Lab 1: Firewall Configuration and Management

Josh Lieberg

Submitted To: Tony Wan

Date Submitted: 9/16/24

Date Due: 9/16/24

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report provides a comprehensive summary of the Firewall Configurations and Management lab, which is a critical project for Computer Industries. The primary purpose of this initiative is to develop, expand, and secure the company's IT infrastructure by implementing robust firewall solutions that protect sensitive internal assets while also providing secure access to external networks. As the company rapidly expands and relies increasingly on digital operations, the need for a segmented and protected network becomes essential to maintain business continuity.

The execution of this project encompasses the installation and configuration of key network infrastructure services to enhance security and productivity across the organization. Several objectives have been outlined for this initiative. First, internal systems—such as critical domain controllers and internal services—must be protected from unauthorized access. Second, external services must be enabled within the DMZ, allowing clients and partners to securely access critical resources while isolating them from the internal network. Third, inbound and outbound traffic must be closely monitored and controlled using the firewalls, which is essential for preventing data breaches and securing proprietary information. Finally, this expansion will provide the company with a fully scalable network, allowing for future service additions or geographic expansion while maintaining a high level of security.

Key technological implementations include the setup of pfSense and VyOS firewalls, each with distinct zones to ensure strong security while effectively managing internal and external traffic. This executive summary reflects the strategic approach and technological advancements anticipated from the Firewall Configuration and Management lab. Additionally, it outlines Computer Industries' commitment to innovation and the adoption of technologies that

guarantee the security, efficiency, and scalability of its IT infrastructure, all while supporting long-term business growth and operational resilience.

BUSINESS CASE

Computer Industries is currently expanding its operations and thus needs to adopt a new structure to support a more scalable and secure network. The company plans to transition its systems to a hybrid architecture that utilizes both UNIX based and Windows based systems. The goal of this design is to enhance operational efficiency, reduce management costs, and improve the overall security of the company.

The proposed solution focuses around the deployment of two separate firewall architectures, pfSense and VyOS. The pfSense firewall is a FreeBSD based firewall that will secure traffic between the Internet, DMZ, and internal networks. It will enable port address translation (PAT) and dynamic NAT (DNAT) in order to manage traffic between the public networks and private networks. This setup is crucial as the Windows Server 2019 domain controllers, which are located in the private network, must communicate securely with external systems.

A second firewall will be configured, a VyOS firewall. The purpose of this firewall is to isolate the DMZ from the public network. This isolation ensures that the internal network remains protected and secure from potential external threats. With this secure network in place, services such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP) will be protected. The added benefit of this architecture is that authorized users will have easier access to these services while maintaining strong security. Pictured below in Figure 1 is the Logical Diagram for the newly proposed network infrastructure.

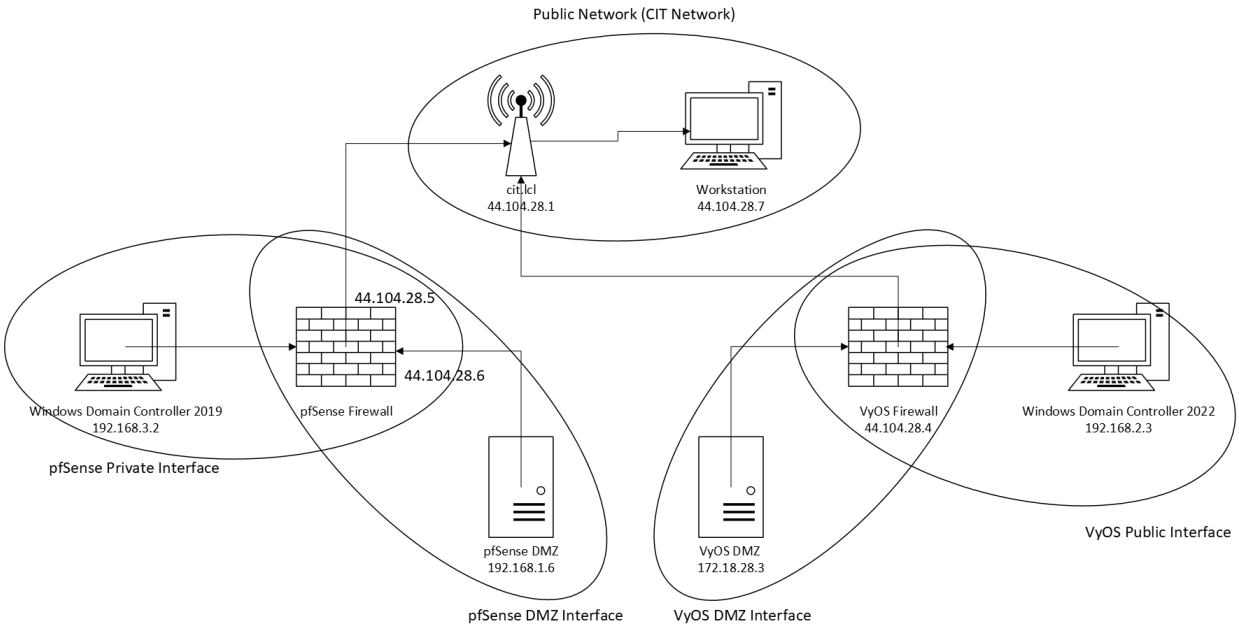

Figure 1: Logical Diagram

During the expansion, several domain controllers will need to be deployed along with Domain Name System (DNS) services. Microsoft Windows Server 2019 will be deployed on the Private A side of the network. Microsoft Windows Server 2022 will be deployed on the Private B side of the network. These active directory servers will centralize authentication, improve stability, and provide security to the infrastructure.

Firewall rules will be set to filter traffic between different network segments. These rules will ensure that communications are secure while also limiting access to only authorized users. The process will utilize pfSense firewall rules to actively monitor and filter traffic, ensuring that only permitted communications occur and that unauthorized traffic is blocked. This comprehensive network upgrade aligns with Computer Industries expansion and future growth plans. The deployment of multiple firewalls, DNS management, and centralized authentication will not only improve security but also enhance scalability and operational efficiency across the

organization. This infrastructure will provide Computer Industries with a robust, future proof network that supports current operations and enables growth without compromising security.

PROCEDURES

This procedure section goes phase by phase for the objectives completed during lab two, Microsoft Windows Administration. The troubleshooting techniques used can be found in Appendix A. In this section, the **buttons** used will be in bold, typed in computer instructions are in `Courier New`, *options* selected/pressed will be italicized, and steps requiring menu navigation will be represented by the pipe symbol. In rare occurrences, there are sometimes *options* interpreted as a **button**, which is represented by both italicized and bolded ***words***.

Table 1. Formatting Key

Representation	Format in Report
Button	**Button**
Options	*Options*
Text Entered in Computer	`Courier Text`
Menu Navigation	*Start* | *Programs* | *MS Office* | *Word*

Creation of Windows 10 Workstation

The following steps cover the installation process for the latest version of Windows 10 for future use of desired Computer Industries clients which is installed from an ISO image. The following procedures are from start to finish.

1. Right clicked on *CNIT455G28* | *New Virtual Machine…* | **Next** | Named machine name: `CNIT45500.g28.WindowsPUBLIC` | **Next** | *stvmsrv22haas.cit.lcl* | **Next** | *HaaS Storage Cluster* | **Next** | **Next** | *Windows* | *Microsoft Windows 10 (64-bit)* | **Next** | `4 CPU 8GB memory 50GB` | Selected *Thin Provision* | *CNIT455G28* | *New CD/DVD file* | *Datastore ISO File* | *rtfmhaas.iso* | *Windows* | *Client* | *en-us_windows_10_consumer_editions_version_22h2_x64_dvd_8da72ab3.iso* | **OK** | *Connect at Power On* | **Next** | **Finish**
2. Clicked **Send Control+Alt+Delete** | **Enter** | **Enter** | **Next** | **Install Now**
3. Pressed **Next** | Entered `YP8N9-2VG2H-92278-BRC7J-82QFM` | **Next**
4. Selected *Windows Server 2019 Standard (Desktop Experience)* | **Next** | *I accept license terms* | **Next** | *Custom Install* | **Next**
5. Selected *Yes* | *Yes* | *Skip* | *I don't have internet* | *Continue with limited setup*
6. Typed `Public` | **Next** | Typed Secure Password | **Next**
7. Selected *What was your first pet's name?* | Typed `Deadman` | **Next** | *What was your childhood nickname?* | `Deadman` | **Next** | *What's the first name of your oldest cousin?* | `Deadman` | **Next** | *Accept* | *Not Now*
8. Opened *Control Panel* | *Network and Internet* | *Network and Sharing Center* | *Change adapter settings* | *Ethernet* | *Properties* | *Internet Protocol Version 4 (TCP/ IPv4) Properties*

9. Typed in *IP address, subnet mask, default gateway* for `WindowsPUBLIC`
10. Selected *Use the following DNS server addresses* | Typed in *Preferred DNS Server, Alternate DNS Server* for `WindowsPUBLIC`| **OK | Yes**

Creation of Private A Domain Controller

The following steps cover the installation process for the latest version of Windows Server 2019 which is installed from an ISO image. Installing the latest version of Windows Server 2019 is important because the latest version ensures the Virtual Machine (VM) installed will work properly and not corrupt due to any legacy glitches not patched. Windows Server 2019 will allow the VMs to create Microsoft Active Directories. For network configurations, please refer to Appendix B: Table 1.

1. Right clicked on *CNIT455G28* | *New Virtual Machine…* | **Next** | Named machine name: `CNIT45500.g28.PrivA` | **Next** | *stvmsrv22haas.cit.lcl* | **Next** | *HaaS Storage Cluster* | **Next** | *Windows* | *Microsoft Windows Server 2019 (64-bit)* | **Next**
2. Configured Virtual Machine with *4 CPU 4GB memory 50GB* | Selected *Thin Provision* | *CNIT455G28* | *New CD/DVD file* | *Datastore ISO File* | *rtfmhaas.iso* | *Windows* | *Server* | *en-us_windows_server_2019_x64_dvd_f9475476.iso* | **OK** | *Connect at Power On* | **Next** | **Finish**
3. Clicked **Send Control+Alt+Delete** | **Enter** | **Next** | **Install Now**
4. **Next** | Typed `N69G4-B89J2-4G8F4-WWYCC-J464C` | **Next**
5. Selected *Windows Server 2019 Standard (Desktop Experience)* | **Next** | *I accept license terms* | **Next** | *Custom Install* | **Next**
6. Entered Password | **Finish** | **Send Ctrl-Alt-Delete**

7. Entered Login Credentials
8. Right clicked Internet Icon | *Open Network and Internet Settings* | *Change Adapter Settings* | *Ethernet* | *Properties* | *Internet Protocol Version 4 (IPv4)* | **Properties |** *Use the following IP address:* | Configured Static IP according to Appendix B
9. Right clicked on *CNIT45500.g28.privA* | *Edit settings…* | *Add New Device* | *Network Adapter* | *Browse…* | *Private-A* | **OK** | **OK**

Promoted Private A and Private B to Domain Controller

The following steps cover the process of promoting the newly created Private A and Private B virtual machines to a domain controller. Promoting these machines to a domain controller allows for the computers in the domain to be on a centralized network.

1. Selected *Manage* | *Add Roles* | **Next** | **Next** | **Next** | *Active Directory Domain Services* | **Add Features** | *DNS Server* | **Add Features** | **Next** | **Next** | **Next** | **Next** | *Restart the destination server automatically if required* | **Yes** | **Install** | **Close**
2. Clicked *Flag Notification* | *Promote this server to a domain controller* | *Add a new forest*
3. Typed `PrivA.lcl` | **Next**
4. Entered a password for DSRM | **Next** | **Next** | **Next** | **Next** | **Next**
5. Selected *Install* **| Restart Now**
6. Repeated Steps 1-5 while on Private B to promote that machine to a domain controller

Creation of the Private B Domain Controller

The following steps cover the installation process for the latest version of Windows Server 2019 which is installed from an ISO image. Installing the latest version of Windows

Server 2019 is important because the latest version ensures the VM installed will work properly and not corrupt due to any legacy glitches not patched. Windows Server 2019 will allow the VMs to create Microsoft Active Directories. For network configurations, please refer to Appendix B: Table 1.

1. Right clicked on *CNIT455G28* | *New Virtual Machine…* | **Next** | Named machine name: `CNIT45500.g28.PrivB` | **Next** | *stvmsrv22haas.cit.lcl* | **Next** | *HaaS Storage Cluster* | **Next** | *Windows* | *Microsoft Windows Server 2022 (64-bit)* | **Next**
2. Configured Virtual Machine with *4 CPU 4GB memory 50GB* | Selected *Thin Provision* | *CNIT455G28* | *New CD/DVD file* | *Datastore ISO File* | *rtfmhaas.iso* | *Windows* | *Server* | *en-us_windows_server_2022_updated_july_2023_x64_dvd_541692c3.iso* | **OK** | *Connect at Power On* | **Next** | **Finish**
3. Clicked **Send Control+Alt+Delete** | **Enter** | **Next** | **Install Now**
4. **Next** | Typed `VDYBN-27WPP-V4HQT-9VMD4-VMK7H` | **Next**
5. Selected *Windows Server 2019 Standard (Desktop Experience)* | **Next** | *I accept license terms* | **Next** | *Custom Install* | **Next**
6. Entered Password | **Finish** | **Send Ctrl-Alt-Delete**
7. Entered Login Credentials
8. Right clicked Internet Icon | *Open Network and Internet Settings* | *Change Adapter Settings* | *Ethernet* | *Properties* | *Internet Protocol Version 4 (IPv4)* | **Properties |** *Use the following IP address:* | Configured Static IP according to Appendix B
9. Right clicked on *CNIT45500.g28.privb* | *Edit settings…* | *Add New Device* | *Network Adapter* | *Browse…* | *Private-B* | **OK** | **OK**

Creation of pfSense Firewall Virtual Machine

The following steps cover the installation process for the latest version of pfSense which is run on a Free-BSD OS. The creation of this VM will allow for Computer Industries to start configuring the firewall to suit correct business operations.

1. Accessed vSphere
2. Clicked CNIT455G28 | **Create a New Virtual Machine**
3. Pressed **Next**
4. Entered `CNIT455.g28.pfSense` | clicked **Next**
5. Selected *stvmsrv22haas.cit.lcl* | clicked **Next** | selected *HAAS Storage Cluster* | clicked **Next** | **Next**
6. Selected *Other* | *FreeBSD 14 or later versions (64-bit)* | clicked **Next**
7. Entered `2` for CPU | entered `4` for memory | entered `16` hard disk
8. Clicked New Hard disk | Disk Provisioning | selected *Thin Provision*
9. Selected New Network | selected *CNIT455G28 Public* | clicked **OK**
10. Clicked New CD/DVD Drive | *Data ISO File* | selected *rtfmhaas.iso* | *pfSense* | pfSense-CE-2.7.2-RELEASE-amd64.iso | clicked **OK**
11. Pressed **Connect At Power On** | **Next** | **Finish**

Configuration of pfSense on CNIT45500.g28.FWALL

The following steps cover the configuration process for the latest version of pfSense which is run on a Free-BSD OS. The configuration of pfSense will allow Computer Industries to start configuring the firewall to suit correct business operations.

1. Powered CNIT34220.Group28.FWALL on
2. Clicked **Launch Web Console**
3. Clicked **Accept**
4. Selected *Installed pfSense* | *Auto Guided Root - ZFS* | clicked **OK**
5. Selected *Stripe*
6. Clicked **OK** | pressed Space bar | clicked **OK**
7. Selected *Proceed with installation*
8. Clicked **Enter** | **YES** | **Reboot**

Creation of pfSense DMZ

The following steps cover the creation process for the latest version of AlmaLinux which is being utilized to run the DMZ VM for pfsense. The creation of this VM will allow for Computer Industries to start configuring the firewall via the web configurator.

1. Right clicked on *CNIT455G28* | *New Virtual Machine…* | **Next** | Named machine name: `CNIT45500.g28.pfDMZ` | **Next** | *stvmsrv22haas.cit.lcl* | **Next** | *HaaS Storage Cluster* | **Next** | *Linux*| *Alma Linux (64-bit)* | **Next**
2. Configured Virtual Machine with *4 CPU 8GB memory 16GB* | Selected *Thin Provision* | *CNIT455G28* | *New CD/DVD file* | *Datastore ISO File* | *rtfmhaas.iso* | *Linux* | *AlmaLinux (CentOS)* | *AlmaLinux-9.3-x86_64-dvd.iso* | **OK** | *Connect at Power On* | **Next** | **Finish**
3. Right clicked on *CNIT45500.g28.pfDMZ* | *Edit settings…* | *Add New Device* | *Network Adapter* | *Browse…* | *DMZ-A* | *OK* | *OK*
4. *Continue* | *Root Password* | *entered secure password* | *Clicked Allow root SSH login with password* | *Done* | *Installation destination* | *Done* | *Begin Installation*

Configuration of 1:1 NAT on pfSense

The following steps cover the process of configuring 1:1 NAT on the pfSense web configurator. This process is done in order to map the internal network of Computer Industries to the external public network.

1. Logged into CNIT45500.g28.pfDMZ
2. Opened Firefox
3. Entered `http://192.168.1.1`
4. Logged into pfSense Web Configurator
5. Clicked *Firewall* | *NAT* | **1:1** | **Add**
6. Selected *WAN* for interface | *Address* for External subnet IP
7. Entered `44.104.28.6`
8. Selected *Address* for Internal IP
9. Entered `192.168.1.6`
10. Clicked **Save**

Configuration of DNAT/PAT on pfSense

The following steps clever the process of configuring DNAT/PAT on pfSense via the web configurator. This process is done to route packets once they reach the firewall. Additionally it allows for Computer Industries to map the internal private addresses to a single external public address.

1. Logged into CNIT45500.g28.pfDMZ
2. Opened Firefox
3. Entered `http://192.168.1.1`

4. Logged into pfSense Web Configurator
5. Clicked *Firewall* | *NAT* | Add
6. Changed *Protocol* to *TCP*
7. Changed Destination Port Range to 80
8. Changed Redirect Target IP to 192.168.3.2
9. Clicked Save
10. Repeated steps 5-9 for FTP (Port 21)

Configuration of pfSense Firewall Rules

The following steps cover the process of implementing rules on the pfSense Firewall vit the web configurator. This process was done in order to correctly manage the flow of traffic from all machines on the network. See Appendix C for full firewall rule tables.

1. Logged into CNIT45500.g28.pfDMZ
2. Opened Firefox
3. Entered `http://192.168.1.1`
4. Logged into pfSense Web Configurator
5. Selected *Firewall* | *Rules*
6. Selected interface as *WAN*
7. Clicked **Add**
8. Edited rules according to Appendix C: Table 1
9. Repeated steps 5-8 for interface LAN and OPT1 using Appendix C: Table 2 and Appendix C: Table 3
10. Selected *Firewall* | *NAT* | *Outbound*

11. Entered configuration using Appendix C: Table 4

Creation of VyOS Router/Firewall

The VyOS machine acts as both a router and a firewall, providing internet connectivity to the private zones on the right side of the network as well as limiting traffic flows. The router allows HTTP and FTP traffic to the pfSense side of the network, while allowing HTTP, FTP, and TFTP traffic to flow into this part of the network.

1. Migrated to https://studentvc.cit.lcl
2. Right clicked *CNIT455G28* | *New Virtual Machine…* | **Next**
3. Named machine `CNIT455.G28.VyOS` | **Next** | *stvmsrv22haas.cit.lcl* | **Next** | *Haas Storage Cluster* | **Next** | **Next |** *Other* | *Other (64-bit)* | **Next**
4. Configured Virtual Machine with *4 CPU 8GB Memory 40GB Hard Disk*
5. Selected *Thin Provision* | *Datastore ISO File* | *rtfm.iso* | *VyOS* | *vyos-1.5-rolling-202406230022-amd64.iso* | **OK** | *Connect at Power on* | **Next** | **Finish**
6. Right clicked on CNIT455.G28.VyOS | Edit Settings | Add New Device | Network Adapter | Browse… | DMZ-B
7. Right clicked on *CNIT455.G28.VyOS* | *Edit Settings* | *Add New Device* | *Network Adapter* | *Browse…* | *Private-B*
8. Right clicked on *CNIT455.G28.VyOS* | *Edit Settings* | *Network Adapter 1* | *Browse…* | *CNIT455G28*

Configured Interfaces on VyOS

In VyOS architecture, interfaces must be made virtually to correlate with physical NICs. Once both the virtual NIC and the physical NIC are matched together, machines are able to have network connectivity. Interfaces are also where firewall rules and other configurations can be placed.

1. Opened VyOS Router VM
2. Typed `configure`
3. Typed `set interfaces ethernet eth0 address 44.104.28.4/24`
4. Entered `set interfaces ethernet eth0 description External`
5. Entered `set interfaces ethernet eth1 address 172.18.28.1/24`
6. Typed `set interfaces ethernet eth1 description DMZ`
7. Typed `set interfaces ethernet eth2 address 192.168.2.1/24`
8. Entered `set interfaces ethernet eth2 description Private B`
9. Entered `set nameserver 44.2.1.44`

Configured Static Routes and NAT

Network Address Translation (NAT) allows for private addresses in a network to reach public facing addresses. VyOS uses a term called ‘masquerade’ to translate these addresses so that they are eligible to reach public sites. Static routes define the path in which traffic will flow to reach the correct public address after traveling through the router.

1. Typed `configure` in VyOS VM
2. Typed `set nat destination rule 20 destination address 44.104.28.4`

3. Entered `set nat destination rule 20 destination port 80`
4. Entered `set nat destination rule 20 inbound interface name eth0`
5. Typed `set nat destination rule 20 protocol tcp`
6. Typed `set nat destination rule 20 translation address 192.168.2.3`
7. Entered `set nat source rule 10 outbound-interface name eth0`
8. Entered `set nat source rule 10 source address 172.18.28.0/24`
9. Typed `set nat source rule 10 translation address masquerade`
10. Typed `set nat source rule 20 outbound-interface name eth0`
11. Entered `set nat source rule 20 source address 192.168.2.3`
12. Entered `set nat source rule 20 translation address masquerade`
13. Typed `set protocols static route 0.0.0.0/0 next-hop 44.104.28.1`

Configure Firewall Rules

Firewall rules are configured in any network to limit network traffic to only allow the necessary movement of PDUs. In this lab environment, HTTP and FTP traffic is allowed between the private networks while FTP is only allowed from the pfSense side to the VyOS side.

1. Typed `configure` in VyOS VM
2. Typed `set firewall global-options all-ping enable`
3. Entered `firewall ipv4 forward filter rule 5 action jump`

4. Entered `firewall ipv4 forward filter rule 5 inbound-interface name eth0`
5. Typed `firewall ipv4 forward filter rule 5 jump-target wan2lan`
6. Typed `firewall ipv4 name wan2lan default -action drop`
7. Entered `firewall ipv4 name wan2lan rule 2 action accept`
8. Entered `firewall ipv4 name wan2lan rule 2 description Allow establihsed/related`
9. Typed `firewall ipv4 name wan2lan rule 2 state established`
10. Typed `firewall ipv4 name wan2lan rule 2 state related`
11. Entered `firewall ipv4 name wan2lan rule 10 action accept`
12. Entered `firewall ipv4 name wan2lan rule 10 destination address 172.18.28.3`
13. Typed `firewall ipv4 name wan2lan rule 10 destination port 80`
14. Typed `firewall ipv4 name wan2lan rule 10 protocol tcp`
15. Entered `firewall ipv4 name wan2lan rule 10 source address 44.104.28.0/24`
16. Repeated steps 11-15 for rules 20, 30, and 40 which allow traffic on ports 69, 20, and 21 respectively

Creation of VyOS DMZ

An Alma Linux machine was created to host certain services for the VyOS side of the network. Configured services in this machine include HTTP, FTP, and TFTP. These services are accessible from a public machine on the laboratory network and the pfSense domain controller.

1. Right clicked on *CNIT455G28* | *New Virtual Machine…* | **Next** | Named machine name: `CNIT45500.g28.VyOSDMZ` | **Next** | *stvmsrv22haas.cit.lcl* | **Next** | *HaaS Storage Cluster* | **Next** | *Linux*| *Alma Linux (64-bit)* | **Next**
2. Configured Virtual Machine with *4 CPU 8GB memory 16GB* | Selected *Thin Provision* | *CNIT455G28* | *New CD/DVD file* | *Datastore ISO File* | *rtfmhaas.iso* | *Linux* | *AlmaLinux (CentOS)* | *AlmaLinux-9.3-x86_64-dvd.iso* | **OK** | *Connect at Power On* | **Next** | **Finish**
3. Right clicked on *CNIT45500.g28.VyOSDMZ* | *Edit settings…* | *Add New Device* | *Network Adapter* | *Browse…* | *DMZ-B* | *OK* | *OK*
4. *Continue* | *Root Password* | *entered secure password* | *Clicked Allow root SSH login with password* | *Done* | *Installation destination* | *Done* | *Begin Installation*

Created Apache Server on DMZ Alma Servers

To allow for HTTP traffic to be accessed on both DMZ machines, an Apache web server was created. This service was accessed by going to a web browser and searching for the IP of the machine it is hosted on. Access to this service showed that port 80 traffic was enabled within the firewall.

1. Migrated to *CNIT455.G28.VyOSDMZ*
2. Opened a terminal

3. Typed `sudo dnf update | sudo dnf install httpd -y|sudo systemctl start httpd|sudo firewall-cmd –permanent –add-service=http|sudo firewall-cmd –reload`
4. Typed `sudo nano /var/www/html/index.html`
5. Entered "`This is the VyOS DMZ webpage!`"
6. Repeated Steps 1-4 for the pfSense DMZ
7. Entered "`Welcome to our fake company that I have not come up with a fun name for yet!`"

Enabled FTP on DMZ Alma Servers

FTP, or File Transfer Protocol, was enabled in order to allow for machines to access files not available locally. This service was enabled on both DMZ machines to allow for file transfers between machines on different networks.

1. Migrated to *CNIT455.G28.VyOSDMZ*
2. Entered `sudo dnf update | sudo dnf install vsftpd|sudo systemctl enable vsftpd|sudo systemctl start vsftpd`
3. Typed `sudo nano /etc/vsftpd/vsftpd.conf`
4. Changed anonymous_enable to `YES`
5. Set local_enable to `YES`
6. Set write_enable to `YES`
7. Changed local_umask to `022`
8. Repeated Steps 2-7 on pfSense DMZ machine

Installed TFTP Service on VyOS DMZ Machine

TFTP, or Trivial File Transfer Protocol, was enabled on the VyOS DMZ machine to allow machines located on the pfSense or laboratory network to access the service located within the VyOS network. Unlike FTP, TFTP is connectionless and less secure than FTP.

1. Migrated to *CNIT455.G28.VyOSDMZ*
2. Opened a terminal
3. Entered `sudo dnf install tftp-server tftp -y`
4. Typed `sudo mkdir -p /var/lib/tftpboot`
5. Typed `sudo chmod 777 /var/lib/tftpboot`
6. Entered `sudo nano /atv/systemd/system/tftp.socket`
7. Entered `ListenDatagram=69|WantedBy=sockets.target`
8. Saved the file
9. Entered `sudo systemctl enable –now tftp.socket`

RESULTS

The team at Computer Industries has successfully deployed a fully realized and secure network infrastructure that meets the needs of the company. The new network includes a multitude of security measures along with a scalable architecture that promotes future expansions. With this infrastructure, secure and efficient communication will be possible while maintaining high availability and centralized management.

Since the previous architecture was falling behind on efficiency due to company expansion, a new architecture was implemented. To address this, the new architecture transitions to a hybrid solution utilizing both UNIX and Windows systems. Computer Industries takes advantage of VMware vCenter to virtualize much of the environment to reduce costs but increase flexibility. This aligns with the goals and values of the company where expansion is always at the forefront.

At the heart of the new architecture is the pfSense firewall, which directs traffic between multiple zones, including the DMZ, the internal network, and the Internet. The firewall offers granular control over network traffic, ensuring that only necessary communications are allowed into the network. It is configured with PAT and DNAT to manage traffic from the public network to the private domain where the Microsoft Server 2019 domain controller is located.

Alongside the pfSense firewall, a VyOS firewall has been deployed to further isolate the DMZ from the public network, ensuring the security of the internal network. This ensures that services such as HTTP, FTP, and TFTP in the DMZ are protected from external threats while remaining accessible to authorized users.

Computer Industries uses Windows Server 2019 and Windows Server 2022 both acting as domain controllers. These domain controllers streamline user management through Active

Directory Domain Services (ADDS), which centralizes authentication and improves network stability. This setup also makes it easy to add on new services or users as the company continues to expand.

Figure 2 below illustrates how connected the various components in the network are, showing the pfSense firewall managing traffic between zones, the VyOS firewall isolating the DMZ, and the deployment of Windows Server 2019 and 2022 for authentication and directory services. The entire architecture is designed to be scalable and secure, allowing Computer Industries to continue the main goal of expanding as much as possible.

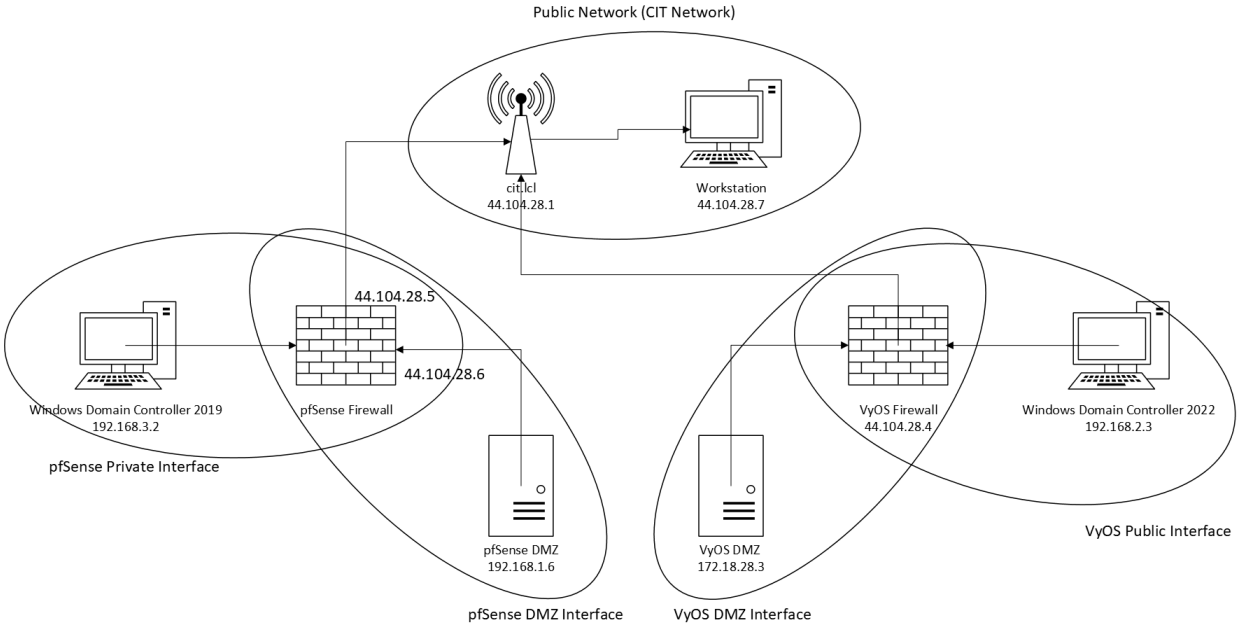

Figure 2: Logical Diagram

In addition to the new security measures, the network includes firewall rules that help prevent unauthorized users and traffic from engaging with the network. These rules ensure that only the traffic that is authorized flows through the different segments of the network. Having rules allows for the company to boost performance while also creating a more secure network. The final network infrastructure is tied directly to Computer Industries' belief in expansion. The

deployment of new firewalls, DNS services, and centralized authentication significantly enhances both security and operational efficiency, perfectly aligning with Computer Industries growth objectives and commitment to a secure, scalable infrastructure.

CONCLUSIONS AND RECOMMENDATIONS

All business requirements were completed in order to complete the project to the fullest extent. As shown in the business case, the goal of the project was to create a network administration system that supported Computer Industries growth by securing the network with much needed updates. The previous Computer Industries architecture required key updates in order to make this infrastructure more secure.

First, the team at Computer Industries installed new UNIX and Windows based systems onto the network. These new machines were installed with the idea of creating two separate firewall architectures. Both firewalls were implemented into the architecture by using PAT as well as NAT which was one of the Computer Industries requirements for the new architecture. By implementing these two protocols, network traffic is able to flow between the public networks as well as the private networks inside of the Computer Industries domain. The previously configured Windows Server 2019 and 2022 machines were moved into a private network in order to have more secure communication with these systems facing the public network. Both of these firewalls were configured to only allow the necessary protocols into the network, being HTTP, FTP, and TFTP. These protocols were defined by the business requirements.

To summarize, the newly developed enterprise network administration system created for the Computer Industries organization serves to address all of the organization's security requirements. The end result of this process is a secure enterprise network administration system that supports the business needs of Computer Industries while also protecting against the possibility of external threat actors that could be or will be trying to attack the network.

Recommendations

To improve upon the firewall configuration and processes taken to complete the objectives associated with this new infrastructure, the team has put together a few recommendations to improve future configurations and eliminate common issues.

Recommendation 1: Configure pfSense and VyOS firewall rules as the last step

Computer Industries gave the team objectives which could have been completed in any order. The team created necessary, and some unnecessary, pfSense and VyOS firewall rules after installing the virtual machines. This was done to establish connections that were appropriate and to stay inbound with the predetermined network infrastructure. However, the firewall rules were incorrect which made initial network connection difficult.

Recommendation 2: Assess the company's objectives before getting ahead of ourselves

Initially, the team at Computer Industries jumped into the project to start taking down the smaller tasks first. The objectives were assessed periodically instead of conducting an upfront comprehensive assessment. The periodic approach required the time for the team to understand the security objectives before moving on with the next step. In the future, the team needs to get a grasp of the overall goals instead of the smaller, individual ones for the next project.

Recommendation 3: Verify connectivity before going ahead to the next step

In order for the network to be functional according to the Computer industries standards, the network must flow where the network is needed to flow. The team should have prioritized network connectivity at all stations before implementing any protocols or features on the

installed virtual machines. Moving forward, ensuring connectivity on the newly installed machines needs to happen first before

BIBLIOGRAPHY

How to install apache on linux (AlmaLinux). Liquid Web. (2024, July 11). https://www.liquidweb.com/help-docs/how-to-install-apache-on-linux-almalinux/

Khan, I. (2022, September 22). *How to install the PfSense firewall on a virtual machine*. 4Sysops.https://4sysops.com/archives/how-to-install-the-pfsense-firewall-on-a-virtual-machine/

Lab Information, C. I. T.-N. E. T. (n.d). Lab Report Template. Brightspace

Outbound NAT | pfSense Documentation. https://docs.netgate.com/pfsense/en/latest/nat/outbound.html.

pfSense Documentation | pfSense Documentation. https://docs.netgate.com/pfsense/en/latest/.

Quick start. Quick Start - VyOS 1.5.x (circinus) documentation. (n.d.). https://docs.vyos.io/en/latest/quick-start.html

Ramirez, M. (2024, August 22). *How to create an FTP server and account in AlmaLinux.* Liquid Web. https://www.liquidweb.com/blog/create-ftp-account-almalinux/

Rawles, P (n.d.). *CNIT 45500 Lab 1 Firewall Configuration and Management*

Rawles, P (n.d.). *IP Configuration Information*

VyOS User Guide — VyOS 1.4.x (Sagitta) Documentation. https://docs.vyos.io/en/sagitta/.

Windows Server 2019 | Microsoft Evaluation Center. (n.d.). Retrieved September 14, 2024, from https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

Windows Server 2022 | Microsoft Evaluation Center. (n.d.). Retrieved September 14, 2024, from https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022

Zone based firewall. Zone Based Firewall - VyOS 1.5.x (circinus) documentation. (n.d.). https://docs.vyos.io/en/latest/configuration/firewall/zone.html

APPENDIX A: PROBLEM SOLVING

Problem 1: Could not access the pfSense web configurator

Problem Description: Once the pfSense was installed and configured on a virtual machine, the interfaces were added and the next step was to configure pfSense using the web configurator. However, the web configurator was not accessible. On multiple client machines, pfSense would not grant access even though the credentials were correct. Even the pfSense was granting a "successful login" message but the computer would not be directed to the config.

Possible Solutions: One potential solution to fix the problem at hand is to adjust the firewall rules. The rules might be blocking access to the web configurator in particular. A second solution is a potential misconfiguration in the web config settings, which might prevent logins. The final solution was that there may be an issue with the virtual machines setup, such as misconfigured network adapters. Misconfigured network adapters would prevent proper communication between the client machines.

Attempted Solutions: The first solution, as well as the second solution, were both attempted in tandem. To attempt these solutions, the pfSense virtual machine was reinstalled into the Computer Industries infrastructure and configured carefully. The first and second solution did not solve the problem because the problem persisted across all clients. Next, troubleshooting efforts focused on verifying the client virtual machines, as well as the pfSense machine, had the correct network adapters in settings.

Final Solution: The final solution involved rebooting both the client machines, and the pfSense machine after reinstalling a new version. After both reboots, the web configurator finally became accessible. The reboot must have solved a temporary networking issue or cleared a cache which caused the problem.

Problem 2: VyOS Machines unable to access internet and pfSense machines

Problem Description: After initial creation and configuration of the VyOS machines, IP addresses were assigned to the domain controller and the Alma Linux server and virtual interfaces were created on the VyOS router. However, each machine did not have internet access and was unable to reach other machines within the network. Each machine, even the VyOS router, was unable to ping a 1.1.1.1 address as well as any of the other machines on that side of the network.

Possible Solutions: One potential solution would be to check the firewall status on each of the machines besides the router. Local firewall policies may have prevented the outflow of traffic from the local machine and blocked connection to other machines. Another potential solution would be to check the network adapters installed on each of the machines. If the IP address does not match the corresponding network adapter, the machine will not be able to send traffic out. Another potential solution would be to check the gateways of each machine. Interfaces and their gateways were set on the VyOS router and if they were not configured correctly on the endpoint machines they would not receive connectivity.

Final Solution: The final solution involved the configuration of a static route within the VyOS router. A static route needs to be configured to enable a specific path for information to travel within a network. Once a static route was configured, each machine was able to gain internet connectivity as well as connect with public facing machines such as the pfSense firewall and the network located behind it.

Problem 3: pfSense DMZ virtual machine connectivity issues

Problem Description: After resolving the issues with the VyOS machines, a new problem arose with the DMZ machine on the pfSense side. The pfSense DMZ was no longer able to ping or communicate with any devices outside the network, including the pfSense machine. The DMZ was unable to ping machines within the Computer Industries infrastructure or the network gateways.

Possible Solutions: One solution was to check the firewall rules in pfSense to ensure traffic from the DMZ was not being accidentally blocked. pfSense could have been configured in a way that rules were restricting the DMZ from sending or receiving traffic outside of the local subnet. Another possibility was a simple routing issue. Incorrect routes in pfSense could prevent the DMZ from reaching other networks. Lastly, the network interfaces could be misconfigured. The DMZ interface could have been assigned the wrong IP address.

Attempted Solutions: The first approach to problem three was to review and adjust the firewall rules for the DMZ interface. Rules were checked to ensure that relevant traffic types were allowed from and to the DMZ. New rules were created to specifically permit traffic but the problem still persisted. The pfSense routing tables were examined but everything in the routing table checked out. Lastly, the configuration of the DMZ interface was inspected.The Computer Industries requirements were referenced and the configuration of the DMZ was confirmed. The problem still persisted.

Final Solution: The final solution involved resetting the network interfaces, as well as restarting the routing services on pfSense. The DMZ regained the ability to communicate with the gateway as well as the external networks. A configuration change made during initial troubleshooting

may have not fully applied until the services were restarted. Restarting the services resolved the issue.

APPENDIX B: VIRTUAL MACHINE NETWORK SETTINGS CONFIGURATION

Appendix B gives the IP Address, Subnet mask, Default Gateway, Preferred DNS, Alternate DNS settings, and Domain Controller assignments for each VM computer. Appendix B also gives the IP address and Subnet mask of the interfaces attached to pfSense.

Table 1: Virtual Machine Networking Configuration Settings

PC/Interface	IP address	Subnet Mask	Gateway	Pref. DNS	Alt. DNS
pfDMZ	192.168.1.6	255.255.255.0	192.168.1.1	44.2.1.44	44.2.1.45
pfSense	44.104.28.5	255.255.255.0	192.168.1.1	192.168.1.5	192.168.2.2
privA	192.168.3.2	255.255.255.0	192.168.3.1	127.0.0.1	
privB	192.168.2.3	255.255.255.0	192.168.3.1	44.2.1.44	44.2.1.45
VyOS	44.104.28.4	255.255.255.0	192.168.3.1	44.2.1.44	44.2.1.45
VYosDMZ	172.18.28.3	255.255.255.0	172.18.28.1	44.2.1.44	44.2.1.45
WINDOWSPublic	44.104.28.7	255.255.255.0	192.168.3.1	44.2.1.44	44.2.1.45

APPENDIX C: PFSENSE FIREWALL RULE CONFIGURATION

Table 1: WAN Interface Rules

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	IPv4 ICMP	*	*	*	*	*
Pass	IPv4 TCP/UDP	*	*	44.104.28.6	80	*
Pass	IPv4 TCP/UDP	*	*	44.104.28.6	20-21	*
Pass	IPv4 TCP/UDP	*	*	WAN address	80	*
Pass	IPv4 TCP/UDP	*	*	192.168.1.6	80	*
Pass	IPv4 TCP/UDP	*	*	192.168.1.6	20-21	*
Block	IPv4 *	*	*	*	*	*

Table 2: LAN Interface Rules

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	IPv4 *	*	*	LAN	*	*
Pass	IPv4 TCP	*	*	*	*	*
Pass	IPv4 *	*	*	*	*	*
Pass	IPv4 *	PRIVATE	*	*	*	*
Pass	IPv6 *	PRIVATE	*	*	*	*
Block	IPv4 *	*	*	*	*	*

Table 3: OPT1 Interface Rules

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	*	*	*	OPT Address		*
Pass	IPv4 TCP	OPT1	*	LAN	*	*
Pass	IPv4 *	OPT1	*	*	*	*
Pass	IPv4 TCP/UDP	*	*	OPT1	21000-21999	*
Pass	IPv4 TCP/UDP	OPT1	*	*	53	*
Pass	IPv4 TCP/UDP	OPT1	*	*	80	*
Pass	IPv4 TCP/UDP	OPT1	*	*	443	*
Pass	IPv4 TCP/UDP	OPT1	*	*	20-21	*
Pass	IPv4 TCP/UDP	OPT1	*	*	*	*
Pass	IPv4 TCP/UDP	OPT1	*	*	123	*
Pass	IPv4 TCP/UDP	OPT1	*	*	25	*
Block	IPv4 *	*	*	*	*	*

Table 4: NAT Outbound Rules

Interface	Source	Port	Destination	Port	NAT Address	Port
WAN	192.168.1.6/32	*	*	*	44.104.28.6/32	*
WAN	192.168.3.0/24	*	WAN	*	WAN	*
WAN	192.168.3.0/24	*	*	*	44.104.28.6	*
WAN	192.168.1.0/24	*	WAN	*	WAN	*
WAN	192.168.1.0/24	*	*	*	44.104.28.6	*

APPENDIX D: VyOS Router/Firewall Configuration

```
group28@Router1# show
 firewall {
    global-options {
        all-ping enable
    }
    ipv4 {
        forward {
            filter {
                rule 5 {
                    action jump
                    inbound-interface {
                        name eth0
                    }
                    jump-target wan2lan
                }
            }
        }
        name wan2lan {
            default-action drop
            rule 2 {
```

```
        action accept
        description "Allow established/related"
        state established
        state related
    }
    rule 10 {
        action accept
        destination {
            address 172.18.28.3
            port 80
        }
        protocol tcp
        source {
            address 44.104.28.0/24
        }
    }
    rule 20 {
        action accept
        destination {
            address 172.18.28.3
            port 69
        }
        protocol tcp
```

```
        source {
            address 44.104.28.0/24
        }
    }
    rule 30 {
        action accept
        destination {
            address 172.18.28.3
            port 20
        }
        protocol tcp
        source {
            address 44.104.28.0/24
        }
    }
    rule 40 {
        action accept
        destination {
            address 172.18.28.3
            port 21
        }
        protocol tcp
        source {
```

```
                address 44.104.28.0/24
            }
        }
    }
}
interfaces {
    ethernet eth0 {
        address 44.104.28.4/24
        description External
        hw-id 00:50:56:91:41:7f
    }
    ethernet eth1 {
        address 172.18.28.1/24
        description DMZ
        hw-id 00:50:56:91:2e:64
    }
    ethernet eth2 {
        address 192.168.2.1/24
        description "Private B"
        hw-id 00:50:56:91:81:62
    }
    loopback lo {
```

```
    }
}
nat {
    destination {
        rule 20 {
            description "DNAT for Priv"
            destination {
                address 44.104.28.4
                port 80
            }
            inbound-interface {
                name eth0
            }
            protocol tcp
            translation {
                address 192.168.2.3
                port 80
            }
        }
    }
    source {
        rule 10 {
            outbound-interface {
```

```
            name eth0
        }
        source {
            address 172.18.28.0/24
        }
        translation {
            address masquerade
        }
    }
    rule 20 {
        outbound-interface {
            name eth0
        }
        source {
            address 192.168.2.3
        }
        translation {
            address masquerade
        }
    }
  }
}
protocols {
```

```
    static {
        route 0.0.0.0/0 {
            next-hop 44.104.28.1 {
            }
        }
    }
}
 service {
    ntp {
        allow-client {
            address 0.0.0.0/0
            address ::/0
        }
        server time1.vyos.net {
        }
        server time2.vyos.net {
        }
        server time3.vyos.net {
        }
    }
    ssh {
        listen-address 44.104.28.4
        port 22
```

```
    }
}
system {
    config-management {
        commit-revisions 100
    }
    conntrack {
        modules {
            ftp
            h323
            nfs
            pptp
            sip
            sqlnet
            tftp
        }
    }
    console {
        device ttyS0 {
            speed 115200
        }
    }
    host-name Router1
```

```
    login {
        user group28 {
            authentication {
                encrypted-password
$6$rounds=656000$K03Cy4G03Ucf9iM8$jQ/EYjPCrGJaPFirFAlp6rdBOhb962ojShJve.x/yknL
MpWmwFBuVf0YDnPqyu49mBTH9DqF4ulS.hR0CkY2m/
            }
        }
        user vyos {
            authentication {
                encrypted-password
$6$QxPS.uk6mfo$9QBSo8u1FkH16gMyAVhus6fU3LOzvLR9Z9.82m3tiHFAxTtIkhaZSWssSg
zt4v4dGAL8rhVQxTg0oAG9/q11h/
                plaintext-password ""
            }
        }
    }
    name-server 44.2.1.44
    syslog {
        global {
            facility all {
                level info
            }
```

```
            facility local7 {
                level debug
            }
        }
    }
}
[edit]
group28@Router1#
```