Virtual Private Networks

Josh Lieberg

Submitted To: Tony Wan

Date Submitted: 10/21/24

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report provides a comprehensive summary of the Virtual Private Networks lab, which is a critical project for Computer Industries. The primary purpose of this initiative is to develop and expand the current architecture by implementing three different types of virtual private networks (VPNs). As the company rapidly expands and relies increasingly on digital operations, the need for access to differing networks becomes essential in the continuation of business operations.

This phase implements a total of five VPNs, an IPsec Site-to-Site, an IPsec Client-Access, an L2TP over IPsec Client-Access, an OpenVPN Client-Access, and an OpenVPN Site-to-Site VPN. The reason for this new expansion is to ensure users are able to access all necessary resources to complete tasks outlined in their job description. In order to complete the setup of the IPsec VPNs, a Radius server was implemented on both of the Domain Controllers that already exist within the architecture. Through the use of pre-shared keys, users are able to authenticate and utilize that VPN. In order to implement both OpenVPN solutions, a Certificate Authority was created on the pfSense machine and necessary Certificate Services were installed on both Domain Controllers. These changes allowed for any authenticated users to access needed networks while working.

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 has decided to expand again to ensure that its infrastructure remains secure yet accessible. The company plans to implement multiple VPNs across the entire network to allow for better security as well as remote access. 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 these five VPNs into the already existing architecture. The IPsec Site-to-Site VPN will allow for connections between both Domain Controllers located on the Private networks, the IPsec Client-Access VPN will allow for any public client to be able to access the pfSense DMZ, the L2TP over IPsec Client-Access VPN will allow for any public client to access the VyOS Private network, the OpenVPN Client-Access VPN will allow for any public client to access the pfSense Private network, and the OpenVPN Site-to-Site VPN will allow for connections between both the pfSense DMZ and the VyOS DMZ.

In order to complete the goal of increased security and remote access, a Radius server was created on both Domain Controllers. This service is able to receive requests from the VPN and authenticate the user based on credentials located within the Active Directory. If the credentials are valid, then a connection is established to the network through the VPN. Also installed within this project were Certificate Services. A standalone Certificate Authority (CA) was initialized to incorporate machines not integrated into Windows Active Directory while still allowing for a Public Key Infrastructure (PKI). A CA was created on both sides of the architecture with certificates being shared between the two in order to create trust between the

networks. Figure 1 shows the current layout of the logical architecture which includes two Alma Linux machines, two Windows 2019 Servers, and Windows 10 machine, a pfSense firewall, and a VyOS Router.

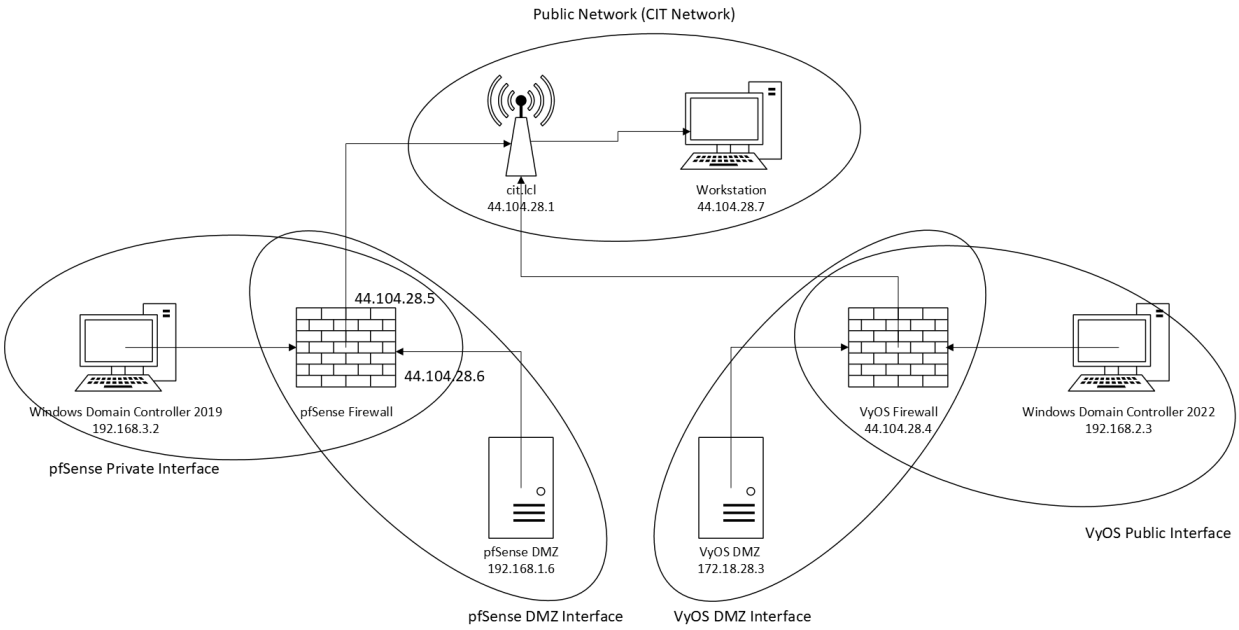

Figure 1: Logical Diagram

The changed system would not require any upgrades to any machines currently located within the existing architecture. Firewall rules will be updated to accommodate the new traversal of information across the network and to ensure the continued promise of a secure network.

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*

L2TP Over IPSec VPN

The steps below describe the process used to create L2TP VPN. This VPN allows for public users to connect to the Private network through the VyOS Router.

1. Typed `configure` in VyOS router
2. Typed `set vpn l2tp remote-access authentication local users username group28 password cyber455`
3. Entered `set vpn l2tp remote-access authentication mode radius`
4. Entered `set vpn l2tp remote-access authentication radius server 192.168.2.3 key group28key`
5. Typed `set vpn l2tp remote-access authentication radius server 192.168.2.3 port 1812`
6. Typed `set vpn l2tp remote-access authentication radius source-address 192.168.2.1`
7. Entered `set vpn l2tp remote-access client-ip-pool L2TP-POOL range 192.168.10.100-192`
8. Entered `set vpn l2tp remote access default-pool L2TP-POOL`
9. Typed `set vpn l2tp remote access ipsec-settings authentication mode pre-shared-secret`
10. Typed `set vpn l2tp remote access ipsec-settings authentication pre-shared-secret group28key`
11. Entered `set vpn l2tp remote-access name server 192.168.2.3`
12. Entered `set vpn l2tp remote-access outside access 44.104.28.4`

13. Entered `set vpn l2tp remote-access ppp-options ipv4 allow`

Deploy RADIUS Server on Domain Controllers

RADIUS is used to authenticate users accessing the network through the VPN. The VPN queries the firewall, which sends that request to the RADIUS server to authenticate the user. Upon successful authentication the connection is established.

1. Opened Private B machine
2. Opened Server Manager
3. Selected *Manage*
4. Chose Add Roles and Features
5. Clicked **Next** | *Role based* | **Next** | **Next**
6. Selected *Network Policy and Access Services* and then **Next**
7. Selected *Network Policy Server* | **Next** | **Install** | **Close**
8. Repeated steps 2-7 on Private A machine

Configuration of RADIUS

RADIUS is used to authenticate users when trying to access a network over a VPN. After installation it must be configured to allow authentication.

1. Opened Server Manager
2. Selected *Tools* and then *Network Policy Server*
3. Right-clicked *NPS (local)*
4. Selected *Register server in Active Directory* | **OK** | **OK**
5. Selected *RADIUS Clients and Servers* | *RADIUS Clients* | **New**

6. Entered VPN Server for the friendly name
7. Entered the IP address of the DC
8. Set the shared secret to `group28key` and clicked **OK**
9. Selected *Policies* | *Network Policies* | **New**
10. Entered `VPN Connection` as policy name
11. Selected *Remote Access Server (VPN - Dial-Up)* and then **Next**
12. Clicked *Add* | *User Groups* | *Add Groups* | *VPN Users* | **OK** | **Next**
13. Set Authentication to *Access Granted* and Authentication Method to *MS-CHAPv2*
14. Selected **Finish**

Open VPN (SSL) Client Access VPN

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. Clicked VPN | OpenVPN | Servers
2. Clicked Add | Changed Server mode to Remote Access (User Auth)
3. Changed IPv4 Tunnel Network to `44.104.28.5/24`
4. Changed IPv4 Local network(s) to `192.168.1.0/24`
5. Clicked System | Certificates | Authorities | Add
6. Typed CAfor OpenVPN as Descriptive Name | Selected US as Country Code
7. Typed Indiana for State or Province | Typed West Lafayette for City | Typed PrivA.lcl as Organization | Clicked Save

Creation of Certificate Authority

A Certificate Authority is needed to create certificates that are usable within the network to provide authentication. These certificates can be used by endpoint machines as well as between CAs to provide trust.

1. Opened *Server Manager* | *Manage* | *Add roles and Features* | **Next** | **Next** | **Next** | *Active Directory Certificate Services* | **Add Features** | **Next** | **Next** | **Next** | *Certificate Authority Web Enrollment* | **Add Features** | **Next** | **Next** | **Next** | **Install**
2. Clicked Configure Active Directory Certificate Services on this computer | Next | Certification Authority | Standalone CA | next | Root CA | next | Create a new private key | Next | Typed PrivateBCA for Common Name | Next | Next | Next | Configure
3. Tools | Certification Authoritry | Right Clicked PrivateACA | Properties | View Certificate | Details | Copy to File… |

Adding DNS to pfSense

In order to ensure that clients are able to access internal resources, DNS was configured to ensure that internal connectivity continued to be established over a VPN.

1. Logged into CNIT45500.g28.pfDMZ
2. Opened Firefox
3. Entered https://192.168.1.1
4. Logged in
5. Clicked *System* | *General Setup*
6. Entered `44.2.1.44` and `cit.lcl`

7. Clicked **Save**

Installed openvpn-client-export package

Installing the openvpn-client-export package allows for the exporting of OpenVPN client configuration files. In order to use OpenVPN on a client, that user must install and import the configuration file in order to be able to use the VPN.

1. Logged into CNIT45500.g28.pfDMZ
2. Opened Firefox
3. Entered `https://192.168.1.1`
4. Clicked *System* | *Package Manager* | *Available Packages*
5. Clicked **Install** on openvpn-client-export

Adding a Certificate Authority Into pfSense

The Certificate Authority (CA) created within pfSense acts as the central CA. Certificates created in this location are added to other CAs in order to provide trust throughout the whole network.

1. Logged into CNIT45500.g28.PrivA
2. Opened Google Chrome
3. Entered `https://192.168.1.1`
4. Logged in
5. Clicked *System* | *Certificates* | *Authorities* | **Add**
6. Entered `OpenVPN_CA` into Descriptive Name
7. Checked **Add this Certificate Authority to the Operating System Trust Store**
8. Entered `OpenVPN_CA` into Common Name

9. Clicked **Save**

Adding a Certificate Into pfSense

A certificate must be created on the CA before it can be sent to other CAs. This is the document that users and other machines will authenticate against.

1. Clicked *System* | *Certificates* | *Certificates* | **Add**
2. Entered `OpenVPN_Cert` into Descriptive Name
3. Selected *OpenVPN_CA* for the Certificate Authority
4. Entered `365` into Lifetime (days)
5. Entered `OpenVPN_Cert` into Common Name
6. Selected *Server Certificate* for the Certificate Type
7. Clicked **Save**

VPNUserCreating Constant VPN Users On Domain Controller

In order to be able to use a VPN, users must have an account already created within Active Directory. This is the way in which they will be authenticated and able to use the VPN.

1. Logged into CNIT45500.g28.PrivA
2. Opened Active Directory Users and Computers
3. Clicked *Users* | *New* | *Group*
4. Entered `VPNUsers` into Group Name
5. Clicked **OK |** *Josh Lieberg* | *Add to a group…*
6. Entered `VPNUsers`
7. Clicked **Check Names | OK**

Adding an Authentication Server Into pfSense

An Authentication Server is another form of authentication implemented into pfSense itself. It also confirms user credentials to ensure that valid credentials are granted access to a VPN and invalid credentials are not allowed.

1. Opened Google Chrome
2. Entered `https://192.168.1.1`
3. Clicked *System* | *User Manager* | *Authenticated Servers* | **Add**
4. Entered `Active Directory` into Descriptive Name
5. Entered `192.168.3.2` into Hostname or IP Address
6. Selected *OpenVPN_CA* for the Peer Certificate Authority
7. Selected *Entire Subtree* into Search Scope
8. Entered `DC=PrivA,DC=lcl` into Base DN
9. Entered `CN=Users,DC=PrivA,DC=lcl` into Authentication Containers
10. Selected **Select a container | Ok**
11. Unchecked *Bind Anonymous*
12. Entered `jlieberg@PrivA.lcl` and `PASSWORD` into Bind Credentials
13. Selected *Microsoft AD* for Initial Template
14. Clicked **Save**

Adding an OpenVPN Server Into pfSense

An OpenVPN server allows for the creation of tunnels. This allows for the creation of encrypted channels for information to flow through. These channels improve security and privacy within the network.

1. Clicked *VPN* | *OpenVPN* | *Servers* | **Add**
2. Entered `Corp_VPN` into Description
3. Selected *Remote Access (User Auth)* for Server Mode
4. Selected *Active Directory* for Backend for Authentication
5. Selected *TCP on IPv4 Only* for Endpoint Configuration Protocol
6. Entered `11940` for Endpoint Configuration Local Port
7. Selected *OpenVPN_CA* for Peer Certification Authority
8. Selected *OpenVPN_Cert (Server: Yes, CA: OpenVPN_CA, In Use)* for Server Certificate
9. Unchecked *Enforce Key Usage*
10. Entered `192.168.28.0/24` into IPv4 Tunnel Network
11. Entered `192.168.3.0/24` into IPv4 Local Network(s)
12. Entered `100` into Concurrent Sessions
13. Selected *Decompress incoming, do not compress outgoing (Asymmetric)* for Allow Compression
14. Selected *Adaptive LZO Compression [Legacy style, comp-lzo adaptive]* for Compression
15. Checked *Inter-client* | *Dynamic IP* | *DNS Default Domain*
16. Entered `PrivA.lab` for DNS Default Domain
17. Checked *DNS Server Enable*
18. Entered `192.168.3.2` for DNS Server 1
19. Checked *NetBIOS Enable* | *IPv4 Only*
20. Clicked **Save**

Adding OpenVPN Rules Into pfSense

Firewall rules over the OpenVPN interface allow admins to control the flow of traffic over the VPN. By only allowing certain types of traffic to travel over the interface, network security is improved.

1. Clicked *Firewall* | *Rules* | *OpenVPN* | **Add**
2. Selected *Any* for Protocol
3. Entered `OpenVPN Traffic` for Description
4. Clicked **Save | Apply Changes | WAN | Add**
5. Entered `11940` for Destination Port Range
6. Entered `OpenVPN WAN Traffic` for Description
7. Clicked **Save | Apply Changes**

Client Export for OpenVPN

In order for a client machine to be able to use OpenVPN, they must first import the correct files. These steps showed how the client export was configured to allow a client to be able to import that configuration.

1. Selected *VPN* | *OpenVPN* | *Client Export*
2. Selected *Corp_VPN TCP4:11940* for Remote Access Server
3. Clicked **Most Clients** under Export Inline Configurations
4. Opened File Explorer C:\Users\Administrator\Downloads
5. Copied pfSense-TCP4-11940-config into Google Drive

Installing OpenVPN on CNIT45500.g28.WindowsPUBLIC

In order for a client machine to be able to use OpenVPN, they must first download the application. These steps showed how the client export was configured to allow for the public machine to connect to the VPN.

1. Opened Google Chrome
2. Entered `https://openvpn.net/client/client-connect-vpn-for-windows/`
3. Clicked **Download OpenVPN Connect v3 |** *openvpn-connect-3.5.0.3818_signed.msi* **| Run | Next | I accept the terms in the License Agreement | Next | Install | Finish | Agree |** *Upload File*
4. Dragged pfSense-TCP4-11940-config into OpenVPN Connect
5. Entered `jlieberg@PrivA.lcl`
6. Clicked **Connect**
7. Entered `Password`
8. Clicked **Connect**

IPSec Site-to-Site VPN

An IPSec Site-to-Site VPN was established between two virtual machines on different private networks. The VPN was configured on the PfSense web configurator as well as VyOS.

1. Opened *CNIT45500.g28.VyOS*
2. Typed `set vpn ipsec authentication psk vyos id 44.104.28.4 | set vpn ipsec authentication psk vyos id 44.104.28.5 | set vpn ipsec authentication psk vyos secret pickle`

3. Typed `set vpn ipsec esp-group ESPGroup lifetime 3600 | set vpn ipsec esp-group ESPGroup proposal 1 encryption aes256 | set vpn ipsec esp-group ESPGroup proposal 1 hash sha256 | set vpn ipsec esp-group ESPGroup pfs dh-group14`
4. Typed `set vpn ipsec ike-group IKEGroup proposal 1 dh-group '14' | set vpn ipsec ike-group IKEGroup proposal 1 encryption aes256 | set vpn ipsec ike-group IKEGroup proposal 1 hash sha256 | set vpn ipsec ike-group IKEGroup lifetime 28800`
5. Typed `set vpn ipsec site-to-site peer right authentication mode pre-shared-secret | set vpn ipsec site-to-site peer right authentication remote-id 44.104.28.5 | set vpn ipsec site-to-site peer right authentication local-id 44.104.28.4`
6. set `vpn ipsec site-to-site peer right default-esp-group ESPGroup | set vpn ipsec site-to-site peer right ike-group IKEGroup | set vpn ipsec site-to-site peer right local-address 44.104.9.4 | set vpn ipsec site-to-site peer right remote-address 44.104.9.5`
7. Typed `set vpn ipsec site-to-site peer right tunnel 1 local prefix 192.168.2.0/24 | set vpn ipsec site-to-site peer right tunnel 1 remote prefix 192.168.3.0/24 | commit`
8. Entered `https://192.168.1.1`
9. Logged in | Clicked **VPN** | **IPSec** | **Add P1**

10. Changed Remote Gateway to `44.104.28.4` | Changed My identifier to IP Address `44.104.28.5` | Changed Peer Identifier to IP Address `44.104.28.4` | Changed Pre-Shared key to `pickle`
11. Changed Encryption Algorithm to *AES 256bits* | Changed Hash to *SHA256* | Changed DH Group to *14* | Changed Life Time to `28800`
12. Clicked **Show Phase 2 Entries** | **Add P2**
13. Changed Local Network to `192.168.3.0/24` | Changed Remote Network to `192.168.2.0/24`
14. Changed Encryption Algorithms to AES 256 bits | Selected a Hash of *SHA256* | Selected a PFS key group of *14 (2048 bit)*
15. Clicked **Save** | **Apply Changes**

RESULTS

The team at Computer Industries has successfully implemented a secure and comprehensive virtual private network (VPN) infrastructure that meets the evolving needs of the organization. The new network includes multiple VPN solutions, enhancing security and scalability while ensuring high availability and ease of management. These upgrades were necessary as the previous architecture lacked the capabilities to support the company's growing operations and security demands.

To address the concerns that the previous architecture had, the team transitioned to a VPN-centric architecture, utilizing a range of VPN solutions, including IPsec, L2TP, and SSL. This hybrid approach allowed Computer Industries to enhance security and remote connectivity while maintaining a flexible and scalable environment.

The IPSec Site-to-Site VPN allows encrypted communication between the different office locations, ensuring secure data transfer between internal and private networks. The IPSec Client-Access VPN allows remote employees and third-party employees of Computer Industries to access the company’s internal resources. The L2TP over IPsec Client-Access VPN provides remote access to specific private networks with RADIUS authentication. Utilizing RADIUS is crucial to ensure that users are securely verified before gaining access to critical internal systems. The OpenVPN SSL Site-to-Site allows secure communication between the companies DMZ’s of different locations within the Computer Industries network. The OpenVPN SSL Client-Access allows external clients to securely connect to the company's network.

Figure 2 below illustrates how the various VPN solutions are interconnected within the network, showing the pfSense firewall managing traffic across different zones and the VyOS firewall facilitating secure communication between the internal and external networks. The

diagram highlights the deployment of multiple VPN solutions, including the IPsec Site-to-Site VPN for secure office-to-office communication, the IPsec and L2TP over IPsec Client-Access VPNs for remote user access, the OpenVPN SSL Site-to-Site VPN for encrypted communication between the DMZs, as well as the OpenVPN SSL Client-access VPN. This entire VPN architecture is designed to be secure, scalable, and flexible, allowing Computer Industries to support continued growth while maintaining a high level of security.

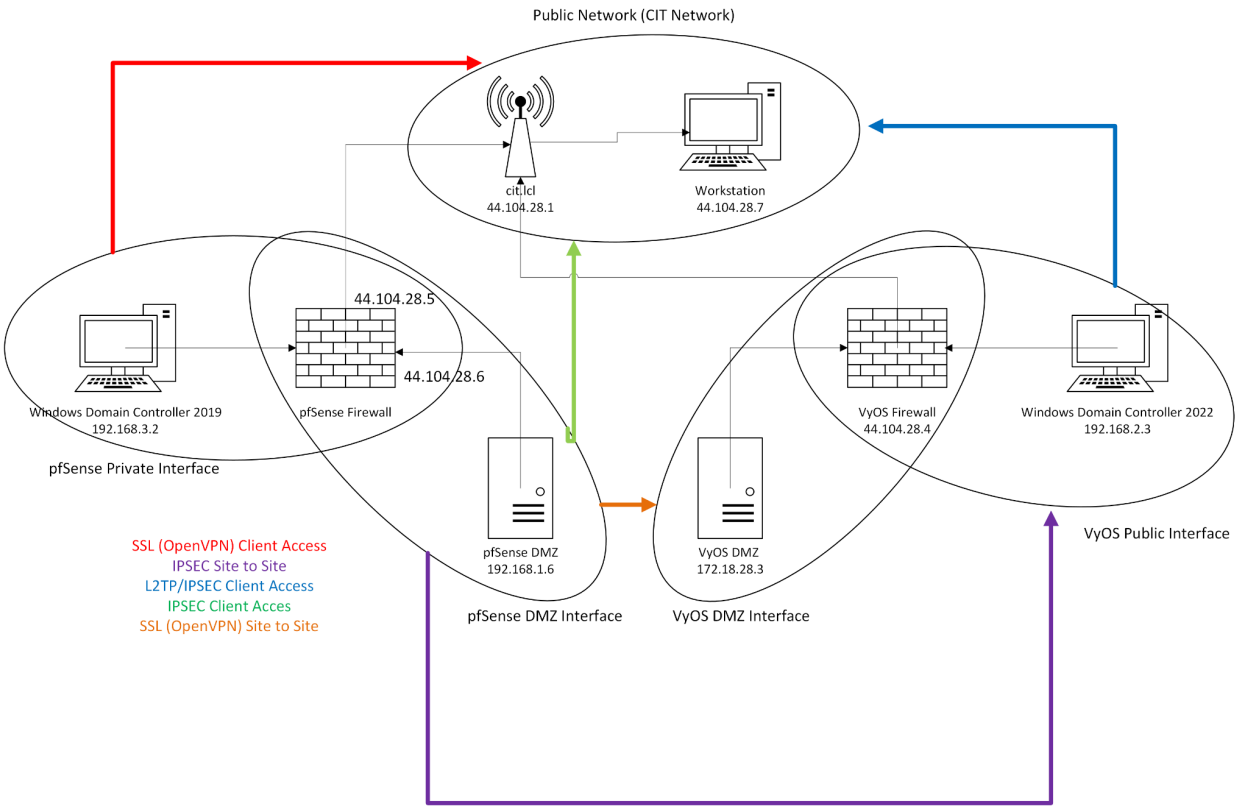

Figure 2: Logical Diagram

The pfSense firewall and VyOS firewall play a pivotal role in managing traffic across these VPNs, ensuring that only authorized traffic flows between the public and private networks. With this deployment, all VPN traffic is encrypted and routed efficiently between the appropriate zones, minimizing potential attack surfaces and maximizing security.

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 modernize the network infrastructure at Computer Industries by implementing secure Virtual Private Network (VPN) solutions. The old network architecture did not have the robust security measures required to safely secure sensitive data and ensure secure communication, making it essential to build a more advanced VPN-based solution.

The team at Computer Industries was tasked with deploying multiple VPN solutions to meet the organization's growing security demands. Five distinct VPN configurations were implemented: an IPsec Site-to-Site VPN, an IPsec Client-Access VPN, an L2TP over IPsec Client-Access VPN, an OpenVPN SSL Client-Access VPN, and an OpenVPN SSL Site-to-Site VPN. These VPNs were designed to work concurrently and provide secure connections across different parts of the network. The project team ensured that each VPN configuration adhered to the security protocols outlined in the business requirements. Throughout the process, all VPN traffic was encrypted and tested to confirm that the connections were stable, secure, and resistant to potential threats.

In conclusion, the newly implemented VPN architecture successfully addressed all of Computer Industries' network security requirements. The deployment of these VPNs has strengthened the company's infrastructure, providing secure, reliable remote access and protecting against external threats. This network upgrade will support the company's growth by allowing employees and clients to connect safely from anywhere, without compromising the integrity of the system.

Recommendations

To improve upon basic VPN 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: Divide & Conquer

Computer Industries gave the team a broad objective of completing the five VPN configurations for the infrastructure. The team carried out these tasks one by one, focussing all of our power on one before moving on to another. However, dividing the tasks among the three team members might have yielded better results. Each team member would have been able to focus on one or two specific areas and allow for simultaneous progress on tasks.

Recommendation 2: Manage Time Better

Initially, the team at Computer Industries was allotted four weeks to complete the VPN configuration project. However, as the team members balanced other ongoing responsibilities, it became difficult to maintain a steady focus on the VPN setup. When the VPN configurations were due, the team was not fully prepared to showcase the completed infrastructure. This problem could have been mitigated by better task management and proactive timeline adjustments.

Recommendation 3: Test Configuration More Than Once

One of the bigger issues the team faced with the VPN setup was inconsistent results during testing. Sometimes certain VPN's would work perfectly during tests but when it came time to show an operational VPN, the VPN failed. The testing issues were unforeseen which left the

team in a bad place. Testing the configurations more than once would allow for accurate consideration if the VPN was done or not.

BIBLIOGRAPHY

adrianp918, Vollans, da_Beast, SteveITS, Glacialcalamity, Antoniojf, Pritchard, S., Raymondd, Jacobss, Antony, C., Snigy, Billy_C, & JonathanLee. (2024, August 9). *Pfsense new install no software packages available.* Netgate Forum. https://forum.netgate.com/topic/178200/pfsense-new-install-no-software-packages-available

IPsec site-to-site VPN example with pre-shared keys¶. IPsec Site-to-Site VPN Example with Pre-Shared Keys | pfSense Documentation. (n.d.). https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html

IPsec. IPsec - VyOS 1.5.x (circinus) documentation. (n.d.). https://docs.vyos.io/en/latest/configuration/vpn/ipsec.html

L2TP. L2TP - VyOS 1.5.x (circinus) documentation. (n.d.). https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html

OpenVPN client export package¶. OpenVPN Client Export Package | pfSense Documentation. (n.d.). https://docs.netgate.com/pfsense/en/latest/packages/openvpn-client-export.html

PfSense OpenVPN Setup tutorial – strongvpn. (n.d.). https://support.strongvpn.com/hc/en-us/articles/360038592794-pfSense-OpenVPN-Setup-Tutorial

Phase 1 settings¶. Phase 1 Settings | pfSense Documentation. (n.d.). https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/configure-p1.html#ipsec-phase1

says, R. T., Tracy, R., says, A. B., Bas, A., says, R. P. V., Villalon, R. P., says, V., Vip, Says, Y., Yunus, says, M., Marcus, says, M., Miki, says, M. C., Chen, M., says, J., Jc, says, N., …

Nuno. (2022a, November 3). *L2TP/ipsec VPN on windows server 2019.* Snel.com. https://www.snel.com/support/how-to-set-up-an-l2tp-ipsec-vpn-on-windows-server-2019/

says, R. T., Tracy, R., says, A. B., Bas, A., says, R. P. V., Villalon, R. P., says, V., Vip, Says, Y., Yunus, says, M., Marcus, says, M., Miki, says, M. C., Chen, M., says, J., Jc, says, N., …

Nuno. (2022b, November 3). *L2TP/ipsec VPN on windows server 2019.* Snel.com. https://www.snel.com/support/how-to-set-up-an-l2tp-ipsec-vpn-on-windows-server-2019/

APPENDIX A: PROBLEM SOLVING

Problem 1: IPSec VPN not establishing

Problem Description: After configuring both pfSense and VyOS firewalls to set up an IPsec VPN, the VPN tunnel failed to establish. Despite correctly inputting all necessary parameters, including pre-shared keys, encryption algorithms, and network ranges, the VPN connection status did not establish.

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 VPN or the private machines. A second solution is a potential misconfiguration in the phase one or phase two web config settings, which might prevent the tunnel from establishing. The final solution was that there may be an issue with the VyOS configuration. An error in the VyOS configuration would stop the traffic between the two endpoints.

Attempted Solutions: The first solution was attempted initially by setting all firewall rules on both sides to allow all traffic. While allowing all traffic is not best practice, allowing all traffic is necessary for troubleshooting. This solution did not work as the problem persisted. Solution two and three were also attempted. Both configs were combed over carefully but the team could not find anything inherently incorrect.

Final Solution: Unfortunately, there was no final solution to this problem. Further investigation is required to identify any underlying issues, including a potential review of logs for any misread error messages, testing with different configurations, or seeking external assistance for more advanced troubleshooting.

Problem 2: OpenVPN LDAP authentication error

Problem Description: After configuring OpenVPN with LDAP authentication, the test user began experiencing issues where their previously functional usernames and passwords no longer authenticated. This sudden failure in authentication prevented the user from establishing VPN connections, despite no apparent changes to the configuration or user credentials.

Possible Solutions: One solution is to ensure that the LDAP Server can connect with the OpenVPN server. Any network issues could prevent successful authentication. Another simple solution is to confirm that the user credentials are still enabled in the Active Directory. Any account lockouts, expired passwords, or changes to user permission could cause this issue. A third solution is to flush the DNS and IP cache of the domain controller. Flushing the DNS and IP cache would allow any incorrect network information that may interfere with authentication requests to resolve.

Attempted Solutions: The first solution was attempted but did not fix the problem because the connection to the LDAP server was established and steady. The second solution also did not fix the problem because the user was confirmed to be enabled in the Active Directory.

Final Solution: The third solution fixed the problem. Running `ipconfig /flushdns` and `ipconfig /registerdns`. This improvement confirmed that the VPN connection was now functioning correctly, allowing users to establish secure connections without encountering previous errors. The successful resolution not only restored access but also highlighted the importance of maintaining up-to-date DNS records within the network infrastructure.

Problem 3: L2TP communication problems

Problem Description: After successfully establishing a connection to the L2TP VPN, a new issue arose where the client could connect to the VPN but was unable to ping any machines within the network or access the internet. This lack of connectivity prevented the client from interacting with internal resources or reaching external sites.

Possible Solutions: One solution was to check the firewall rules in pfSense to ensure traffic from the L2TP clients was not being accidentally blocked. Another solution was to fix the routing table on the VPN server so that L2TP clients could reach other networks in the infrastructure. A third solution was to check the L2TP configuration to ensure all clients were not isolated from the network.

Attempted Solutions: The first approach involved adjusting the firewall rules to allow all traffic, just like problem one. Again, this is not necessarily best practice but is tremendously helpful for troubleshooting. The routing tables of the two VPN servers were checked to confirm the configuration was correct. Finally, the L2TP server was inspected.

Final Solution: Unfortunately, there was no final solution to this problem. Further investigation is required to identify any underlying issues, including a potential review of logs for any misread error messages, testing with different configurations, or seeking external assistance for more advanced troubleshooting.

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: OpenVPN

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	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: 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 5: 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	*

Table 2: IPsec

Action	Protocol	Source	Port	Destination	Port	Gateway

Pass	IPv4 *	*	*	*	*	*

APPENDIX D: VYOS CONFIGS

```
group28@Router1# show
 firewall {
    global-options {
        all-ping enable
    }
    ipv4 {
        forward {
            filter {
                rule 5 {
                    action jump
                    inbound-interface {
                        name eth0
                    }
                    jump-target site2site
                }
            }
        }
        name l2tp {
            rule 100 {
                action accept
                protocol esp
            }
```

```
        rule 110 {
            action accept
            destination {
                port 500
            }
            protocol udp
        }
        rule 120 {
            action accept
            destination {
                port 4500
            }
            protocol udp
        }
        rule 130 {
            action accept
            destination {
                port 1701
            }
            ipsec {
                match-ipsec
            }
            protocol udp
        }
        rule 140 {
            action accept
```

```
            destination {
                port 1812
            }
            protocol udp
        }
    }
    name one {
        rule 1 {
            action reject
        }
    }
    name site2site {
        default-action accept
    }
    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
        ip {
            enable-proxy-arp
        }
    }
    loopback lo {
    }
    openvpn vtun0 {
        encryption {
            cipher aes256
        }
        hash sha256
        local-address 192.168.69.2 {
            subnet-mask 255.255.255.252
        }
        local-host 44.104.28.4
        local-port 1194
        mode site-to-site
        persistent-tunnel
        protocol udp
        remote-address 192.168.69.1
```

```
        remote-host 44.104.28.5
        remote-port 1194
        shared-secret-key group28
    }
    tunnel tun0 {
        encapsulation gre
        remote 192.168.3.1
        source-address 192.168.2.1
    }
}
 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 65 {
            destination {
                address 192.168.3.0/24
            }
            exclude
            outbound-interface {
                name eth0
            }
        }
        rule 110 {
            outbound-interface {
                name eth0
```

```
            }
            source {
                address 192.168.2.0/24
            }
            translation {
                address masquerade
            }
        }
    }
}
 pki {
    openvpn {
        shared-secret group28 {
            key
8402c53f0031bc3fc2d8b9d0825cc8121f1a7c8102f11ae13b6c97c52da5f56b029229f1815c8662
46117b037b30cb90302a45ec0a7838bf11b2b79a654af53d02b94a53f2248725cd1385bf7e3afc1
cf989d62a2cd2bcef0c7af159adcd2bc7d898ee59a26be511748731343af8f4510f5f237cf607a2ac
1e2076009aca884d8d70e9ca573273afc11f6e228a6ebf4687b4fe9db46fa0ec53e9fb3d4ffa134b6
bd79c7e6a5db0221e6e2c76396fe074c6eec4d694abeed3d2467949f70af4cd46f273857a55d88a
e3b95b28a096b3482468955aee005b40aab2524fcd7b029c7162924d2a7862cedf263f71af4e60
14643b5ac4c80a289ec0be8f788ba71a3e
        }
    }
}
 protocols {
    static {
```

```
        route 0.0.0.0/0 {
            next-hop 44.104.28.1 {
            }
        }
        route 192.168.1.0/24 {
            interface vtun0 {
            }
        }
        route 192.168.2.0/24 {
            next-hop 192.168.2.1 {
            }
        }
    }
}
 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 {
        radius {
            server 192.168.2.3 {
                key group28key
                port 1812
                timeout 5
            }
        }
        user group28 {
            authentication {
                encrypted-password
$6$rounds=656000$K03Cy4G03Ucf9iM8$jQ/EYjPCrGJaPFirFAlp6rdBOhb962ojShJve.x/yknLM
pWmwFBuVf0YDnPqyu49mBTH9DqF4ulS.hR0CkY2m/
            }
        }
        user vyos {
            authentication {
                encrypted-password
$6$QxPS.uk6mfo$9QBSo8u1FkH16gMyAVhus6fU3LOzvLR9Z9.82m3tiHFAxTtIkhaZSWssSgzt
4v4dGAL8rhVQxTg0oAG9/q11h/
                plaintext-password ""
            }
        }
    }
    name-server 44.2.1.44
```

```
    syslog {
        global {
            facility all {
                level info
            }
            facility local7 {
                level debug
            }
        }
    }
}
vpn {
    ipsec {
        authentication {
            psk vyos {
                id 44.104.28.4
                id 44.104.28.5
                secret pickle
            }
        }
        esp-group ESPGroup {
            lifetime 3600
            pfs dh-group14
            proposal 1 {
                encryption aes256
                hash sha256
```

```
        }
    }
    ike-group IKEGroup {
        lifetime 28800
        proposal 1 {
            dh-group 14
            encryption aes256
            hash sha256
        }
    }
    site-to-site {
        peer right {
            authentication {
                local-id 44.104.28.4
                mode pre-shared-secret
                remote-id 44.104.28.5
            }
            default-esp-group ESPGroup
            ike-group IKEGroup
            local-address 44.104.9.4
            remote-address 44.104.9.5
            tunnel 1 {
                local {
                    prefix 192.168.2.0/24
                }
                remote {
```

```
                prefix 192.168.3.0/24
            }
        }
    }
}
l2tp {
    remote-access {
        authentication {
            local-users {
                username group28 {
                    password cyber455
                }
            }
            mode radius
            radius {
                server 192.168.2.3 {
                    key group28key
                    port 1812
                }
                source-address 192.168.2.1
            }
        }
        client-ip-pool L2TP-POOL {
            range 192.168.10.100-192.168.10.200
        }
```

```
            default-pool L2TP-POOL
            gateway-address 192.168.2.1
            ipsec-settings {
                authentication {
                    mode pre-shared-secret
                    pre-shared-secret group28key
                }
            }
            name-server 192.168.2.3
            outside-address 44.104.28.4
            ppp-options {
                ipv4 allow
            }
        }
    }
}
[edit]
group28@Router1#
```