CNIT 45500: Network Security

CNIT45500-010

Group 32

Ethn Hammond

Tyler Hiatt

Submitted To: Tony Wan

Date Submitted: 10/19/23

Date Due: 10/20/23

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In a medium sized business enterprise environment, VPNs can be incredibly important to the functionality of a company’s network. For client convenience and network efficiency, 5 VPNs were configured and established into the network environment. An IPsec Site-to-Site VPN was established between the two client zones. An L2TP Client access VPN was set up from the private B to the public internet. An IPsec client access VPN was set up from private A to the public internet. An OpenVPN client access VPN was set up between the DMZ A and the public internet. Lastly, an OpenVPN Site-to-Site VPN was set up between the two DMZs. These VPNs allow employees to work remotely as well as multiple job sites to be interconnected on the same network through VPNs. ET Corp VPNs have been mostly set up, the troubleshooting of which can be seen below in Appendix A. The report will contain a business case, procedures for setting up the lab, and conclusions/recommendations of the final lab.

BUSINESS CASE

Upon implementing multiple different segments of networks, ET Corp has now decided to implement multiple VPN connections for remote workers to securely connect to proper resources. It is imperative that certain VPNs can only contact certain services, as this will ensure security throughout the network. In addition to the VPNs, different authentication methods need to be set up as well in order for users to be authenticated. The five different VPNs that need to be established are: IPsec Client-Access VPN from the public internet to DMZ A, IPsec Site-to-Site VPN from Private A to Private B, L2TP over IPsec Client-Access VPN from the public internet to Private B, an OpenVPN SSL Client-Access VPN from the public internet to Private A, and an OpenVPN SSL Site-to-Site VPN from DMZ A to DMZ B. It is crucial to note that the VPN from the public internet to Private A requires Active Directory authentication via LDAP. Another authentication method that is required is RADIUS for the L2TP VPN. The IPsec Site-to-Site VPN requires the use of pre-shared keys, and the traffic needs to be encrypted as well, as this traffic navigates between the two private segments of the network. After all of the VPNs are fully configured, encrypted remote traffic will be able to flow between the various parts of the network.

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*.

IPsec Site-to-Site VPN VyOS Configuration

1. Created the ESP group for the VPN with `set vpn ipsec esp-group site-to-site-esp {`

    a. `Compression disable`

    b. `Lifetime 1800`

    c. `Mode tunnel`

    d. `Pfs enable`

    e. `Proposal 1`

        i. `Encryption aes256`

        ii. `Hash sha1`

2. Implemented the IKE group with `set vpn ipsec ike-group site-to-site-ike {`

    a. `Ikev2-reauth no`

    b. `Key-exchange ikev1`

    c. `Lifetime 3600`

    d. `Proposal 1`

        i. `Dh-group 2`

        ii. `Encryption aes256`

        iii. `Hash sha1`

3. Created the VPN with `set vpn ipsec site-to-site` {

    a. `Peer 44.104.32.4 {`

        i. `Authentication` {

            1. `Mode pre-shared-seceret`

            2. `Pre-shared-secret CNIT455g32`

        ii. `Ike-group site-to-site-ike`

        iii. `Local-address 44.104.32.4`

        iv. `Tunnel 1` {

            1. `Esp-group site-to-site-esp`

            2. `Local prefix 192.168.2.0/24`

            3. `Remote prefix 44.104.32.0/24`

IPsec Site-to-Site pfSense Configuration

1. Logged into the pfSense web browser and selected VPN | IPsec
2. Selected “Add P1”.
3. Chose *IKEv1* Key Exchange version
4. Used the *WAN* interface with a gateway of 44.104.32.4
5. Changed the *Pre-Shared Key* field to CNIT455g32
6. Changed the *encryption algorithm* to AES 256 with SHA1 1024 bit hash.
7. Changed *NAT Traversal* to “Force”.
8. Clicked “Add P2”.

9. Changed *Local network* to “LAN subnet”.
10. Changed *Remote Network* to a network address of 192.168.2.0/24.
11. Modified the *encryption algorithm* field to be AES 256 with SHA1 1024 bit hash.
12. Selected Status | IPsec on the top menu bar and clicked “Connect P1 and P2” to start the VPN connection.

IPsec Client Access VPN pfSense Configuration

1. Logged into the pfSense web browser and selected VPN | IPsec | Mobile Clients.
2. Clicked “Add P1” to add a VPN instance.
3. Set the *key exchange version* to IKEv1.
4. Set the interface to *WAN*.
5. Changed the *Encryption* to AES 256 with SHA256 2048 bit hash.
6. Set *NAT Traversal* to Force.
7. Clicked “save” and then “Add P2”.
8. Changed the *Local Network* to OPT1 subnet.
9. Set the *encryption algorithms* to AES 256 with SHA256 2048 bit hash.

IPsec Client Access VPN Windows Client Configuration

1. Downloaded and installed ShrewSoft VPN Client for Windows.
2. Launched the VPN application.
3. Changed the *hostname* of the connection to 44.104.32.5.
4. Clicked into the “Client” tab and changed *NAT Traversal* to “force-rfc”.
5. Clicked the “Authentication” tab and changed the following on Mutual PSK:
    a. Local Identity Identification Type: IP Address

    b. String: 192.168.2.10

    c. Remote Identity Identification Type: IP Address

    d. String: 44.104.32.5.

    e. Credentials: Pre Shared Key: CNIT455g32

6. Clicked “Phase 1” and changed *encryption* to AES 256 with SHA256 2048 bit hash.

7. Changed the same items as number 6 in phase 2.

8. Clicked *connect* to connect to the VPN.

L2TP over IPsec Client-Access VPN VyOS Configuration

1. Created the ESP group with `set vpn ipsec esp-group client-access-l2tp-esp` {

    a. `Lifetime 1800`

    b. `Proposal 1 encryption aes256`

    c. `Proposal 1 hash sha256`

2. Created the IKE group with `set vpn ipsec ike-group client-access-l2tp` {

    a. `Ikev2-reauth no`

    b. `Lifetime 3600`

    c. `Proposal 1` {

        i. `Dh-group 14`

        ii. `Encryption aes256`

        iii. `Hash sha256`

3. Created the L2TP VPN with `set vpn l2tp remote access` {

a. `Authentication` {

   i. `Mode radius`

   ii. `Radius server 192.168.2.10 key CNIT455g32`

   iii. `Radius source-address 192.168.2.3`

   iv. `Require mschap-v2`

b. `Ccp-disable`

c. `Client-ip-pool start 192.168.2.100`

d. `Client-ip-pool stop 192.168.2.105`

e. `Gateway-address 192.168.2.3`

f. `Ipsec-settings authentication mode pre-shared-secret`

g. `Ipsec-settings pre-shared-secret CNIT455g32`

h. `Name-server 44.2.1.44`

i. `Name-server 44.2.1.45`

j. `Outside-address 44.104.32.4`

L2TP over IPsec Client-Access VPN Windows Client Configuration

1. Opened Control Panel | Network and Internet | Network and Sharing Center and clicked *Set up a new connection or network.*
2. Chose the VPN option and put 44.104.32.4 as the IP address.
3. Navigated back to *Network and Sharing Center* and clicked Change Adapter Settings.
4. Right clicked the VPN connection and selected *properties*.
5. Clicked the “Security” tab and changed *Type of VPN* to L2TP Over IPsec.
6. Clicked “Advanced Settings” and changed the *Pre-Shared-Key* to CNIT455g32
7. Right Clicked the VPN and clicked *connect*.

8. Entered RADIUS credentials to authenticate onto the VPN.

SSL (OpenVPN) Client-Access VPN, Client and PfSense

1. Updated PfSense to the newest version to support Client Export.
2. Downloaded Client Export Add On
3. Created a Client Export with the following configurations
    a. Server UDP4:1194
    b. Host Name: 44.104.32.5
    c. High Encryption
    d. Added VPN user to the certificate name.
4. Downloaded OpenVPN Client on Client PC
5. Imported Client Export into OpenVPN client on client PC.
6. On PfSense navigated to OpenVPN | Servers | Created with the following configurations:
    a. Server mode: `Remote Access (SSL/TLS + User Auth)`
    b. Authentication: `AD` | Interface: `WAN`
    c. Local Port: `1194` | CA: `OpenVPN_CA`
    d. Use the same encryption ciphers
    e. IPv4 tunnel network: `192.168.200.0/24`
    f. IPv4 Local Networks: `192.168.3.0/24`
    g. Save

SSL (OpenVPN) Site-to-Site VPN for PfSense

1. Navigated to PfSense | VPN | OpenVPN | Servers | Add

2. Configured the Server with the following configurations:
    a. Server Mode: Peer to Peer (SSL/TLS) | Interface: WAN
    b. Local Port: 1197 | CA: OpenVPN_CA
    c. Ensure encryption ciphers are equal between hosts.
    d. IPv4 tunnel network: `44.104.32.0/24`
    e. IPv4 Local Networks: `192.168.1.0/24`
    f. Save

RESULTS

The result of lab 2 was a functioning network architecture with all clients that needed to communicate with each other able to. This was achieved through the implementation of two site-to-site VPNs as well as 3 client access VPNs. The site-to-site VPNs were placed between the two private networks to ensure access between private clients in both areas. Secondly, site-to-site VPNs were placed between the DMZs so that services in the zones can communicate with each other. For client convenience, there were client access VPNs put in place for the clients to be able to access services and IP addresses from outside of the network and zones that they are in. Figures 1.1 and 1.2 show the physical and logical diagrams of the lab architecture. Each router has outward facing public addresses and inside facing private addresses for each of their zones they are mediating. DMZs were set in place for services to be held in quarantine before they are able to talk to the private network. If a device is authorized to interact with the private, the communication will be forwarded as such.

Figure 1.1: Screenshot of the Logical Diagram

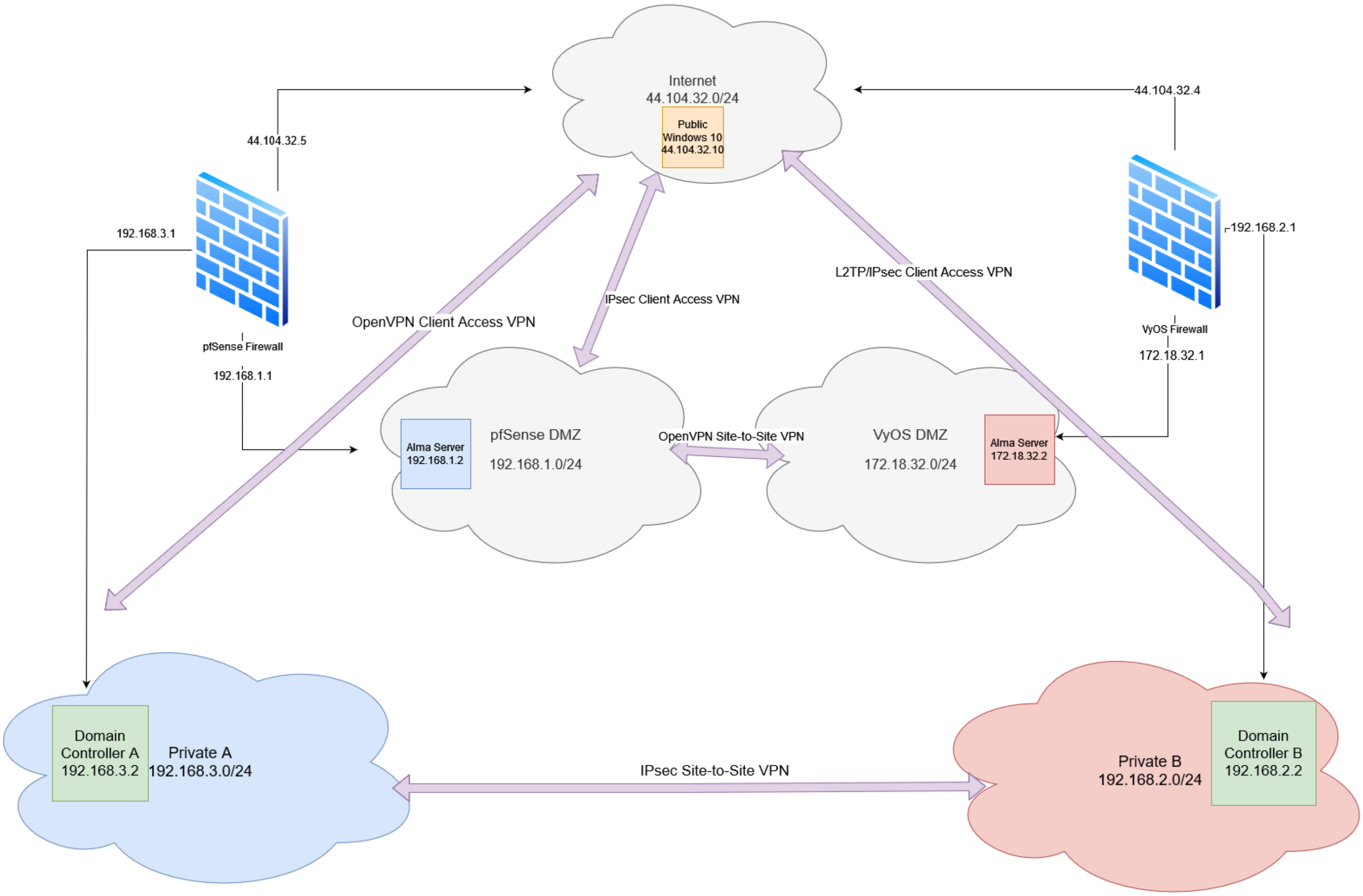
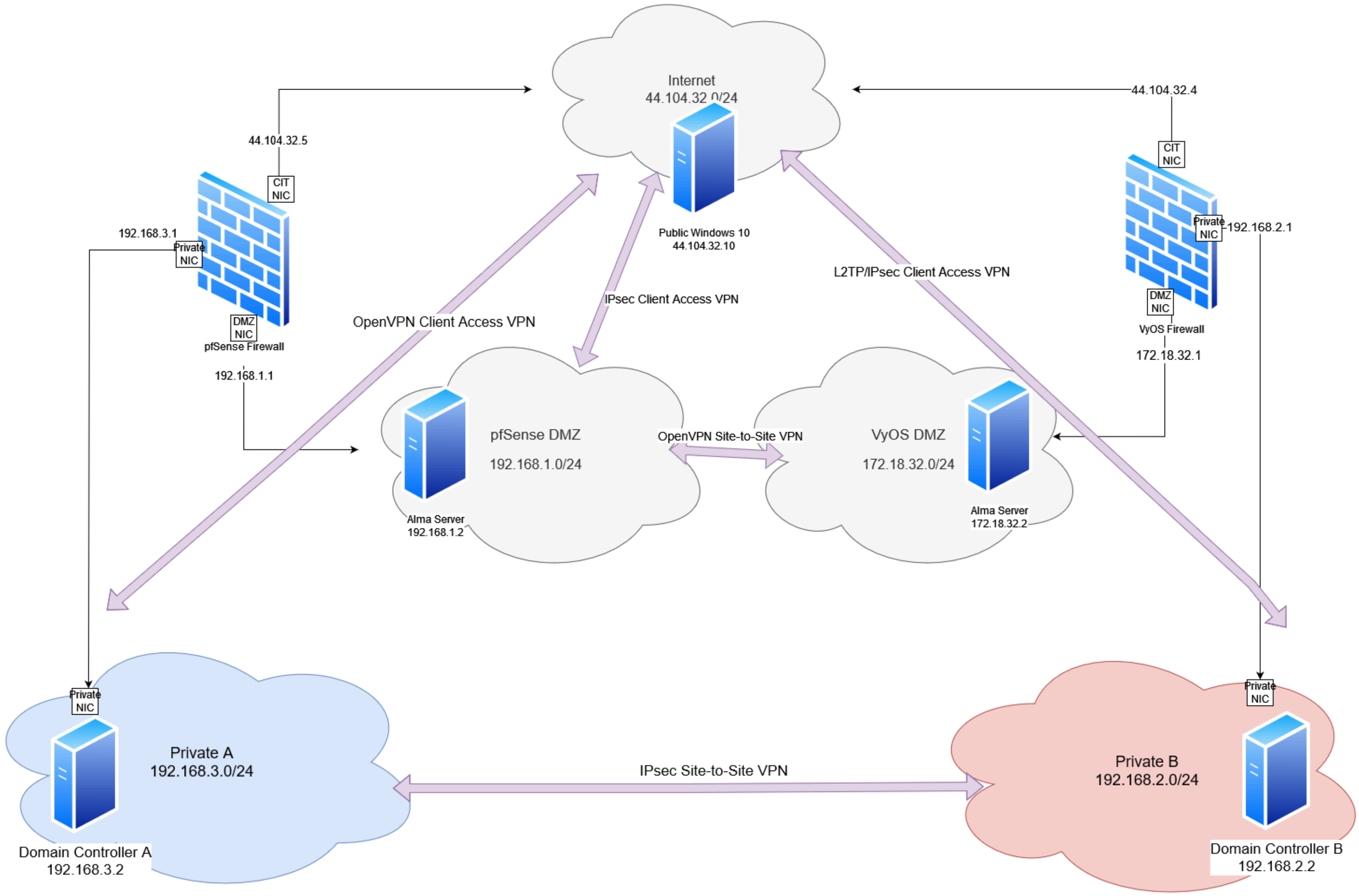


Figure 1.2: Screenshot of the Physical Diagram



CONCLUSIONS AND RECOMMENDATIONS

Within a medium sized company like ET Corp, VPNs are necessary for the business to run effectively. Site-to-site VPNs are a necessity when two different job sites are to be connected on the same network. This type of VPN is used seamlessly unknowingly by the clients, but can interconnect the two sites to be used efficiently between all clients and servers. All VPNs besides the L2TP Client Access and OpenVPN Site-to-Site VPNs were fully working and functional. The OpenVPN Site-to-Site VPN worked before an unfortunate critical system error before checkoff. The L2TP Client Access VPN was not functioning correctly as the clients could not get past the authentication of the VPN, which will take further troubleshooting to fix. The IPsec VPNs were configured via the pfSense web configurator and VyOS CLI, and the OpenVPN VPNs were configured through the OpenVPN client, pfSense, and the VyOS CLI.

Recommendations for future implementation include troubleshooting and completing the remainder of the VPNs. Troubleshooting would include tracerouting for the OpenVPN site-to-site VPN for access to information regarding where the traffic is flowing, and further investigation in the ShrewSoft VPN client for the L2TP network. It is also recommended to switch the L2TP and IPsec VPNs to SSL VPN solutions, as they provide better security as well as better user-friendliness for implementation and client usage. Also, although it is easier to configure a VPN with little security, it is important to enhance security measures on the VPNs using the strongest key exchange protocols as well as the best hash algorithms that the solution offers for a more secure connection.

REFERENCES

Chultaeiz, D. G. (2022, October 11). *Vyos configuration VPN L2TP*. VyOS Forums. https://forum.vyos.io/t/vyos-configuration-vpn-l2tp/9629

Geek., D. (2010, May 25). *Home*. DNS Knowledge - DNS Tutorial, News and Tools. https://www.dnsknowledge.com/tutorials/centos-tutorials/bind-9/howto-setup-dynamic-dns-ddns/It blog. (2017, December 10). https://www.informaticar.net/how-to-setup-openvpn-on-pfsense/

Install the shrew soft VPN client software. (n.d.). http://www.watchguard.com/help/docs/fireware/12/en-us/Content/en-US/mvpn/ipsec/client/shrew_client_install_c.html

Jammal, B. (2017, July 9). *Site-to-site VPN on a single host using openvpn*. Medium. https://medium.com/@bjammal/site-to-site-vpn-on-a-single-host-using-openvpn-e9c5cdb22f92

L2TP/IPsec Remote Access VPN configuration example¶. pfSense® software Configuration Recipes - L2TP/IPsec Remote Access VPN Configuration Example | pfSense Documentation. (n.d.-a). https://docs.netgate.com/pfsense/en/latest/recipes/l2tp-ipsec.html

LDAP authentication on Active Directory - TechExpert.tips. (n.d.). https://techexpert.tips/pfsense/pfsense-ldap-authentication-active-directory/

Pippin, & Grimson. (2018, November 8). *How to remove ca and certs?*. Netgate Forum. https://forum.netgate.com/topic/137573/how-to-remove-ca-and-certs/3

Site-to-site. Site-to-Site - VyOS 1.3.x (equuleus) documentation. (n.d.). https://docs.vyos.io/en/equuleus/configuration/vpn/site2site_ipsec.html

Troubleshooting authentication¶. Troubleshooting - Troubleshooting Authentication | pfSense Documentation. (n.d.). https://docs.netgate.com/pfsense/en/latest/troubleshooting/authentication.html

Virtual private networks¶. Virtual Private Networks | pfSense Documentation. (n.d.). https://docs.netgate.com/pfsense/en/latest/vpn/index.html

APPENDIX A: PROBLEM SOLVING

Problem 1

Problem Description: An issue with the Certificate authority is preventing the OpenVPN Client Access VPN from working and connecting properly.

Problem Solutions: Delete the current certificate authority and recreate another one, restarting various services, install client export on PfSense.

Solutions Attempted: Delete the current certificate authority and recreate another one, and installing the client export add on for PfSense.

Final Solution: The final solution that worked properly was installing the client export add on for PfSense. This allowed the certificate authority to properly be configured. Before this worked, however, PfSense needed to be updated to the newest version to allow for add-ons to be downloaded and installed.

Problem 2

Problem Description: The L2TP VPN would not allow clients past the authentication step.

Solutions Attempted: Solutions that were attempted for allowing clients past the authentication step of the VPN was to use older key exchange algorithms which did not work, adding MSCHAPv2 requirements which did not work, trying various ShrewSoft VPN Client configurations, and implementing a RADIUS box for authentication, which also did not work.

Final Solution: The final solution attempted was to change the authentication to open, but without a client authentication solution in place, the VPN cannot be established in the first place. Further troubleshooting will need to follow to fix this issue.

Problem 3

Problem Description: Could not get the Site-to-Site VPN to connect both ways between the two DMZs. DMZ A could ping and communicate to DMZ B, but DMZ B could not talk back.

Problem Solutions: Change the IP configurations around to ensure the issue does not rely on IPv4, change and ensure the encryption ciphers are the same, ensure the devices have the same keys, ensure the settings are the same.

Solutions Attempted: The solutions that were attempted involve ensuring the IP addresses were correct, ensuring the devices had the same settings, and ensuring the same encryption was used. Devices were also shutdown and restarted as a last effort.

Final Solution: The final solution was never found, and the Site-to-Site OpenVPN solution was only a one way working VPN tunnel. Unfortunately, after much troubleshooting, the solution was never discovered.

APPENDIX B: IP Addressing

CentOSA: 192.168.1.2

CentOSB: 172.18.32.2

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: 172.18.32.1

PrivB NIC: 192.168.2.1

Winpublic: 44.104.32.7

WinsrvA: 192.168.3.2

WinsrvB: 192.168.2.2