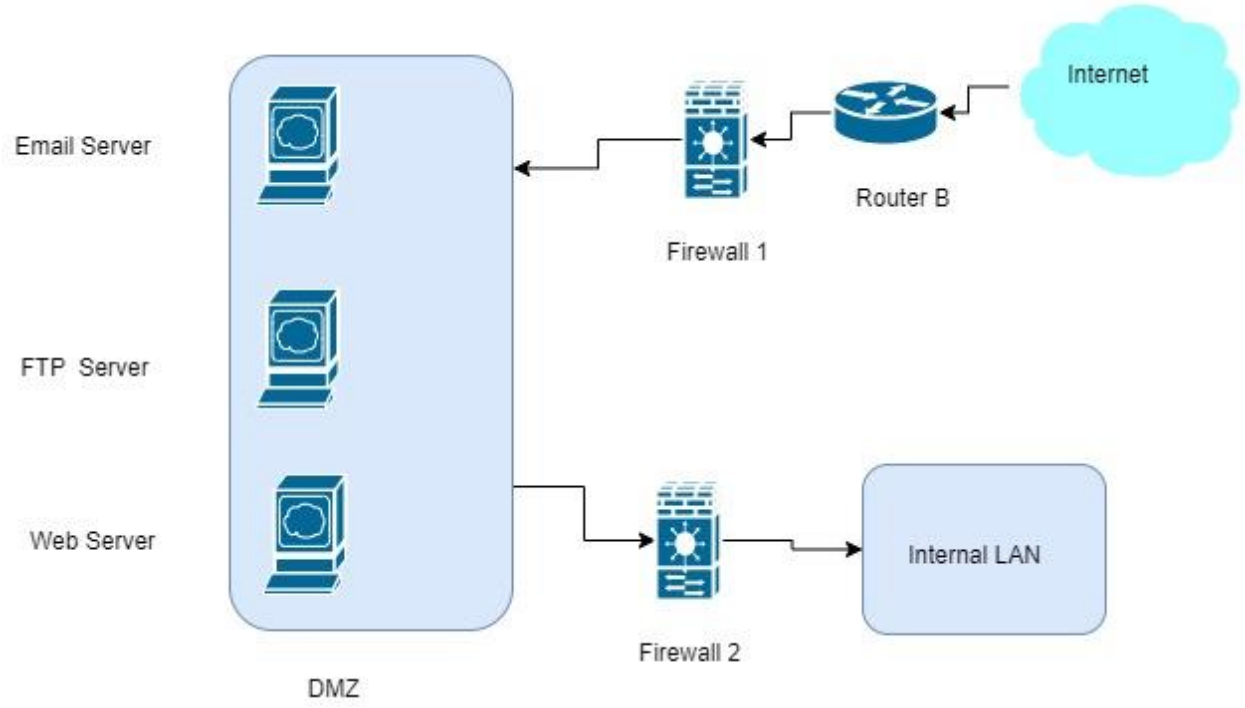
a. Type 1 is something you know. An example of Type 1 would be a password.
b. Type 2 is something you have. An example of Type 2 would be something like a smart card, RFID, ID badges, or text sent to your preregistered smartphone.
c. Type 3 is something you are. An example of Type 3 would be your biometrics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

With multifactor authentication, Company Techs would have the security that protects them from many attacks.

Network of Corporation Techs



DMZ of Corporation Techs



References

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