James Everett Tourtellotte IV

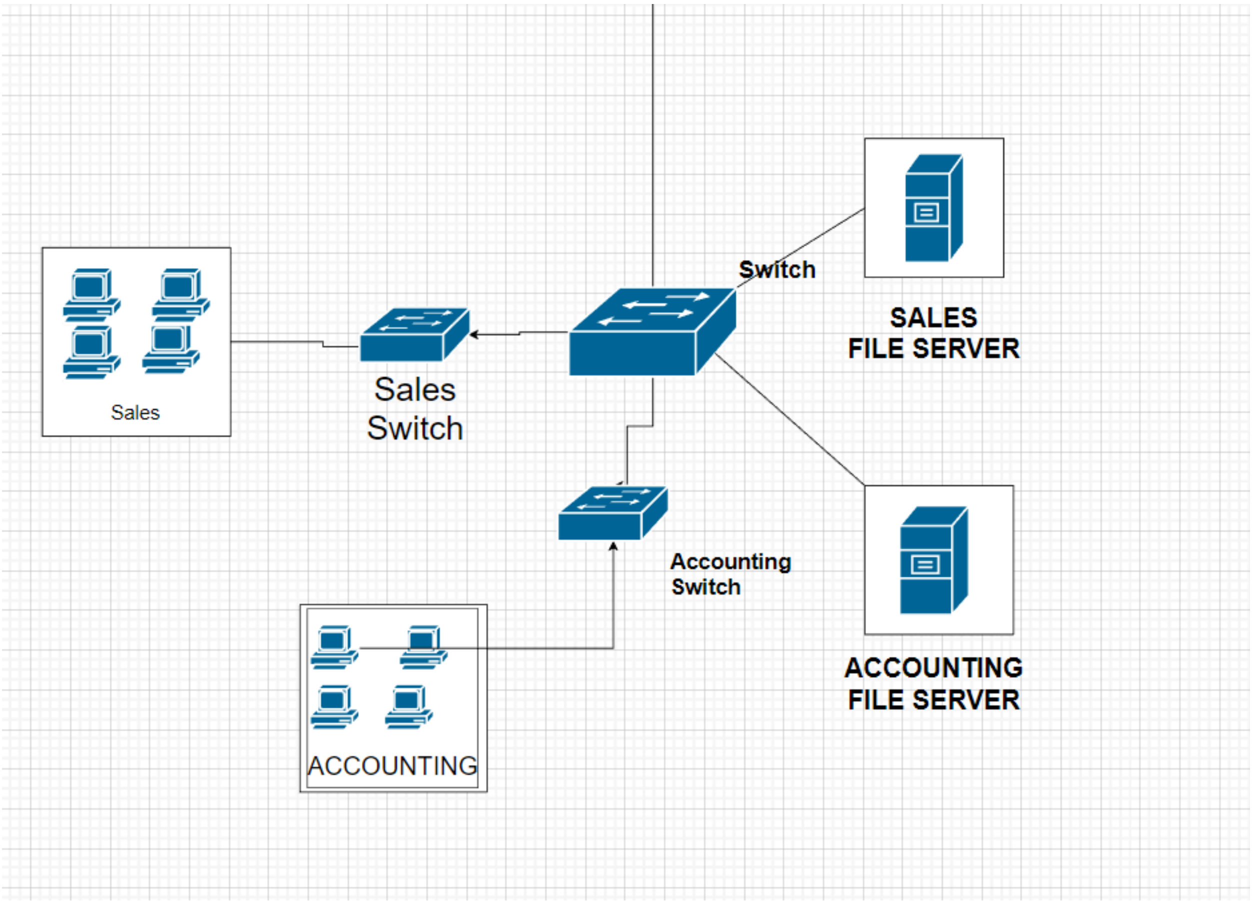
ITN 263

3/5/2023

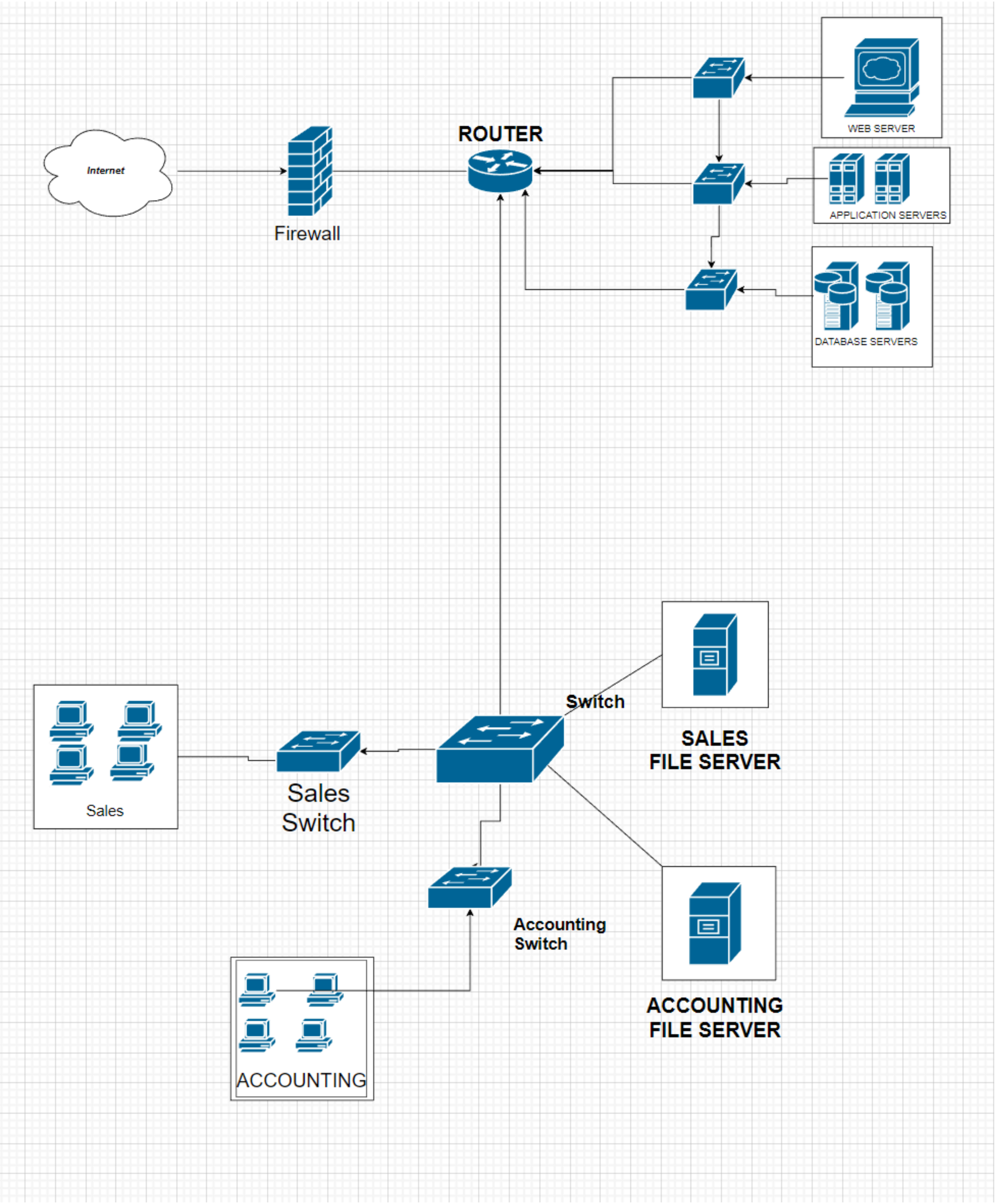
Project Part 1

Given the Corporation Techs' current network consists of 1 web server accessible by the public, 2 application servers, 2 database servers, 2 file and print servers, and 50 workstations, I would separate them in a manner that allows full functionality to the public and internal network. This would be done through a method of segmentation, by means of switches.

These fifty workstations would be presumably split equally into two subnets connected to their own respective switches. This is to control access of data flow from what I would refer to as the intranet, in this situation. Below is a figure of two subnets, connected to two switches, connected to another switch, that has both Fileservers connected to the aforementioned switch.



The aforementioned switches would use access control to determine which data flows into and out of the file servers, and into and out of the switch - in regards to internet access. That switch would be connected to a router, which is connected to three other switches and a firewall. Below is the figure showing the aforementioned network portion connected to the router.


Internet
Firewall
ROUTER
WEB SERVER
APPLICATION SERVERS
DATABASE SERVERS
Switch
SALES
FILE SERVER
Sales
Sales
Switch
Accounting
Switch
ACCOUNTING
FILE SERVER
ACCOUNTING

As you can see, each switch that is connected to the router would be connected to: a web server, the two application servers, the two database servers, and then each other respectively. They would be connected to each other as the router cannot forward MAC Address information to maintain Web Server Functionality. The edge firewall will be placed between the internet and the router. The router will send users to the website/webserver. By doing this configuration, the employees can access the web server along with the end users.

I myself would not however remain using IPv4, I would opt to upgrade to IPv6. IPv4 addresses are limited in number and limited in security. IPv6 can authenticate the network's packets. This extra layer of security is net positive when designing a network. I myself would recommend that given the opportunity the corporation should make the switch as soon as possible.

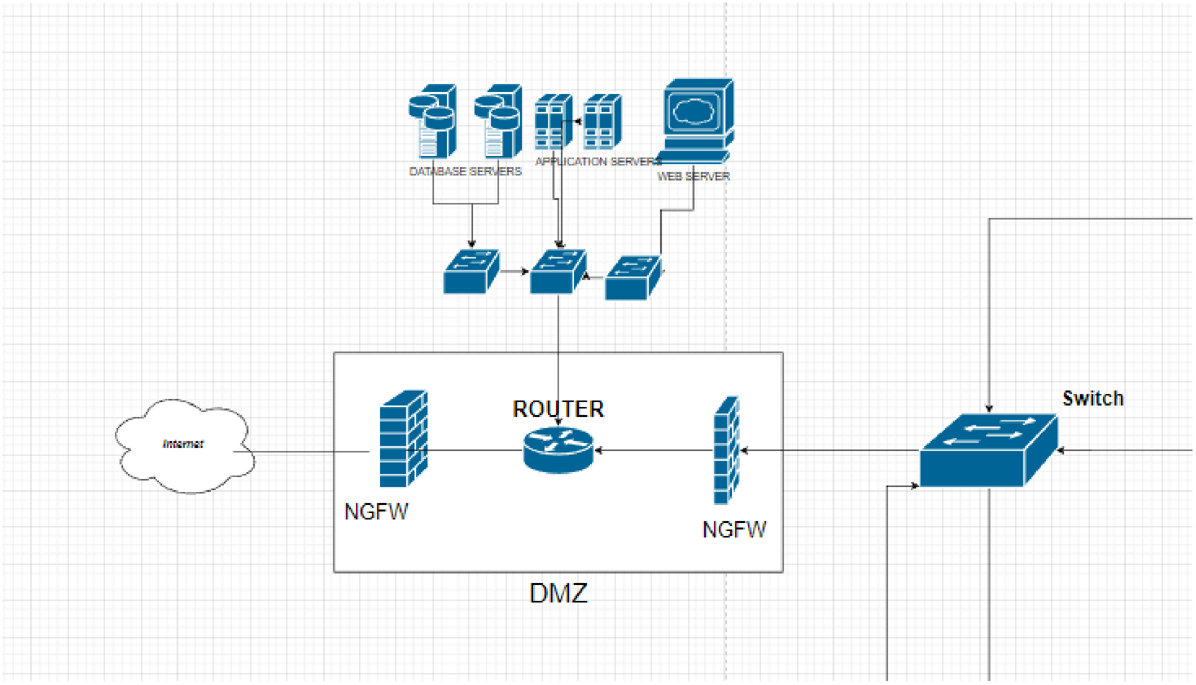
James Everett Tourtellotte IV

ITN 263

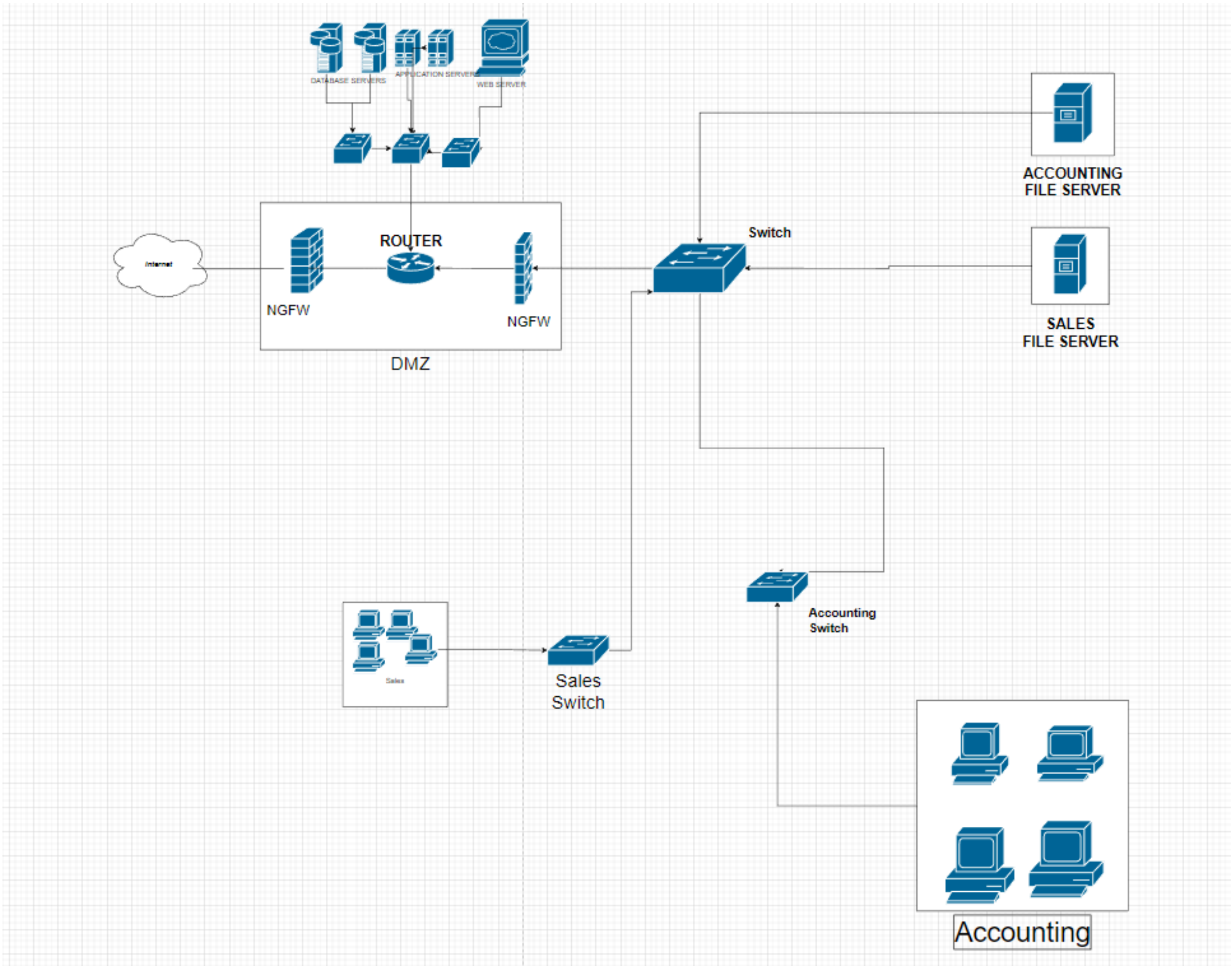
3/5/2023

Project Part 2:

In regards to the previous network configurations, under the current circumstances, I would make the following implementations to the network. First I would replace the edge firewall with a Next-Generation Firewall. I would also add a Next-Generation Firewall between the router connected to the switch from the intranet/company LAN. This would be to ensure full availability between the customers from the internet and the employees from the LAN. Both firewalls would have control of ingress and egress traffic from both directions, ensuring a fully Demilitarized zone in the network. Below is a figure of the NGFW added between the router and the meshed switches:



If the mission is to maintain functionality that allows both departments to access the internet on the same network their web server is on you need to be able to have the web server provide the data for both parties. You will be able to implement access control for users within the intranet by a numerous amount of ways. It could use Deep Packet Inspection (DPI) to prevent database server data from going to the wrong user. It could serve as an Intrusion Prevention System (IPS) by sitting on the edge of the network as well. It is the future of network protection, so in regards to the task at hand it provides both efficiency and efficacy. Below is a fully updated diagram of the new Network:



The aforementioned uses of an NGFW are what makes me use a firewall to establish a DMZ - specifically around the router. With a Next-Generation Firewall you have the state-of-the-art configurations to prevent data from being exfiltrated by people from outside the internet, but also within your own network. It allows only certain packets to enter and exit the most crucial aspect of the network, that is why you want that area to be a DMZ.

In terms of applying a more secure form of authentication, two-factor authentication comes to mind. We would use this for the web server on the appropriate location. This two-factor authentication would run via a cloud-based MFA solution. Either Google Authenticator or Microsoft Authenticator. This solution provides a quick and easy means of authentication that is cheaper and just as effective. This saves money and provides the solution required. You can typically use a mobile application or a hardware token to provide the second factor of authentication, and it can be integrated with your existing authentication system, such as LDAP or Active Directory.

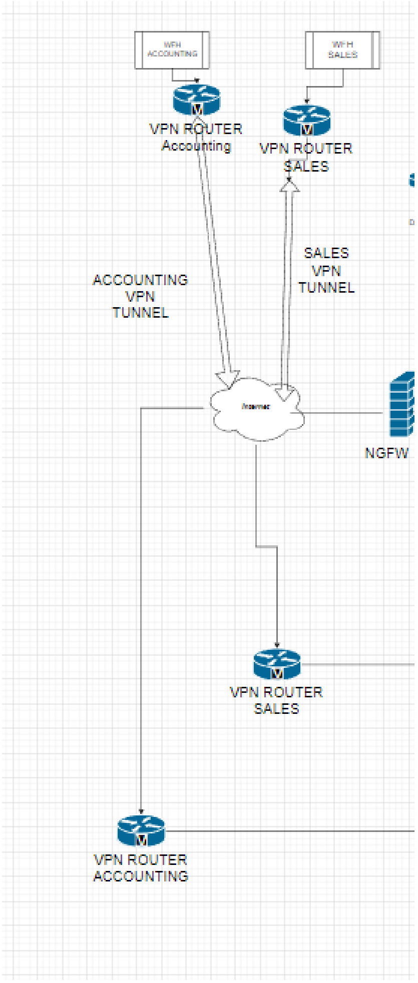
James Everett Tourtellotte IV

ITN 263

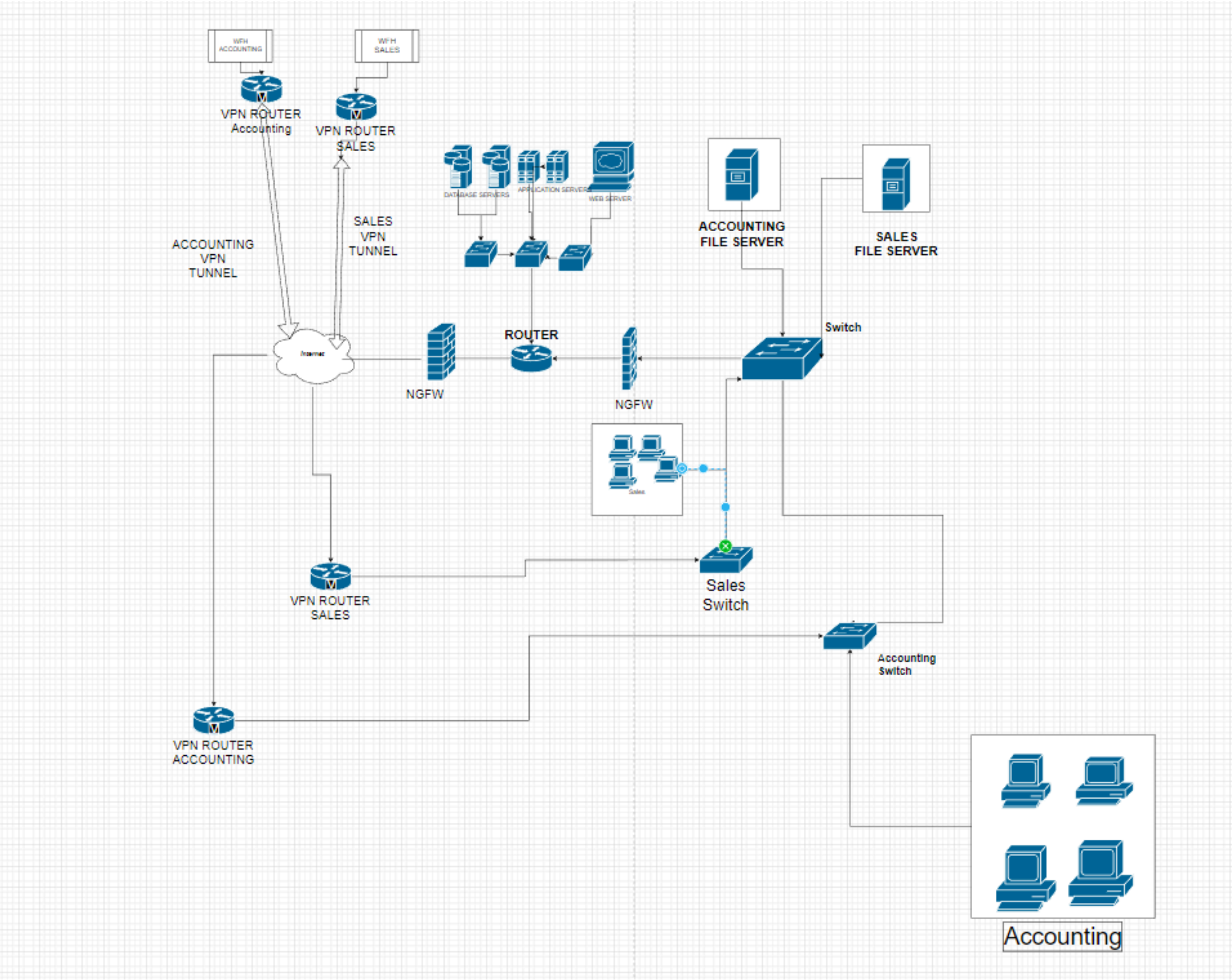
3/5/2023

Project Part Three

In regards to the current network configurations, I would only add two VPN routers to the entire network design. These two routers would be separated by department, each receiving from an SSL/TLS VPN that is for their respective department. Below is a figure depicting that segment of the network by itself:



As depicted above one can see the VPN Router for each department is connected to the respective switch of the internal employees department.This allows for, hopefully, similar access control rules to be applied in relation to the flow of data for each department. It would do this whilst also not compromising network functionality, as the VPN routing is a very separate aspect of this network. Below is a figure of the entire network diagram including the solution for the Work at Home employees:



This is a crucial aspect for the business to take note on as it leaves so much room for scaling. Even under the condition that all your employees become “Work from Home”, using this routing configuration allows for great scaling in the event it is necessary. You could remove all those workstations if need be, as the respective VPNs are connected to their respective switches.