CNIT 45500: Network Security

CNIT45500-010

Group 32

Ethn Hammond

Tyler Hiatt

Submitted To: Tony Wan

Date Submitted: 09/21/23

Date Due: 09/22/23

TABLE OF CONTENTS

BUSINESS CASE

ET Corp is a tech company that is creating an environment with multiple complex features. Security is a great concern of ET Corp, and it is imperative that there is a DMZ in between the public internet and their two private network segments. In order to have a fully functional environment, ET Corp integrated network security into their environment by adding 2 firewalls leading to their own DMZs and private networks. They added a private A network behind a pfSense firewall, and private B network behind a VyOS firewall with their own CentOS machines for DMZs. They did this to test the different ways that firewalls can be implemented into an environment. SNAT and routing were also used to test usability and efficiency on both sides of the network. The most important part of having a firewall is having rules to let traffic in/out and block traffic in/out. On both sides, All traffic from the DMZ to the public network were blocked other than FTP, TFTP, HTTP, and ICMP. This blocks all traffic from the outside internet into the DMZ that does not come on one of those ports or from a specific IP address. This also blocks users from inside the network reaching places that they shouldn't be. This must be used in corporations to lock down sensitive information and prevent unauthorized access from the internal networks.

PROCEDURES

The formatting key of the following section will obey rules below: buttons are **bold**; options are *italicized*; text entered into the computer is in `Courier New style`; menu, folder navigation, and repetitive commands are shown with the pipe symbol and are *italicized*: *Start* | *Programs* | *MS Office* | *Word*.

Installing and Provisioning VMs

To implement network security in an environment, a test environment of VMs were created and provisioned.

1. Installed and provisioned 1 Windows Server 2019 VM.
2. Installed and provisioned 1 Windows Server 2022 VM.
3. Installed and provisioned 2 Almalinux 9 VMs.
4. Installed and provisioned 1 Windows 11 VM.
5. Installed and provisioned 1 VyOS VM.
6. Installed and provisioned 1 pfSense VM.

Network Configuration

After creation of the VMs, the network interfaces of all of the machines needed to be configured with the right port groups and IP addresses.

1. Opened vSphere and clicked on the networking tab

2. Selected the Group 32 vSwitch and created 4 new port groups named privA, privB, vyosDMZ, and pfsenseDMZ.
3. Added the following port groups to the machines:
    a. CentOSA: pfSenseDMZ
    b. CentOSB: vyosDMZ
    c. pfSense: CNIT455G32, pfSenseDMZ, privA
    d. vyosFW: CNIT455G32, privB, vyosDMZ.
    e. Winpublic: CNIT455G32
    f. winsrvA: privA
    g. winsrvB: privB
4. Added IP addresses according to the IP addressing sheet in Appendix B.

Windows Server Configuration

Windows servers were installed for domain controllers so that the machines can all be on different domains for testing purposes.

1. Added Active Directory Domain Services to both Windows Servers in Server Manager.
2. Created new forests and domains on each domain controller.
3. Added FTP and TFTP client features on the domain controllers through server manager.

PfSense Configuration

pfSense was the first firewall method that was going to be used in the VM test environment. This is a GUI based firewall solution for packet filtering.

1. Navigated to Firewall/NAT/1:1

2. Entered the following settings:
    a. Interface
        i. WAN
    b. External IP
        i. 44.104.32.10
    c. Internal IP
        i. 192.168.1.11
    d. Destination IP
        i. *
3. Navigated to Firewall/Rules/WAN
    a. Created a rule to allow any any
4. Navigated to Firewall/Rules/LAN
    a. Created a rule to allow any any
5. Navigated to Firewall/Rules/OPT1
    a. Created a rule to allow any any
6. Navigated to Interfaces/Interface Assignments
    a. Matched the NIC MAC addresses to the appropriate interfaces.
    b. Created OPT1 interface for Private A

VyOS Configuration

VyOS was the second firewall solution that was implemented to do routing instead of SNAT to the DMZ.

1. Used conf to enter configuration mode.

2. Typed interfaces ethernet eth{0,1,2} address *ip address* to add IP addresses to the interfaces.
3. Entered protocols static route 0.0.0.0/0 next hop 44.104.32.1.
4. Used nat source rule 100 outbound-interface eth0 to set the uplink.
5. Used nat source rule 100 source address 192.168.2.0/24 to set the source address.
6. Entered nat source rule 100 translation address masquerade to use nat overload.

VyOS Firewall Configuration

After the installation and initial configuration, the VyOS firewall needed to be configured to block and allow specific traffic.

1. Used conf to enter configuration mode.
2. Entered the following commands for the DMZ firewall name:
    a. Firewall name DMZ{
        i. default-action drop
        ii. rule 100 action accept
        iii. rule 100 destination port 69
        iv. Rule 100 protocol tcp
        v. Rule 105 action accept
        vi. Rule 105 destination port 69
        vii. Rule 105 protocol udp
        viii. Rule 110 action accept
        ix. Rule 110 destination port 21
        x. Rule 110 protocol tcp

xi. Rule 115 action accept

xii. Rule 115 destination port 20

xiii. Rule 115 protocol tcp

xiv. Rule 120 action accept

xv. Rule 120 protocol icmp

3. Entered the following commands for the private firewall name:

    a. Firewall name PubToPriv{

        i. Default-action drop

        ii. Rule 200 action accept

        iii. Rule 200 destination port 80

        iv. Rule 200 protocol tcp

        v. Rule 205 action accept

        vi. Rule 205 destination port 69

        vii. Rule 205 protocol udp

        viii. Rule 210 action accept

        ix. Rule 210 destination port 21

        x. Rule 210 protocol tcp

        xi. Rule 215 action accept

        xii. Rule 215 destination port 20

        xiii. Rule 215 protocol tcp

        xiv. Rule 220 action accept

        xv. Rule 220 protocol icmp

4. Added the firewall names to the DMZ interface using interfaces ethernet eth1 firewall out name DMZ.
5. Added the firewall names to the private interface using interfaces ethernet eth2 firewall in name PubToPriv

CentOS FTP Server Configuration

FTP Server was installed on both DMZ machines for port testing purposes. This is also to be unblocked on both firewalls.

1. Installed FTP with Sudo dnf install vsftpd
2. Started the service with Sudo systemctl start vsftpd
3. Enabled the service with Sudo systemctl enable vsftpd –now
4. Added a user with Sudo adduser ftpuser
5. Added a password with sudo passwd ftpuser
6. Created the user's home directory with Sudo mkdir -p /home/ftpuser/ftp_dir
7. Changed file permissions with Sudo chmod -R 750 /home/ftpuser/ftp_dir
8. Changed file ownership with Sudo chown -R ftpuser: /home/ftpuser/ftp_dir
9. Sudo bash -c 'echo ftpuser >> /etc/vsftpd/user_list'
10. Added the following lines to /etc/vsftpd/vsftpd.conf
    a. anonymous_enable=NO
    b. local_enable=YES
    c. chroot_local_user=YES
    d. allow_writeable_chroot=YES
    e. pasv_min_port=30000

f. pasv_max_port=31000

g. userlist_file=/etc/vsftpd/user_list

h. userlist_deny=NO

i. Sudo systemctl restart vsftpd

j. Sudo systemctl stop firewalld

Centos TFTP Server Configuration

TFTP Server was installed on both DMZ machines for port testing purposes. This is also to be unblocked on both firewalls.

1. Used sudo dnf makecache to update the repo.
2. Used sudo dnf install tftp-server to install TFTP.
3. Used $ sudo cp -v /usr/lib/systemd/system/tftp.service/etc/systemd/system/tftp-server.service
4. Used $ sudo cp -v /usr/lib/systemd/system/tftp.socket/etc/systemd/system/tftp-server.socket
5. Added the following lines to /etc/systemd/system/tftp-server.service:
    a. Requires=tftp-server.socket
    b. ExecStart=/usr/sbin/in.tftpd -c -p -s /var/lib/tftpboot
    c. WantedBy=multi-user.target
    d. Also=tftp-server.socket.
6. Added the following lines to /etc/systemd/system/tftp-server.socket:
    a. WantedBy=sockets.target
    b. BindIPv6Only=both

7. Used systemctl enable tftp-server.service to enable the service.
8. Used systemctl start tftp-server.service to start the service.
9. Used sudo chmod 777 /var/lib/tftpboot to set permissions on the TFTP directory.

HTTP Server CentOS Installation

HTTP Server was installed on both DMZ machines for port testing purposes. This is also to be unblocked on both firewalls.

1. Used sudo dnf install httpd to install apache services.
2. Sudo firewall-cmd –permanent –add-service=https.
3. Sudo firewall-cmd –reload.
4. Used systemctl start https to start HTTP
5. Created a directory with sudo mkdir -p /var/www/g2.com/html
6. Used sudo mkdir -p var/www/g2.com/log
7. Entered sudo chown -R $USER:$USER /var/www/example.com/html
8. Used sudo chmod -R 755 /var/www
9. Entered sudo vi /var/www/example.com/html/index.html
10. Used sudo mkdir /etc/httpd/sites-available /etc/httpd/sites-enabled
11. Entered sudo vi /etc/httpd/conf/httpd.conf

RESULTS

All virtual machines were configured to communicate with each other via their IP addresses, MAC addresses, DNAT/PAT, SNAT, routing, and domains. Then, firewall rules were implemented to block unnecessary traffic from reaching the internal network, and unauthorized traffic from the internal outbound. DMZs were implemented to act as a buffer between the public network and the private network. From the public network, the DMZ takes blocked traffic and routes it back to the firewall and out to the private network. This is to create a zone that traffic can flow into and go through a packet filter before it reaches the private network. It also creates a buffer zone from the private network out to the public to be filtered via firewall rules. HTTP, FTP, and TFTP services were implemented successfully to test allowing and blocking different ports from accessing the private network behind the firewall.

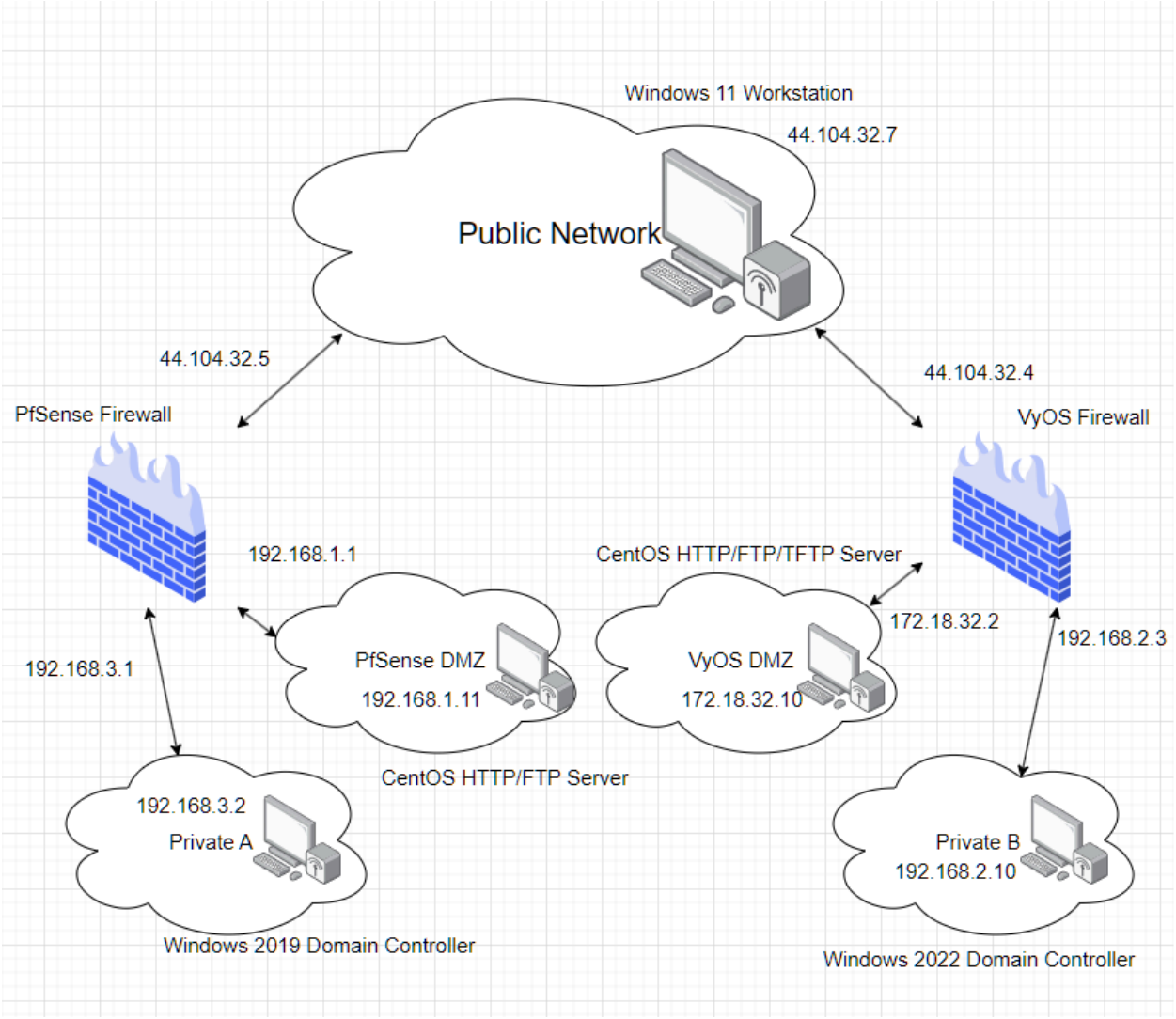

Figure 1.1: Screenshot of the Logical Diagram

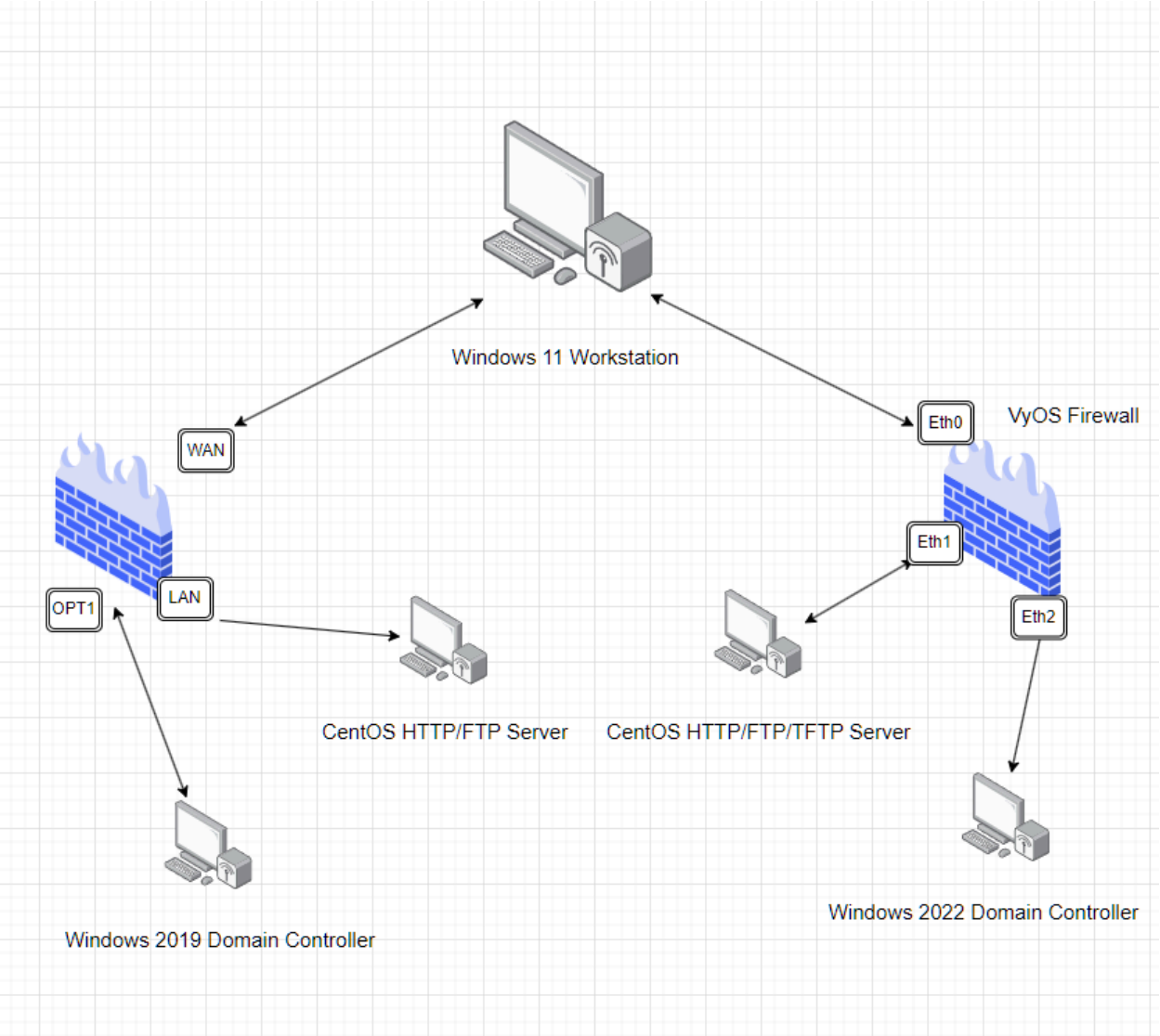

Figure 1.2: Screenshot of the Physical Diagram

CONCLUSIONS AND RECOMMENDATIONS

Upon completion of the architecture, there are a few things that could have been completed in a more efficient manner. To start off, it would be important to ensure connectivity is completely established before any sort of firewall rules take place. If other priorities are being pursued before communication and availability is established, this could make troubleshooting much more difficult. It is also important to double check NAT settings, network settings, NIC settings, and DNS settings before moving on with other troubleshooting efforts. In addition to basic troubleshooting, all services should be reset after being fully configured in order for a fresh start to occur. Sometimes services can be configured properly, but simply need a restart in order to begin operation.

Overall, the implementation of VyOS, PfSense, two domain controllers, two DMZ machines, and a public server allowed for an efficient topology. Firewall rules allow certain traffic to enter into the architecture, and this helps protect the business and environment overall. In the future, these recommendations should be taken into consideration in order for deployment time reduction. Other than the recommendations, there should be no other changes in the methods performed.

REFERENCES

Firewall. Firewall - VyOS 1.3.x (equuleus) documentation. (n.d.). https://docs.vyos.io/en/equuleus/configuration/firewall/index.html

Kumar, P., Zoran, Vyas, Kiarie, J., Rjr, Gricel, Jake, & Blade. (2021, January 12). *How to install vsftpd (FTP Server) on centos 8 / rhel 8*. |. https://www.linuxtechi.com/install-vsftpd-server-centos-8-rhel-8/

Mills, H., & Glass, E. (2020, April 24). *How to install the apache web server on centos 8*. DigitalOcean. https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-centos-8

Nat. NAT - VyOS 1.3.x (equuleus) documentation. (n.d.). https://docs.vyos.io/en/equuleus/configuration/nat/index.html

Shovon, S. (1966, January 1). Configure TFTP server on centos 8. https://linuxhint.com/tftp_server_centos8/

APPENDIX A: PROBLEM SOLVING

Problem 1: CentOSB Connectivity Issues

Problem Description: CentOSB did not have internet connection, and was not able to communicate with other devices in the environment.

Problem Solutions: The first solution is the classic turn off the interface and turn it back on. This would hopefully reset the connections and flush any caches that may be affecting the connectivity status of the machine. Another solution could be resetting the IP address on the device and rebooting VyOS. This could potentially refresh the connections to other devices as well. Another potential solution is to double check that NAT and the firewall rules are properly configured.

Solutions Attempted: The solutions that were attempted included double checking the network settings and the NAT and firewall rules, and also powering the interface off and turning it back on.

Final Solution: The final solution that worked was turning the interface off and back on again. This refreshed all connections, flushed all caches, and allowed the devices to successfully communicate with each other as required.

Problem 2: NAT Issues with PfSense

Problem Description: The PfSense DMZ was having issues reaching the internet, and the ultimate issue was misconfigured NAT and this ultimately prevented the DMZ from receiving a proper IP address.

Problem Solutions: The first solution could be to reset the PfSense machine to reset and reestablish connections. Another potential solution could be to change the NAT settings to different machines and IP addresses. A third solution could be to change the NICs on the machines.

Solutions Attempted: The solutions that were attempted included resetting the PfSense machine and changing the NAT settings around.

Final Solution: Changing the NAT settings around successfully solved the issue at hand. The PfSense DMZ started receiving internet connections, and was able to communicate effectively with the environment.

Problem 3: CentOSA Connectivity Issues

Problem Description: CentOSA did not have internet connection, and was not able to communicate with other devices in the environment.

Problem Solutions: The first solution is the classic turn off the interface and turn it back on. This would hopefully reset the connections and flush any caches that may be affecting the connectivity status of the machine. Another solution could be resetting the IP address on the device and rebooting PfSense. This could potentially refresh the connections to other devices as well. Another potential solution is to double check that NAT and the firewall rules are properly configured.

Solutions Attempted: The solutions that were attempted included double checking the network settings and the NAT and firewall rules, and also powering the interface off and turning it back on.

Final Solution: After troubleshooting with these solutions, we found that none of them worked and a solution still needs to be discovered. The next step is to completely delete and provision a new machine to replace it, as this will give us a fresh start with completely new configurations, settings, and caches.

APPENDIX B: IP Addressing

CentOSA: 192.168.1.11

CentOSB: 172.18.32.10

pfSense:

- Public NIC:44.104.32.5
- DMZ NIC: 192.168.1.1
- PrivA NIC: 192.168.3.1

VyOS:

- Public NIC: 44.104.32.4
- DMZ NIC: 172.18.32.2
- PrivB NIC: 192.168.2.3

Winpublic: 44.104.32.7

WinsrvA: 192.168.3.2

WinsrvB: 192.168.2.10