CNIT 45500: Network Security

CNIT45500-010

Group 32

Ethan Hammond

Tyler Hiatt

Submitted To: Tony Wan

Date Submitted: 12/12/23

Date Due: 12/12/23

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ET Corp wants to enhance the security of the company by utilizing enterprise certificates for all VPNs and connections, central authentication to a RADIUS server through the use of active directory, and a captive portal on PfSense. The use of enterprise certificates allows ET Corp to know that they are certifying the VPN connections and the connections to the captive portal. It is critical to have a captive portal to login to the firewalls, as this can force the use of RADIUS authentication, and prevents unauthorized access to the engineering of the infrastructure. In addition to a captive portal, the central authentication for all machines greatly enhances the security posture of ET Corp, as all devices need to be logged in via a RADIUS authentication server located on the domain controller. This prevents unauthorized users from logging in to accounts without having an AD account created first. Overall, the implementation of these tools has greatly increased the security of ET Corp.

BUSINESS CASE

ET Corp is a medium sized organization with a need for an environment containing certificates, centralized authentication, and a captive portal for guest and remote users. Due to these needs, it is imperative to incorporate AD credentials to log into network firewalls. Centralized authentication can be completed by configuring firewalls to source users from an LDAP Windows server. Clients and servers can be configured to authenticate off of a RADIUS server or using PAM and Kerberos hashes. Certificate services can be set up to automatically serve out certificates to all clients and servers through ADCS windows servers. Group policy can be utilized to push these out to domain users. However, for UNIX hosts, certificates must be places manually. Lastly, a captive portal can be used effectively for organizations to allow guests or remote users onto a network. Captive portals can be configured via the firewall application to allow guests to authenticate via guest credentials or via an authentication LDAP or RADIUS server.

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*.

RADIUS configuration on Windows Servers

Windows Servers needed to have RADIUS authentication servers configured on them for centralized authentication across the network.

1. Logged into the Windows server A.
2. Opened server manager and installed Network Policy Services.
3. Opened Network Policy Server and right-clicked NPS (Local) and registered the server.
4. Added a Remote RADIUS Server group and added Windows Server A and Windows Server B to the group.
5. Added a RADIUS Client via IP for all client machines in the domain.
6. Entered the shared secret configured later on pfSense.
7. Repeated steps 1-5 on the Windows B server.

AD Authentication on firewalls

After Windows RADIUS servers were set up, it was necessary to configure the firewalls to receive RADIUS users for authentication.

1. Opened pfSense via a web browser and opened System | User Manager | Authentication Servers.

2. Added a server of type LDAP with the IP of Windows Server A and saved.
3. Opened System | User Manager | Settings.
4. Changed the Authentication Server to the one created in step 2.
5. Logged out of pfSense and logged in with an AD user created on Windows Server A.
6. Logged into the VyOS machine and used set system login radius server 192.168.2.10 {
    a. Key ############# (password)
    b. Port 1812
    c. Timeout 5 }
7. Logged out of the VyOS machine and logged in as an AD user from the Windows server 192.168.2.10.
8. Used conf | show system login to view configurations.

UNIX Machine Centralized Authentication

UNIX machines were configured to source users for login from a Windows LDAP server with PAM and Kerberos hashes.

1. Logged into the AlmalinuxA machine and opened a terminal window.
2. Typed sudo dnf install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation authselect-compat
3. Entered realm discover CNIT455.group32.winA to discover the domain.
4. Used realm join CNIT455.group32.winA -U Administrator to join the domain.
5. Entered sudo authselect select sssd && sudo authselect select sssd with-mkhomedir.
6. Restarted sssd with sudo systemctl restart sssd.

7. Used id guestUser to check if the machine can pull an AD user from the Windows LDAP server.
8. Used su guestUser to switch into the AD user on the Alma machine.
9. Repeated steps 1-8 on the AlmaB machine.

pfSense Captive Portal Configuration

For untrusted or remote users, a captive portal was set up via pfSense to allow users to access the network via their AD credentials.

1. Opened studentvc and opened the vSwitch tab.
2. Added a new port group named Portal and added a NIC of type ‘portal’ on a Windows Guest machine.
3. Added a NIC of type ‘portal’ on the pfSense machine.
4. Opened pfSense web configurator and navigated to Services | Captive Portal.
5. Checked “Enable Captive Portal” and chose the OPT2 interface.
6. Chose ‘Use an authentication backend’ under the authentication tab.
7. Chose the LDAP Windows A server as the authentication server.
8. Navigated to Services | Captive Portal | Guest_Portal | Allowed IP Addresses.
9. Added 44.2.1.44 and 44.2.1.45 CIT DNS Servers as the allowed IP addresses.
10. Logged into the Windows guest machine and opened a web browser.
11. Clicked “Open network portal” when prompted and logged in with AD credentials.

Enterprise Certificate Configuration

The use of Enterprise Certificates greatly increases the security of ET Corp, and the steps for configuring the certificates can be located below.

1. Navigated to Windows Server A.
2. Navigated to mmc.exe and created a new certificate.
3. Exported the certificate and the private key.
4. Downloaded Win64 OpenSSL v3.2.0 and navigated to the terminal.
5. Entered `openssl pkcs12 -in ThisShouldWork.pfx -clcerts -nokeys -out certificate.pem` to export certificate in a format that would work for pfSense.
6. Typed `openssl pkcs12 -in ThisShouldWord.pfx -nocerts -nodes -out private.key` to export the key in a format that pfSense would understand.
7. Navigated to pfSense and imported a certificate authority | entered the certificate and private key data into the boxes.
8. Created a certificate signing request in pfSense and added the IP addresses of all interface gateways.
9. Exported the newly created singing request and pasted the data into the “signed” box.
10. Saved the certificates and edited the OpenVPN configurations to use the newly created Certificate Authority and Signing Request.
11. Navigated to Client Export to utilize the new OpenVPN configurations for the AD users.
12. Saved the configurations and tested the OpenVPN connections.

RESULTS

The ending architecture included working enterprise certificates that were generated by the domain controller, a captive portal for users, and RADIUS authentication for all machines and devices. This created a secure environment, and even secured the VPNs by using the enterprise certificates created by the Windows Server domain controller. The site-to-site VPN was not functional; however the certificates would work identically as the client access VPN. PfSense would need to have a certificate signing request sent out, and the enterprise certificate would need to be handled via Windows64 SSL version 3. Upon utilizing Windows64 SSL version 3, the enterprise certificate would need to be imported into PfSense, and then added to the VPNs. This would allow the VPNs to connect seamlessly while utilizing the new enterprise certificate. In addition to enterprise certificates, a captive login portal needed to be created for users as well. This splash page and captive portal will be useful for other employees and users to log in to the proper resources. In addition to the captive portal, central authentication needed to be added to all devices and machines through the use of RADIUS. This RADIUS authentication server would be hosted on the Windows Server domain controller as well. This would allow all users to authenticate to their respective machines, VPNs, and accounts through active directory, ensuring the security of the accounts. This is all very critical for a secure architecture. Upon completion of the central authentication, the architecture was considered complete.

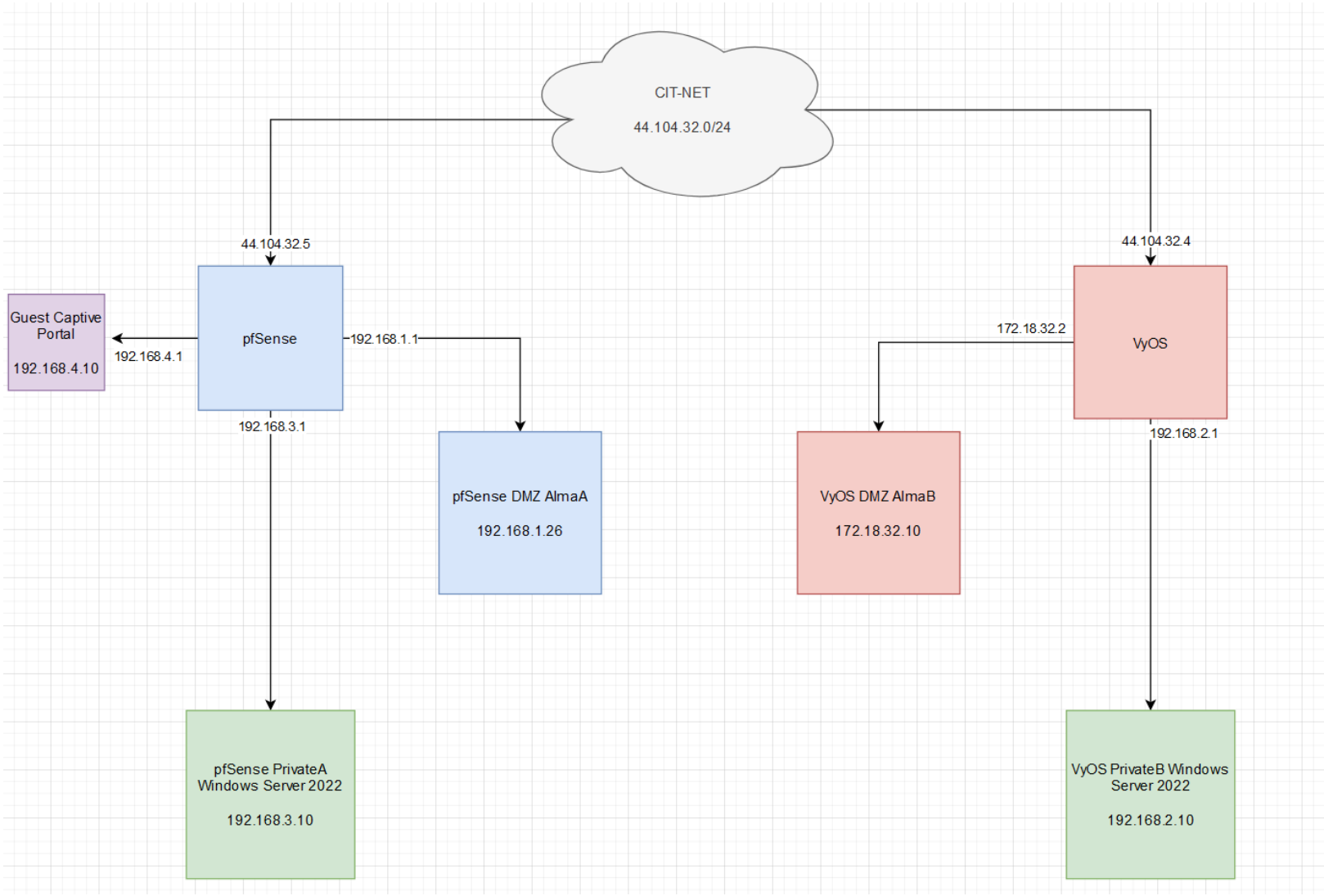

Figure 1.1: Screenshot of the Logical Diagram

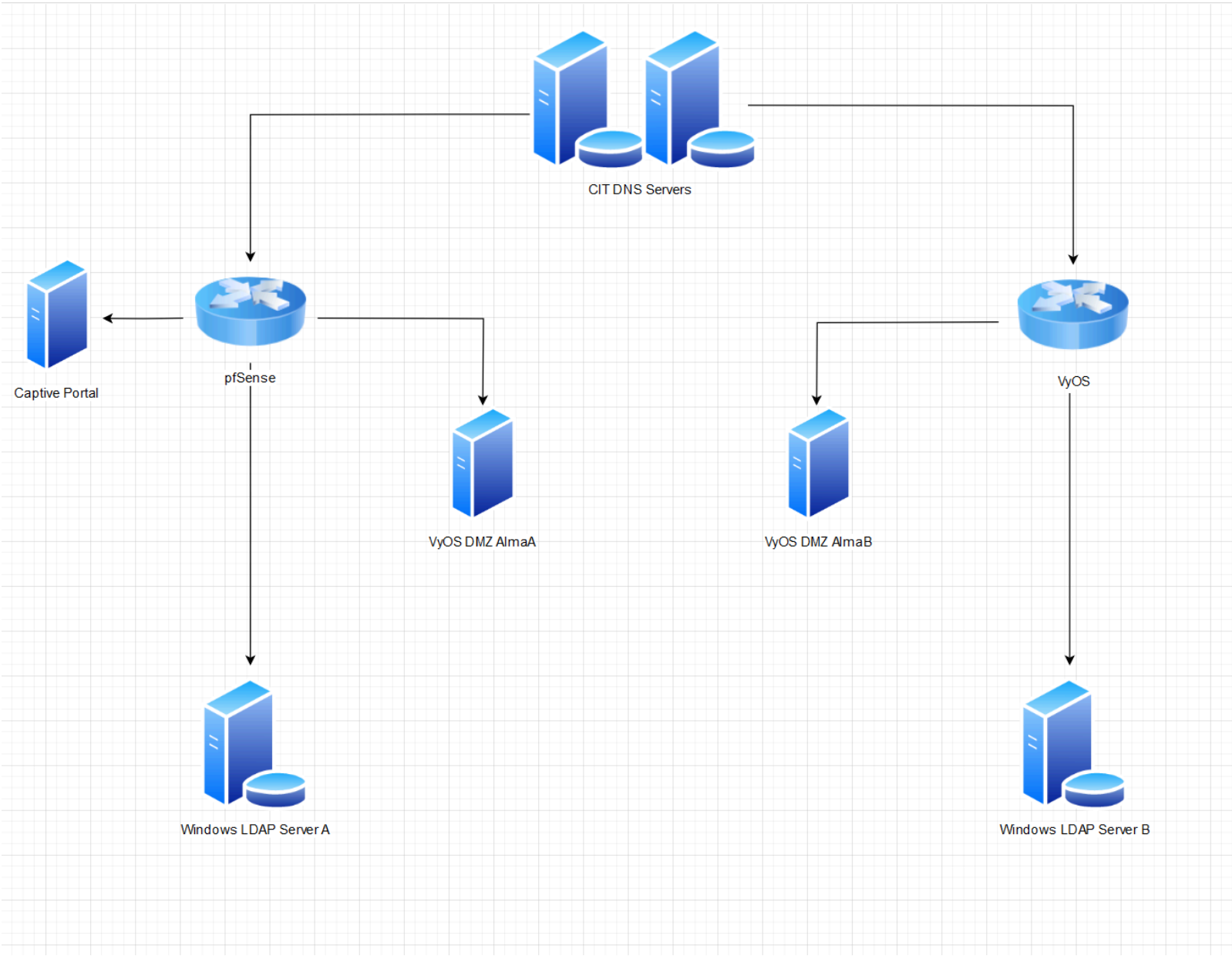

Figure 1.2: Screenshot of the Physical Diagram

CONCLUSIONS AND RECOMMENDATIONS

Upon completion of this architecture, it would be wise to logically understand certificates better. Certificates are difficult to implement when a solid conceptual understanding is not present. However, it is also important to understand the use of client export in PfSense. This client export was needed in order for the authentication of users via the client access OpenVPN configuration. Once these two aspects were fully understood, the implementation was straightforward and fairly simple. When setting up the captive portal, it is recommended to add your DNS servers in the allowed IP address fields so that the servers can forward connection requests onward to the other private DNS servers in the network. It is also recommended to create separate security groups for each segment of users that will be using the captive portal. This way different group policy can be applied to different groups of AD users that would be logging into the network via the captive portal. This can be effective in business environments to implement role-based access control in the network depending on the position and need for access in the network.

REFERENCES

Burke, K. (2021, May 25). *PfSense - OpenVPN site-to-site setup*. Mayfield IT Consulting. https://mitky.com/pfsense-openvpn-site-to-site-vpn/

Captive portal zones¶. Captive Portal - Captive Portal Zones | pfSense Documentation. (n.d.). https://docs.netgate.com/pfsense/en/latest/captiveportal/zones.html

KL, A. (2023, November 16). *Step -by-step procedure to set up an enterprise root ca on windows server*. The Sec Master. https://thesecmaster.com/step-by-step-procedure-to-set-up-an-enterprise-root-ca-on-windows-server/

Mutai-, B., By, Josphat Mutaihttps://computingforgeeks.com/Founder of Computingforgeeks. Expertise in Virtualization, Mutai, J., Founder of Computingforgeeks. Expertise in Virtualization, LinkedinTwitter, & here, P. enter your name. (2023, August 16). *Join centos 8 / RHEL 8 system to Active Directory (AD) domain*. ComputingForGeeks. https://computingforgeeks.com/join-centos-rhel-system-to-active-directory-domain/

Setup LDAPS on windows server. Drupal.org. (2023, December 8). https://www.drupal.org/docs/contributed-modules/ldap-integration/setup-ldaps-on-windows-server

Tankmek. (2018, October 18). *Using openssl and pfSense to sign a subordinate Windows Enterprise Certificate Authority*. Michael Edie.

https://blog.edie.io/2018/10/18/using-openssl-and-pfsense-to-sign-a-subordinate-windows-enterprise-certificate-authority/

User management. User Management - VyOS 1.3.x (equuleus) documentation. (n.d.). https://docs.vyos.io/en/equuleus/configuration/system/login.html

Vivek. (2022, December 2). *Configure radius on windows server 2019*. SecureW2. https://www.securew2.com/blog/configure-windows-server-2019

Vorkbaard, K. (2023, June 22). *Vorkbaard Uit de Toekomst*. Kapitein Vorkbaard to the rescue! https://vorkbaard.nl/set-up-openvpn-on-pfsense-with-user-certificates-and-active-directory-authentication/

APPENDIX A: PROBLEM SOLVING

Problem 1

Problem Description: The captive portal would pop up on the client machine, but could not authenticate AD users.

Solutions Attempted: It was attempted to reconfigure LDAP on Windows servers and relink the systems. It was attempted to reconfigure the captive portal to use different authentication methods. Neither of these solutions fixed the issue.

Final Solution: The problem was solved by fixing two issues: Entering the correct BIND credentials on the authentication server, and adding the CIT DNS servers as "Allowed IP Addresses" in the captive portal menu on pfSense.

Problem 2

Problem Description: The AlmaB machine successfully sources AD users from Windows Server B and can log in via AD, but AlmaA cannot with the same configuration.

Solutions Attempted: It was attempted to reconfigure the AlmaA the same way as AlmaB. It was attempted to rejoin the Windows A domain, which did not work as well. It was also attempted to recreate the Kerberos keys, which did not work.

Final Solution: The problem was solved by recreating the AlmaA VM and configuring it exactly how AlmaB was created without any misconfigurations.