BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

FULLNAME PRIDE DZITIRO

REG NUMBER B200974B

COURSE CODE IT 400

PROGRAM NAME

BACHELOR OF SCIENCE HONOURS DEGREE IN INFORMATION TECHNOLOGY

RESEARCH PROJECT TITLE

IMPLEMENTATION OF SECURE VPN OVER AN OPEN NETWORK INFRASTRUCTURE. A CASE STUDY OF CHAMPIONS INSURANCE COMPANY

SUBMISSION APPROVAL

I hereby certify that, **PRIDE DZITIRO (Registration Number B200974B)** was under my supervision for the purpose of the Network Engineering in fulfilment of the requirements for the degree of Bachelor Honours Degree in Network Engineering. I also attest that she attended all revisions requirements to my satisfaction and participated in scheduled feedback sessions with me as the supervisor. I further confirm that the student demonstrated the functionality of the system to me. Therefore, the student has been granted permission to submit his/her project documentation for examination.

SUPERVISOR **DATE 09/06/25**

CHAIRPERSON: **DATE 09/06/25**

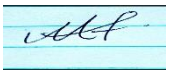
EXTERNAL EXAMINER: **DATE:**

DECLARATION FORM

I Pride Dzitiro hereby declare that this submission is my own work apart from the references of other people's work which has been acknowledged. I hereby declare that, this project has neither been presented in whole or part for any degree at this university or elsewhere

Author: DZITIRO PRIDE

Registration Number: B200974B

Signature: 

Date: 21 November 2024

DEDICATION

This dissertation is devoted to my mother and father, Mr and Mrs Dzitiro

ACKNOWLEDGEMENT

First and most I would like to give thanks to the almighty for gift of life and for helping me embrace this journey. I would also like to give gratitude to my supervisor, Mr Musariwa for her academic input, for her academic guidance which significantly contributed to the successful completion of this project. And I would also like to express my gratitude to all the staff members of the department of computer science for the moral support throughout the duration of the course. I am indebted to my friend Anotida for her encouragement and companionship. Special gratitude to my family, whose enduring patience, financial assistance and technical expertise have been invaluable throughout my whole life

Table of Contents

DECLARATION FORM ---- 3
DEDICATION ---- 4
ACKNOWLEDGEMENT ---- 5
ACRONYMS ---- 8
CHAPTER 1 ---- 10
1.1: INTRODUCTION ---- 10
1.2: BACKGROUND OF THE STUDY ---- 11
1.3: PROBLEM STATEMENT ---- 11
1.4: PROJECT AIM ---- 12
1.5: RESEARCH OBJECTIVES ---- 12
1.6: RESEARCH QUESTIONS ---- 12
1.7: JUSTIFICATION ---- 13
1.8: Project Limitations ---- 13
1.9: Research Hypothesis ---- 14
1.10: CHAPTER SUMMARY ---- 15
CHAPTER 2: LITERATURE REVIEW ---- 16
2.1: Introduction ---- 16
2.1.1: How a VPN works ---- 17
2.2.: Types of VPN ---- 18
2.2.1: Site-to-site VPN ---- 19
2.2.2; IPsec Remote Access VPN ---- 20
2.2.3: Clientless Secure Socket Layer (---- 21
2.3: VPN Tunnelling ---- 22
2.4: VPN Protocols ---- 23
2.4.1: Types of VPN Protocols ---- 23
2.5: VPN Split Tunnelling ---- 26
2.6: IPsec VPN fundamentals ---- 27
2.7: IPSec VPN Negotiations ---- 28
2.8: IPsec protocols ---- 33
2.9: IPsec Modes of Operation ---- 34
CHAPTER 3: Methodology ---- 36
3.1: Introduction ---- 36
3.2: Research design ---- 36
3.3: Requirements Analysis ---- 36
3.3.1 Functional Requirements ---- 36

3.3.2: Non functional requirements----37
3.4: System Development----37
3.4.1: System Development tools----38
3.5: Summary of how the system works ----40
3.6: System Design----40
3.6.1: Dataflow Diagram ----41
3.6.2 Proposed System flow chart----41
3.7: Implementation----41
3.8: Chapter Summary----42
CHAPTER 4: DATA ANALYSIS AND INTEPRETATIONS ----43
4.1: Introduction ----43
4.2: Simulation Setup ----43
4.3: Chapter Summary----47
Chapter 5: RECOMMENDATIONS AND FUTURE WORK ----48
5.1: INTRODUCTION----48
5.3: CONCLUSION ----48
5.4: Recommendations ----48
5.5: Future Work ----48
REFERRANCE----50

ACRONYMS

1. **VPN – Virtual Private Network**
2. **L2TP – Layer 2Tunnnelling Protocol**
3. **PPTP - Point to Point Tunnelling Protocol**
4. **SSL– Secure Socket Layer**
5. **IKE - Internet Key Exchange**
6. **IPsec - Internet Protocol Security**
7. **TLS - Transport Layer Security**
8. **SSL - Secure Sockets Layer**
9. **NAT - Network Address Translation**
10. **PSTN - Public Switched Telephone Network**

CHAPTER 1

1.1: INTRODUCTION

With the increasing need for remote access, mobile workforce, and cloud-based services, Champions Insurance Company has identified the need to implement a secure and reliable Virtual Private Network (VPN) solution to ensure the confidentiality, integrity, and availability of sensitive data transmitted over the open network. The direct connection allows anyone to view your connection and data. ISPs, governments, and cybercriminals have full access to your information given the right tools. A VPN makes sure this doesn't happen by acting as a middle-man between your device and the Internet. All the device's traffic goes through a secured server before connecting to the Internet, and this server is responsible for encrypting said traffic. Once your data becomes encrypted, it becomes unreadable for everyone else on the network. As long as your keep the VPN on, all of your device's traffic will be encrypted The project aims to provide a secure and efficient way to connect remote sites, branch offices, and mobile workers to the central network, while maintaining the security and integrity of the data.

According to a study by Cisco Systems, "The number of remote workers is expected to grow from 73% to 87% by 2030, and 75% of IT professionals believe that remote work is more productive than traditional office work". This trend highlights the need for secure and reliable remote access solutions that can ensure the security and integrity of sensitive data.

The VPN implementation will enable secure communication between devices and applications across the open network, using encryption and authentication protocols to ensure that only authorized personnel can access and transmit sensitive data. The VPN will also provide a secure and reliable connection to cloud-based services and applications, ensuring that data is transmitted securely and efficiently.

As noted by Forrester Research, "VPNs are critical components of enterprise security architectures, as they provide a secure and reliable way to connect remote sites, branch offices, and mobile workers to the central network" . The VPN implementation will be designed to meet the security and performance requirements of the Champions Insurance Company, ensuring that data is transmitted securely and efficiently.

In this project, we will implement a VPN solution that meets the security and performance requirements. The VPN solution will be designed to provide a secure and reliable connection between remote sites, branch offices, and mobile workers, while ensuring that data is transmitted securely and efficiently.

1.2: BACKGROUND OF THE STUDY

1. Champions Insurance Company is a growing insurance company that has been operating in Zimbabwe since 2003. It relies heavily on digital communication and data transfer. As the company expands its operations, the need for a secure and reliable VPN solution has become increasingly critical. Champions Insurance Company is a leading insurance provider in the industry, with a vast network of employees, agents, and customers across the country. They do not have any secure and reliable communications infrastructure that connects their offices across the country. To ensure the security and confidentiality of their data, Champions Insurance Company has decided to establish a secure Virtual Private network (VPN) over their open network infrastructure. Many businesses are now adopting to VPN so that their remote employees can connect to the office and connect to file servers email servers and other services without having to make them directly available over the internet.

1.3: PROBLEM STATEMENT

The organization is facing a critical challenge in ensuring the secure and reliable communication between remote sites, branch offices, and mobile workers to the central network. The current network architecture is not designed to provide secure and reliable communication, thus leaving sensitive data vulnerable to unauthorized access and data breaches.

The current security measures in place, such as firewalls and intrusion detection systems, are not sufficient to prevent unauthorized access and data breaches. The organization is experiencing frequent incidents of data breaches, unauthorized access, and downtime, which is causing significant financial losses and reputational damage.

The specific problems that need to be addressed are:

1. **Insecure Data Transmission**: The current network architecture does not provide secure communication between devices and applications, making it vulnerable to data breaches and unauthorized access.
2. **Lack of Authentication**: The organization lacks a robust authentication mechanism to ensure that only authorized personnel can access and transmit sensitive data.
3. **Inadequate Monitoring**: The current monitoring system is not sufficient to detect and respond to security threats in a timely manner.
4. **Insufficient Scalability**: The current network infrastructure is not designed to scale with the growing needs of the organization, making it difficult to provide secure and reliable communication.

1.4: PROJECT AIM

Designing a secure VPN (Virtual Private Network) for Champions Insurance Company would require considering several objectives to ensure the confidentiality, integrity, and availability of sensitive data. The objectives of the project are as follows:

- Design a secure VPN architecture that can provide a high level of security, throughput, and latency for remote offices, agents, and employees.
- Ensure that all data transmitted between Champions Insurance Company's employees, agents, and customers is protected from unauthorized access. This includes encrypting data in transit and at rest.
- Secure Connectivity: Establish a secure connection between the VPN server and the clients (e.g., employees' devices) using protocols such as SSL/TLS, IPsec, or OpenVPN
- Simulate the designed VPN architecture using a network simulator to evaluate its performance and security.
- Conduct a thorough analysis of the simulation results to identify potential issues and vulnerabilities.
- Develop a plan for implementing the designed VPN architecture in a real-world environment.

1.5: RESEARCH OBJECTIVES

The VPN solution will be designed to:

- Provide secure communication between devices and applications using encryption and authentication protocols.
- Ensure that only authorized personnel can access and transmit sensitive data.
- Monitor and detect security threats in real-time.
- Scale with the growing needs of the organization.

1.6: RESEARCH QUESTIONS

1. What are the tools to be used by the author on designing an algorithm?
2. What are the most effective encryption protocols and algorithms to use in a VPN implementation to ensure secure data transmission?

3. What are the most effective measures to prevent unauthorized access and data breaches in a VPN implementation?
4. What is the impact of implementing a VPN on network performance and user experience?

1.7: JUSTIFICATION

The implementation of a Virtual Private Network (VPN) is a critical project that aims to provide a secure and reliable way to connect remote sites, branch offices, and mobile workers to the central network. The VPN solution will be designed to ensure the confidentiality, integrity, and availability of sensitive data, while also providing a secure and reliable communication channel.

The research justification for this project is based on the following key findings:

Growing Demand for Remote Access: The increasing use of remote access, mobile workforce, and cloud-based services has created a growing demand for secure and reliable communication between devices and applications. A VPN solution will provide a secure and reliable way to connect remote sites, branch offices, and mobile workers to the central network.

Inadequate Security Measures: The current security measures in place, such as firewalls and intrusion detection systems, are not sufficient to prevent unauthorized access and data breaches. A VPN solution will provide an additional layer of security to ensure the confidentiality, integrity, and availability of sensitive data.

Cost Savings: The implementation of a VPN solution will provide cost savings by reducing the need for additional infrastructure, such as dedicated lines or leased lines. A VPN solution will also reduce the need for manual configuration and troubleshooting of remote access connections.

Improved Productivity: A VPN solution will provide employees with secure and reliable access to company resources and applications, allowing them to work more efficiently and effectively. This will improve productivity and reduce the time spent on troubleshooting and configuration.

1.8: Project Limitations

Despite the extensive research and analysis conducted for this project, there are several limitations that should be considered when interpreting the results:

1. **Scalability Limitations**: The VPN solution implemented may not be scalable to accommodate the growing needs of the organization. As the organization expands, the VPN solution may need to be upgraded or replaced to ensure continued performance and security.

2. **Compatibility Issues**: The VPN solution may not be compatible with all devices and operating systems, which could limit its adoption and usage. Future research could focus on developing a more comprehensive compatibility framework.
3. **Security Threats**: The VPN solution may not be able to detect and prevent all types of security threats, such as advanced persistent threats (APTs) and zero-day attacks. Further research is needed to develop more effective security protocols and threat detection mechanisms.
4. **Cost and Resource Constraints**: The implementation of a VPN solution may require significant financial resources and technical expertise, which could be a barrier to adoption for some organizations.
5. **Lack of Standardization**: There is currently a lack of standardization in the VPN industry, which can make it difficult to compare and evaluate different solutions. Future research could focus on developing standards and best practices for VPN implementation.
6. Limited Testing: The testing process for this project is limited, which may not have identified all potential issues or limitations. Future research could focus on conducting more comprehensive testing to identify potential issues earlier.

1.9: Research Hypothesis

The implementation of a Virtual Private Network (VPN) solution will significantly improve the security and reliability of communication between remote sites, branch offices, and mobile workers to the central network, thereby reducing the risk of data breaches and unauthorized access.

Specifically, the research hypothesis is:

1. H1: The VPN solution will reduce the risk of data breaches by at least 80% compared to the current network architecture.
2. H2: The VPN solution will improve the authentication mechanism by at least 90% compared to the current system, ensuring that only authorized personnel can access and transmit sensitive data.
3. H3: The VPN solution will reduce the average downtime by at least 60% compared to the current network infrastructure, resulting in improved business operations and reduced financial losses.
4. H4: The VPN solution will improve the scalability of the network infrastructure by at least 75% compared to the current system, allowing for increased growth and flexibility.

The research hypothesis is based on the following assumptions:

1. The current network architecture is vulnerable to data breaches and unauthorized access.

2. The implementation of a VPN solution will provide secure communication between devices and applications.
3. The VPN solution will improve the authentication mechanism and reduce the risk of data breaches.
4. The VPN solution will reduce downtime and improve business operations.
5. The VPN solution will improve the scalability of the network infrastructure.

The research hypothesis will be tested through a series of experiments and data analysis, including:

1. Security testing: Testing the VPN solution for vulnerabilities and weaknesses.
2. Performance testing: Testing the VPN solution for performance and scalability.
3. User testing: Testing the VPN solution with real users to evaluate usability and user experience.
4. Data analysis: Analysing data from before and after the implementation of the VPN solution to evaluate its effectiveness.

1.10: CHAPTER SUMMARY

In conclusion, this research has aimed to address critical challenges of security and connectivity faced by the organization. The project is aiming to provide a secure and reliable way to connect remote sites, branch offices, and mobile workers to the central network.

The VPN solution is to provide a robust and secure communication infrastructure, enabling the organization to transmit sensitive data securely and reliably. The implementation of the VPN solution has also ensured that only authorized personnel can access and transmit sensitive data, thereby reducing the risk of data breaches and unauthorized access.

CHAPTER 2: LITERATURE REVIEW

2.1: Introduction

Virtual – refers to something that is not physically real or existing but is made to appear so through computer software of technology.

Private – refers to something that is restricted to the use of a particular person or group rather than being available for public access or view. Although the communication between any two parties in a VPN is over a public network, there is no third party who can interrupt this communication.

Network– A group of computers, servers, mainframes, network devices, and other equipment that are linked together to share resources and data is referred to as a network.

According to Black and Smith, (2020), a virtual private network, or VPN, is a network that uses public network paths while preserving private network security and protection. In order to virtually extend a private network, that is, any computer network that is not the public Internet—across one or more other networks that are either untrusted (because they are not under the control of the organization attempting to implement the VPN) or require isolation (making the lower network invisible or not directly usable), a virtual private network, or VPN, is a network architecture.

Black and Smith, (2020); stated that the term "VPN" was used to refer to distant connectivity services like the PSTN (Public Switched Telephone Network). However, in recent years, VPN networks have begun to be associated with IP-based data networking. Businesses had invested a significant amount of effort and money in creating intricate private networks, now known as intranets, prior to IP-based networking. Frame relay, expensive leased line services, and ATMs were used to establish these networks in order to accommodate distant users. Businesses added remote access servers, or ISDN, to their networks to support smaller locations and remote workers. Low-speed switched services were utilized by small and medium-sized businesses that could not afford dedicated leased lines.

As the Internet became more and more accessible and bandwidth capacities grew, companies began to put their Intranets onto the web and create what are now known as Extranets to link internal and external users. However, as cost-effective and quick-to-deploy as the Internet is, there is one fundamental problem which is security. Today's VPN solutions overcome the security factor using special Tunnelling protocols and complex encryption procedures, data

integrity and privacy is achieved, and the new connection produces what seems to be a dedicated point-to point connection. And, because these operations occur over a public network, VPNs can cost significantly less to implement than privately owned or leased services.

Although early VPNs required extensive expertise to implement, technology has matured to a level where deployment can be a simple and affordable solution for businesses of all sizes.

VPN Defined

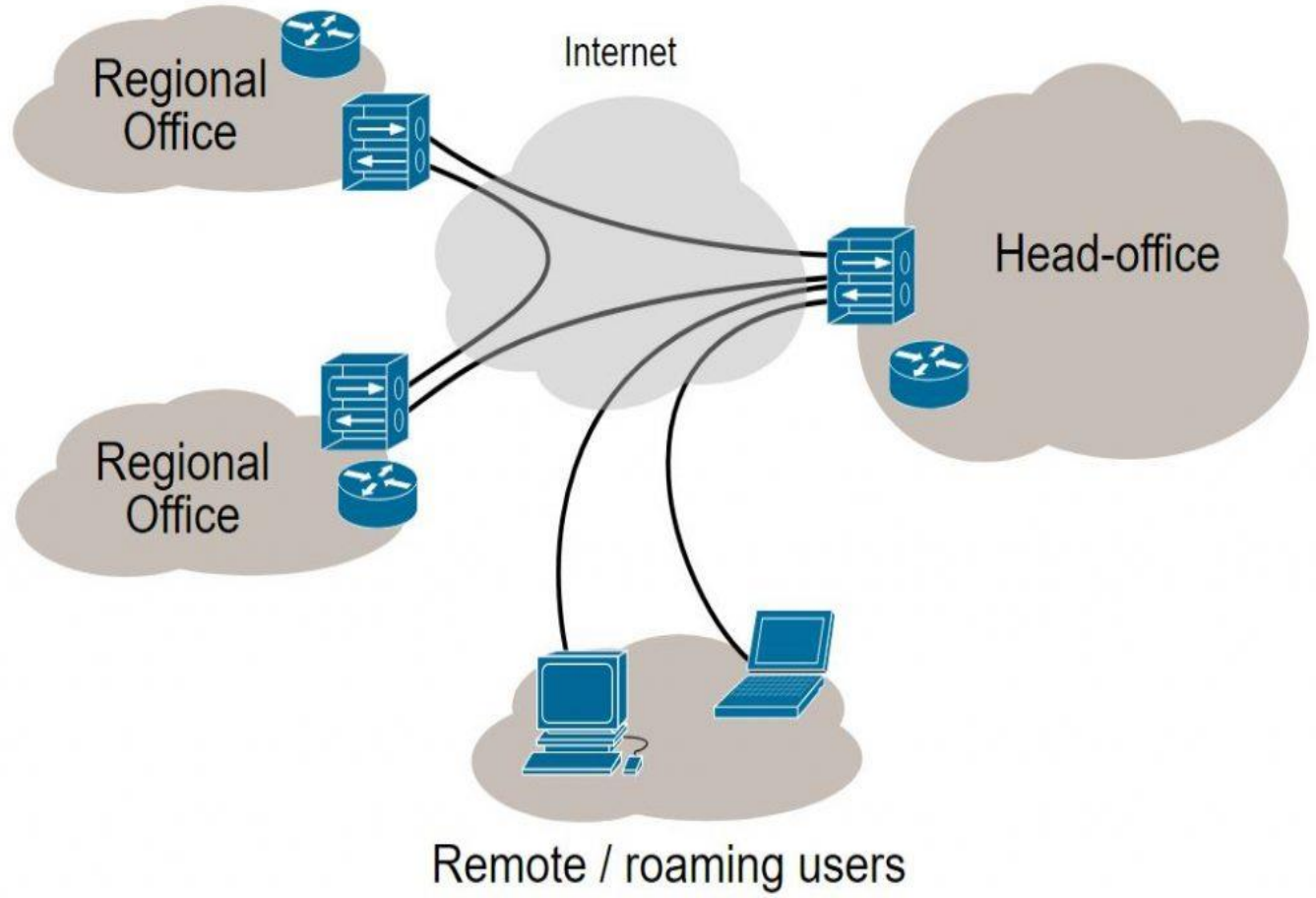


Figure 2.1: Defined VPN

2.1.1: How a VPN works

The IP datagrams containing encapsulated PPP packets are sent. In normal connections, the company's firewall does not allow PPP packets from entering the network; thus, internet users are not able to access a private network. However, VPN services allow users who meet security criteria are admitted. The VPN server disassembles the packet and transfers the packet to the destination computer located in the private network.

When making a VPN connection, there are two connections. The first connection is made to the Internet Service Provider. In connecting to the service provider, TCP/IP (Transmission Control Protocol/Internet Protocol) and PPP (Point-to-Point Protocol) are used to communicate to the ISP. The remote user is assigned an IP address by the ISP. The user logs into the company login. This second connection establishes the VPN connection and a tunnel are created with the use of Point-to-Point Tunnelling Protocol (PPTP) for example, after the user is authorized.

Take notice of the following diagram. It represents one type of implementation of a VPN – a Remote Access VPN.

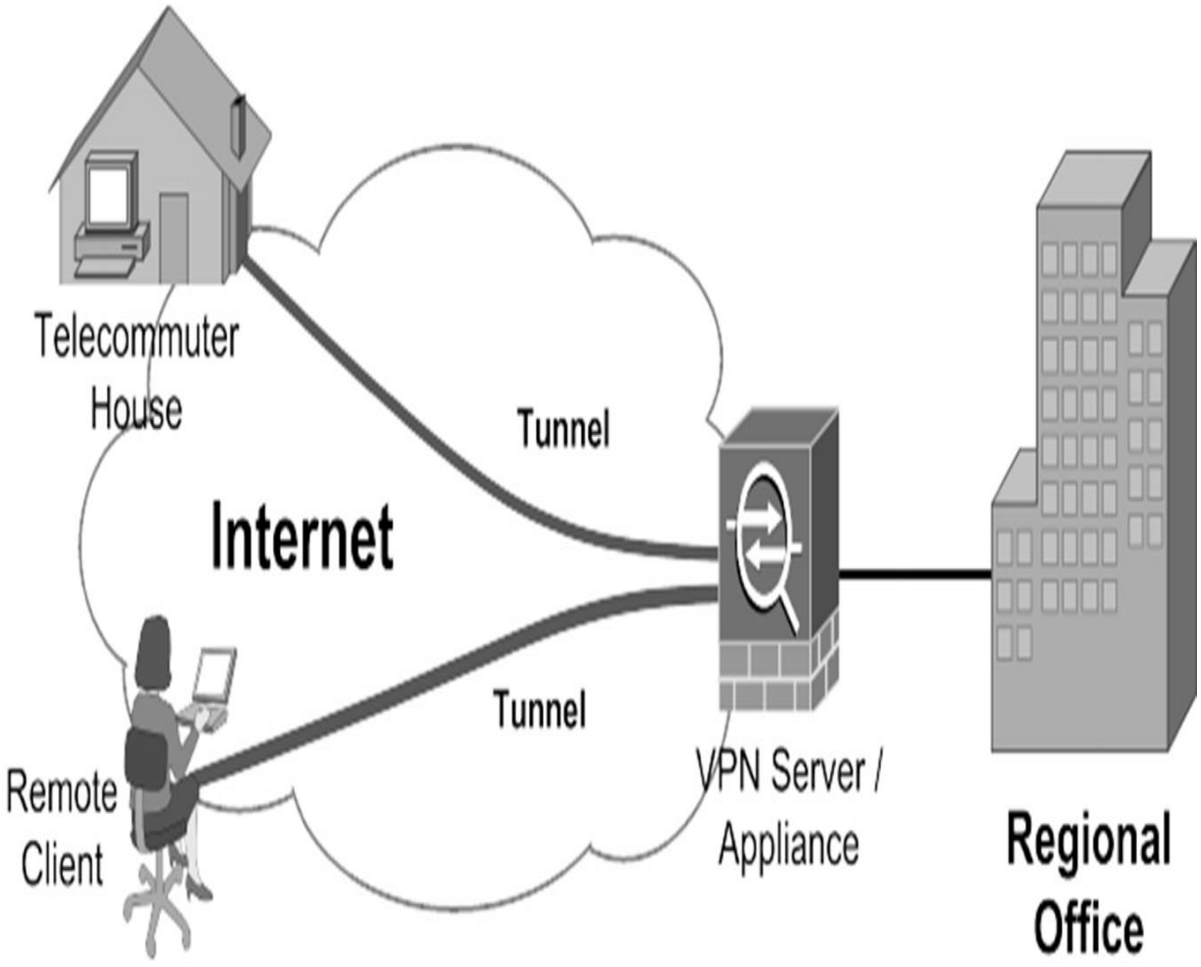


Figure 2.2 Remote Access VPN

2.2.: Types of VPN

VPNs can be categorized as follows:

- Site-to-site VPN
- IPsec Remote access VPN

- Clientless SSL VPNs

2.2.1: Site-to-site VPN

Site-to-Site VPN refers to implementations in which the network of one location is connected to the network of another location via a VPN.

A site-to-site virtual private network (VPN) refers to a connection set up between multiple networks. This could be a corporate network where multiple offices work in conjunction with each other or a branch office network with a central office and multiple branch locations.

Site-to-site VPNs are useful for companies that prioritize private, protected traffic and are particularly helpful for organizations with more than one office spread out over large geographical locations. These businesses often have to access resources housed on a primary network, which could include servers that facilitate email or store data. In some instances, a server may be the operational hub of an application essential to the company's business. A site-to-site VPN can, in that case, give all sites full access to the application—as if it were housed within their physical facility.

Frame Relay, Asynchronous Transfer Mode (ATM) and Multiprotocol label Switching (MPLS) VPNs are examples of site-to-site VPNs.

There are two types of site-to site VPNs:

- **Intranet-based:**
  Allows a company to establish a secure connection with its remote locations. An intranet-based site-to-site VPN connects more than one local-area network (LAN) to form a wide-area network (WAN). A company may also use this kind of setup to incorporate software-defined WAN (SD-WAN). Intranet-based site-to-site VPNs are useful tools for combining resources housed in disparate offices securely, as if they were all in the same physical location.

  An intranet-based site-to-site VPN is particularly helpful if each site either develops its own resources or houses unique processes that the entire company would benefit from having access to. For example, if each office had design schematics that were constantly being updated and adjusted for clients, an intranet-based site-to-site VPN would give decision-makers in a number of offices secure access to everything produced—regardless of their physical location.
- **Extranet-based**
  Allows two companies to work together via a secure connection while preventing access to their separate intranets. Extranet-based site-to-site VPNs are often used by two or more different companies that want to share certain resources but keep others private. With an extranet-based site-to-site VPN, each entity connects to the VPN and chooses what they want to make available to the other companies. In this way, they can collaborate and share without exposing proprietary data.

The lack of VPN client software on hosts is one of the characteristics of site-to-site VPNs. Rather, they merely use a VPN gateway to send and receive standard TCP/IP data. The VPN gateway is in charge of encapsulating and encrypting outgoing traffic. This indicates that

peer-to-peer communication over the Internet is possible using a VPN tunnel. When the packet is received, the peer VPN gateway decrypts the content, removes the headers, and then forwards it to the target host within its private network. In essence, the site-to-site VPN expands the business's network, facilitating communication. A business that has branches in multiple isolated places can serve as an excellent example in this case.

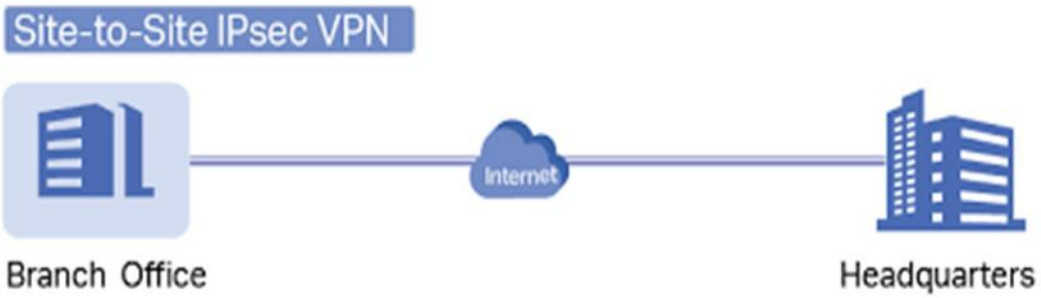


Figure 2.3: Site-to-site VPN Tunnel: simple graphical depiction of a site-to-site VPN tunnel

2.2.2; IPsec Remote Access VPN

A remote access VPN refers to a temporary connection set up between two or more users and a central location. In most cases, a remote access VPN is used to give each location access to a data center. In some situations, a connection that makes use of Internet Protocol security (IPsec) is sufficient. However, it is also common for an organization to utilize a VPN, which avails them of the security positioned at the gateways at each end of the VPN.

For businesses with remote employees who work from home or on the go, a virtual private network (VPN) is a helpful tool. These employees can connect to a remote access VPN if they need to access sensitive or confidential data stored on the company's servers. Each worker can obtain the tools they require to perform their duties in this manner.

With this kind of VPN, employees who operate in different places can have an experience that is comparable to that of employees in the main office who can use an Ethernet cable to connect to the server at their workstations. In a way, the remote access VPN connects a cable directly into each employee's workstation, which includes PCs, laptops, and mobile devices, spanning many kilometers and even international boundaries.

Despite having additional network options, IPsec is frequently contrasted to SSL/TLS as being more complex and requiring more administrative labor. The requirement that the VPN client software be installed on the distant user's computer with administrative rights is another disadvantage of the IPsec distant Access VPN technique, which can impede scalability in large-scale installations.

Navigating via firewalls and NAT devices that are positioned between the client and the gateway can present another difficulty for IPsec VPNs. Matei (2012) Fortunately, there are programs like NAT Traversal that can assist in overcoming these obstacles. We decided to use Cisco's version of this option for this project, which is known as Easy VPN Server.

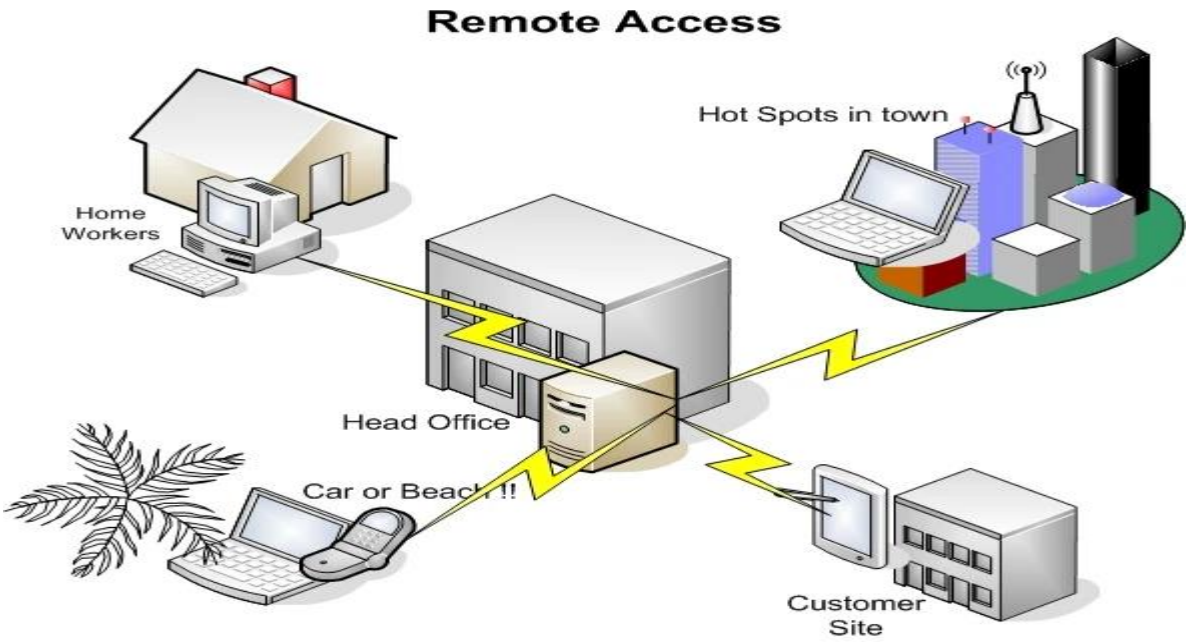


Figure2.4 Remote Access VPN

2.2.3: Clientless Secure Socket Layer (SSL)

The Clientless Secure Sockets Layer (SSL) VPN is by far the most straightforward type of VPN to set up from the standpoint of the end user. End users can use an SSL-enabled Web browser to safely access corporate network resources from any location using a clientless SSL VPN. The user can access pre-configured network resources after initially authenticating with a Clientless SSL VPN gateway. A remote user can use their web browser to access web services operating in their home office LAN once they have launched their browser and successfully authenticated against a Cisco IOS SSL VPN Gateway (or another SSL VPN gateway). A clientless SSL VPN connection can be used to access remote services such as "web servers, shared file directories, web based email systems, shared file directories, web based email systems, applications that run on protected servers and any other services that can be channeled through a web page."

It is crucial to remember that, in general, a clientless SSL VPN cannot be regarded as a comprehensive substitute for an IPsec client VPN or site-to-site VPN. This is because web browser-incompatible applications like Telnet, SNMP, ping, traceroute, FTP, and IP telephony are generally not supported by clientless SSL VPNs. Using a web browser to construct an SSL Tunnel VPN is one way to solve this issue. We'll talk about these choices in a later section.

2.3: VPN Tunnelling

Data transport over the internet is protected by a VPN tunnel, which is a safe, encrypted connection between a network device and a VPN server.

By establishing a private channel, the VPN tunnel protects data being sent from illegal access and interception. During transmission, encryption algorithms transform data into unintelligible code, guaranteeing that even in the event of data interception, it will remain secure and unreadable.

The process of creating a secure, encrypted connection via a network—usually the internet is known as VPN tunneling. This connection is known as a "tunnel" because it offers a secure channel for data transfer between a VPN server and a device.

VPN Tunnelling encrypts a user's data and hides their IP address. This provides security, particularly when utilizing unprotected public Wi-Fi. You can think of the encryption process as being like mailing a sealed envelope. The contents of the envelope are confidential unless someone opens it, even if postal workers see or handle it. VPN Tunnelling includes safeguards such as a kill switch, which halts internet traffic if the VPN connection drops. This prevents the user's public IP address from becoming visible, which maintains the integrity of the secure tunnel.

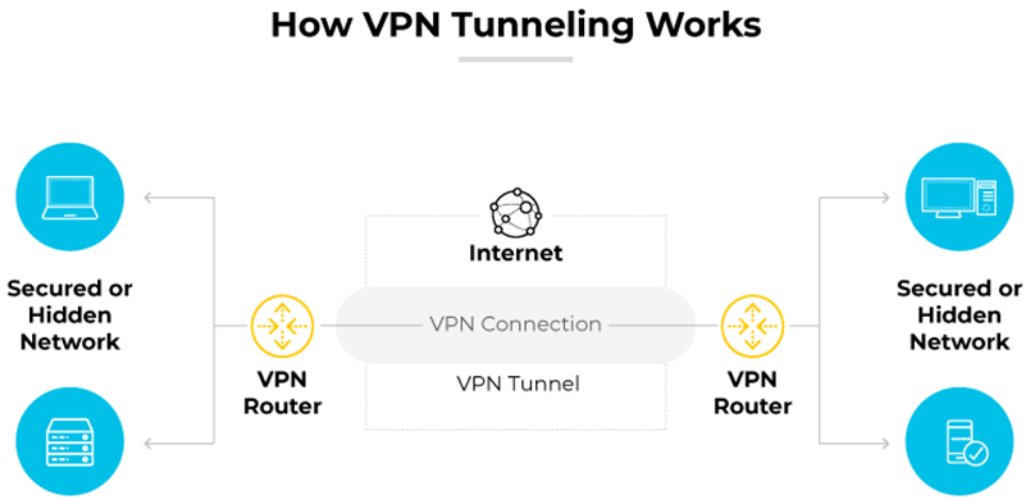


Figure 2.5 VPN Tunneling

To guarantee security and privacy, the Tunnelling procedure consists of the following steps:

1. Establishing a VPN connection

A VPN service must be chosen, and the user's device must be connected to the selected VPN server.

2. The creation of a tunnel with encryption

An encrypted channel is created by the VPN app on the user's device. As the internet traffic travels from the user's internet connection to the VPN server, this encryption protects it from unwanted access.

3. Data encryption

A particular protocol is used to encrypt the data being sent across the tunnel, converting it into a coded format called "ciphertext." Without the right decryption keys, this encrypted data cannot be decoded.

4. At the VPN server, decryption

After receiving the encrypted data, the VPN server employs keys to decrypt it. Once decrypted, the data can continue to its intended destination on the internet.

5. Return of data to the user's device

Data sent from the internet back to the user also passes through the encrypted tunnel, ensuring privacy and security in both directions.

2.4: VPN Protocols

A VPN protocol is a set of rules that decides how your online traffic gets from your device, through the VPN server, and to the web.

Without a VPN, all of your internet traffic only moves between your device and the internet. It complies with a set of guidelines known as the Internet Protocol, or IP, to accomplish that. Just as you and your typical commute to work are familiar with the protocol, so is every gadget connected to the internet. A navigation app is not required; you are already familiar with it.

Your communication is redirected via a safe, encrypted tunnel before it reaches the internet when you connect to a virtual private network (VPN). A VPN protocol is the set of rules that are required for it. When a VPN directs you to a safer alternate route, your device needs the VPN to provide it navigation instructions because it is unfamiliar with it.

VPN protocols provide more than just directions, however. Just like different routes have varying distances, traffic conditions, and road safety, your choice of a VPN protocol determines the speed and level of security you experience with your VPN connection. It influences crucial aspects, such as the VPN encryption standard employed, the routing of various types of traffic through specific ports, and the overall reliability of your connection

2.4.1: Types of VPN Protocols

OpenVPN

OpenVPN is an open-source VPN released in 20011 that has continually improved since. Now the gold standard of VPN protocols, it's compatible with cutting-edge encryption standards and provides fast and reliable speeds. It is an open-source system that creates a private and secure tunnel between networks. It refers to multiple different but related things. OpenVPN creates a secure tunnel for data traffic to pass between the VPN client and server. This process includes authentication of the VPN client and server, creation of a VPN tunnel, data encapsulation and encryption, and data traffic transmission. It works with different authentication methods and encryption algorithms and can secure both TCP and UDP traffic. All the customization makes it a preferred and secure choice for many VPN setups.

How secure is the OpenVPN

OpenVPN is one of the safest VPN protocols. It uses SSL/TLS to ensure data security and has access to the OpenSSL library for further customization, including additional security features. The OpenVPN protocol includes perfect forward secrecy, ensuring that even in the case of a data breach, not all data would be compromised. And it's possible to use OpenVPN with both TCP and UDP protocols, so you can switch to TCP when you prioritize security (and UDP when you need fast speeds).

Layer 2 Transfer Protocol (L2TP)

Like IKEv2, L2TP is frequently used in conjunction with IPSec. It was created by Microsoft and Cisco in the 1990s, and at the time, it was thought to be secure. Although there are currently no known weaknesses, many individuals think that government eavesdropping, particularly by the NSA, is now a possibility.
Internet service providers (ISPs) employ Layer Two Tunnelling Protocol (L2TP), an extension of Point-to-Point Tunnelling Protocol (PPTP), to enable virtual private networks (VPNs). L2TP needs to use an encryption protocol in order to function inside the tunnel and maintain security and privacy.

Since L2TP cannot encrypt data on its own, it is frequently used in conjunction with IPsec. The confidentiality, integrity and authentication of the data packets sent over the VPN tunnel are guaranteed by the combination of L2TP and IPsec. L2TP/IPsec is a popular combination because of its improved security features.

How it works

The way L2TP operates is by enclosing data packets in a network tunnel. The protocol depends on IPsec to ensure the confidentiality, integrity and authentication of the data packets moving over the tunnel because it does not by default encrypt data. The L2TP network server (LNS) and the L2TP Access Concentrator (LAC) are the two main parts of an L2TP implementation. The LAC operates ate the tunnel starting point where it takes client connections. As LNS which is placed at the network's endpoint, is used to start the tunnel. By serving as a bridge, the LNS links the destination network or resources to the secure tunnel. L2TP gives IP addresses from the internet service providers (ISPs) to the L2TP Network Server (LNS) and the LAC when PPP sessions are being established. For control packets to be encapsulated and transmitted via the secure tunnel, this assignment is essential.

For a VPN connections to be secure Layer 2 Transfer Protocol and Internet Protocol Security must be integrated. Data packets sent across the L2TP tunnel are encrypted and secure thanks

to internet protocol security. To create mutual authentication and a secure connection between client and server, it makes use of advanced encryption techniques like 256bit AES and protocols like the Internet Key Exchange (IKE).

How secure is the L2TP

The main functions of Layer 2 Tunnelling Protocol is to establish a tunnel through which data can safely travel, as it does not provide encryption on its own. IPsec is the only method that can guarantee the security of the data in this tunnel. Through the creation of a tunnel and subsequent encryption of the data the combination offers a secondary layer of safety.
The L2TP encapsulate data and enables private data transfer over the internet. In order to secure user to network connections. IPsec employees cryptographic security services to apply strong encryption to this wrapped data. For enterprise networks that transport sensitive data, this compromise data integrity, confidentiality and authentication of origin.

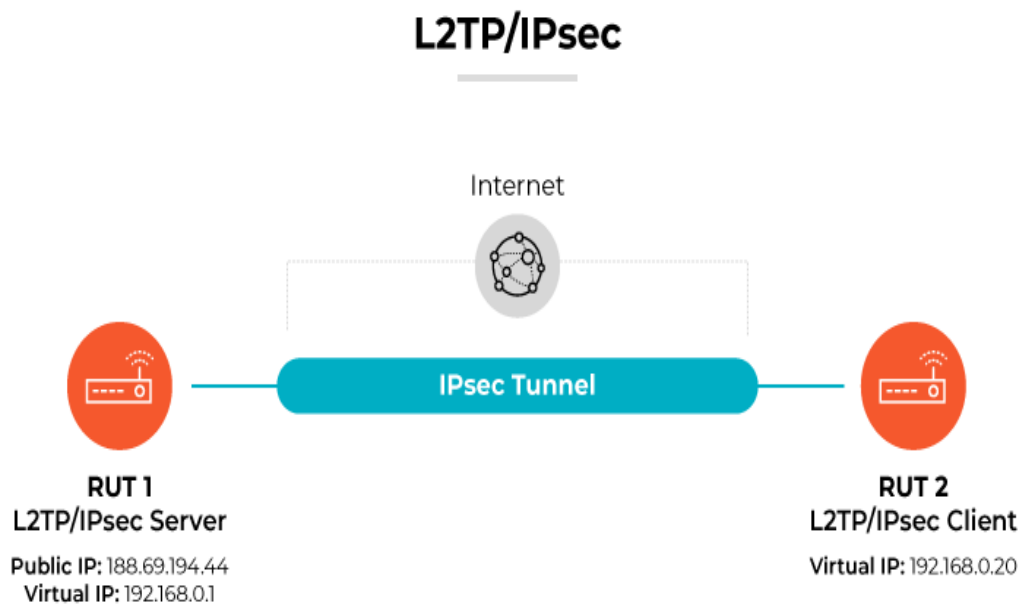


Figure2.6: Layer 2 Transfer Protocol (L2TP)

By creating secure keys during the session and offering robust AES or 3DES encryption to prevent unwanted interceptions Internet Protocol Security collaborations with Layer 2 Transfer Protocol. The encryption and secure data transit that an L2TP/IPsec VPN provides are its main advantages. L2TP/IPsec VPN security protocols additionally protect control packet integrity, guaranteeing that PPP sessions are private and unchanged while in transit.

Point-to-Point Protocol (PPTP)

The first networking protocol for building a VPN was the Point to Point Tunnelling Protocol. At a glance, the PPTP protocol provides all the features found in the majority of VPN protocols. Such as data encryption, VPN tunnel creation, and authentication. But even while the PPTPVPN protocol was popular in the 1990s, it is not up to par with contemporary VPN technology. Because of its serious security flaws, it is susceptible to some kinds of attacks (for example bit flipping attacking where the attacker can change the cipher text in such a way that it results in a change of the plaintext, although the attacker is not able to learn the plain text itself.). let's examine its operation to get a better understanding of the security flaws.

How the PPTP works?

Most notably, PPTP establishes a tunnel between two sites, just like all other tunnelling protocols. All data packets send through the PPTP connections are first wrapped in an IP envelope before being sent to a different router or computer which will handle the data as though it were an IP packet, after that it can be decrypted and made available to the person who requested it.

Data packets and control messages are the two forms of data flow that PPTP is capable of managing. The purpose of the control messages is to decide when the encrypted connection commences and ends. Every VPN protocol that has been developed has enhanced and expanded upon this straightforward procedure.

2.5: VPN Split Tunnelling

VPN split Tunnelling is a feature that allows a user to route some internet traffic through a secure VPN, while other traffic accesses the internet directly, bypassing the VPN. This method permits the division of network traffic into two streams. One stream is encrypted and routed through a VPN tunnel, and the other connects to the internet. This is particularly useful when simultaneous access to resources in both private and public networks is required.

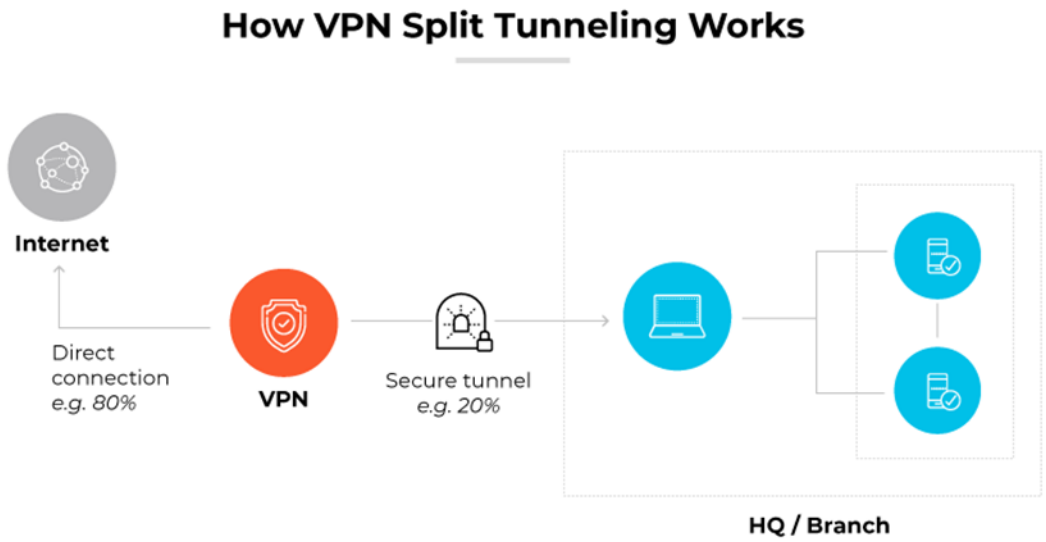


Figure 2.6: VPN split tunnelling

The advantage of split tunnelling is its efficiency. By only directing necessary traffic through the VPN, it can conserve bandwidth and improve speed for the activities that do not require encryption. For instance, an employee could access their company's internal documents through the VPN while streaming music directly via their local internet connection, which does not require VPN security.

However, there are potential risks. The traffic that does not use the VPN is unencrypted, making it potentially vulnerable to threats like data interception. While split Tunnelling can optimize network performance, it must be implemented judiciously to maintain security where it is most needed. This function is contingent on the VPN service provider's support and may vary across different devices and operating systems.

2.6: IPsec VPN fundamentals

IPsec is an IETF standard that acts as a modular framework of open standards that define how a VPN connection is implemented.

The three main security solutions IPsec offers are data integrity, data authentication, and data confidentiality.

Data integrity is accomplished through the use of HMAC, a standard that uses a hash algorithm to create a hash value that is sent along with the packet. Upon receipt, the hash algorithm is run again and compared to the received hash value. The hash values must be identical for the packet to be accepted. The two hash algorithms available to use in IPsec are MD5 and SHA-1.

Data authentication is achieved through pre-shared keys, RSA signatures (digital signatures), or RSA encrypted nonce.

Data confidentiality is attained by encrypting the data. Common encryption algorithms that are available in IPsec are DES, 3DES, AES, and SEAL Triggering the VPN Connection.

There are two ways that an IPsec VPN connection can be set into motion. In a site-to- site connection, “interesting traffic” is identified through the use of an ACL. Any traffic that is permitted by the ACL triggers the IKE process.

In a remote client connection, the user initiates the connection manually by clicking on the connection profile in the software client. Internet Key Exchange (IKE) IKE is used by IPsec to negotiate and establish multiple Security Associations (SA)

2.7: IPSec VPN Negotiations

The devices at either end of an IPSec VPN tunnel are IPSec peers. To build the VPN tunnel, IPSec peers exchange a series of messages about encryption and authentication, and attempt to agree on many different parameters. This process is known as VPN negotiations. One device in the negotiation sequence is the initiator and the other device is the responder.

VPN negotiations happen in two distinct phases: *Phase 1* and *Phase 2*.

Phase 1

The main purpose of Phase 1 is to set up a secure encrypted channel through which the two peers can negotiate Phase 2. When Phase 1 finishes successfully, the peers quickly move on to Phase 2 negotiations. If Phase 1 fails, the devices cannot begin Phase 2.

Phase 2

The purpose of Phase 2 negotiations is for the two peers to agree on a set of parameters that define what traffic can go through the VPN, and how to encrypt and authenticate the traffic. This agreement is called a Security Association.

The Phase 1 and Phase 2 configurations must match for the devices on either end of the tunnel.

Phase 1 Negotiations

In Phase 1 negotiations, the two VPN gateway devices exchange credentials. The devices identify each other and negotiate to find a common set of Phase 1 settings to use. When Phase 1 negotiations are completed, the two devices have a Phase 1 Security Association (SA). This SA is valid for a specified amount of time. If the two VPN gateways do not complete Phase 2 negotiations before the Phase 1 SA expires, then they must complete Phase 1 negotiations again.

The Phase 1 negotiation process depends on which version of IKE the gateway endpoints use. IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure communications channel for negotiating IPSec SAs in Phase 2.

Phase 1 negotiations include these steps:

1. The devices agree on the IKE version to use (IKEv1 or IKEv2). Each device can use IKEv1 or IKEv2. The IKE version for both devices must match.

2. The devices exchange credentials.

The credentials can be a certificate or a pre-shared key. Both gateway endpoints must use the same credential method, and the credentials must match.

3. The devices identify each other.

Each device provides a Phase 1 identifier, which can be an IP address, domain name, domain information, or an X500 name. The VPN configuration on each device specifies the Phase 1 identifier of the local and the remote device. The configurations must match.

4. For IKEv1, the VPN gateways decide whether to use Main Mode or Aggressive Mode for Phase 1 negotiations.

The VPN gateway that starts the IKE negotiations sends either a Main Mode proposal or an Aggressive Mode proposal. The other VPN gateway can reject the proposal if it is not configured to use that mode.

- Main Mode ensures the identity of both VPN gateways, but can be used only if both devices have a static IP address. Main Mode validates the IP address and gateway ID.
- Aggressive Mode is faster but less secure than Main Mode because it requires fewer exchanges between two VPN gateways. In Aggressive Mode, the exchange relies mainly on the ID types used in the exchange by both VPN gateways. Aggressive Mode does not ensure the identity of the VPN gateway. The IKEv1 Aggressive Mode vulnerability described in CVE-2002-1623 means that Aggressive Mode is less secure than Main Mode unless you configure a certificate.

5. The VPN gateways agree on Phase 1 parameters.

- Whether to use NAT traversal
- Whether to use IKE Keep-Alive (between Fireboxes only)
- Whether to use Dead Peer Detection (RFC 3706)

IKE Keep-Alive is an obsolete setting. We recommend DPD instead.

For IKEv2, NAT Traversal and DPD are always enabled, and IKE Keep-Alive is not supported.

6. The VPN gateways agree on Phase 1 Transform settings. The settings in the Phase 1 transform on each IPSec device must exactly match, or IKE negotiations fail.

The items you can set in the Phase 1 transform are:

- **Authentication** — The type of authentication (SHA-2, SHA-1, or MD5)
- **Encryption** — The type of encryption algorithm (DES, 3DES, or AES) and key length
- **SA Life** — The amount of time until the Phase 1 Security Association expires

- **Key Group** — The Diffie-Hellman key group

Phase 2 Negotiations

After the two IPSec VPN gateways successfully complete Phase 1 negotiations, Phase 2 negotiations begin. The purpose of Phase 2 negotiations is to establish the Phase 2 SA (sometimes called the IPSec SA). The IPSec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic.

Phase 2 negotiations include these steps:

1. The VPN gateways use the Phase 1 SA to secure Phase 2 negotiations. The VPN gateways agree on whether to use Perfect Forward Secrecy (PFS).

VPN encryption keys are changed at the interval specified by the **Force Key Expiration** setting. The interval is eight hours by default. To prevent SAs from using Phase 1 keys for Phase 2, PFS forces the DH calculation to happen a second time. This means that Phase 1 and Phase 2 always have different keys, which is harder to break unless you select a DH group lower than 14.
We recommend that you use PFS to keep your data secure. If you want to use PFS, it must be enabled on both VPN gateways, and both gateways must use the same Diffie-Hellman key groups.

2. The VPN gateways agree on a Phase 2 proposal.

The Phase 2 proposal includes the algorithm to use to authenticate data, the algorithm to use to encrypt data, and how often to make new Phase 2 encryption keys.

The items you can set in a Phase 2 proposal include:

- **Type** — For a manual BOVPN, you can select the type of protocol to use: Authentication Header (AH) or Encapsulating Security Payload (ESP). Both AH and ESP encrypt the data and protect against spoofing and packet manipulation (replay detection). We recommend that you use ESP, because you can protect against spoofing in other ways. Managed BOVPNs, Mobile VPN with IKEv2, Mobile VPN with IPSec, and Mobile VPN with L2TP always use ESP.

The IPSec authentication process checks the sequence of encrypted packets to prevent replay attacks. The anti-replay window size for VPN connections is fixed to 32 packets and cannot be modified.

- **Authentication** — Authentication makes sure that the information received is exactly the same as the information sent. You can use SHA-1, SHA-2, or MD5 as the algorithm the VPN gateways use to authenticate IKE messages from each other. SHA-2 is the only secure option.
- **Encryption** — Encryption keeps the data confidential. You can select DES, 3DES, or AES, or AES-GCM. AES and AES-GCM variants are the only secure options.
- **Force Key Expiration** — To make sure Phase 2 encryption keys change periodically, specify a key expiration interval. The default setting is 8 hours. The longer a Phase 2 encryption key is in use, the more data an attacker can collect to use to mount an attack on the key. We recommend that you do not select the **Traffic** option because it causes high Firebox load, throughput issues, packet loss, and frequent, random outages. The **Traffic** option does not work with most third-party devices

A high level visual representation of the IPsec process is shown in the following figure.

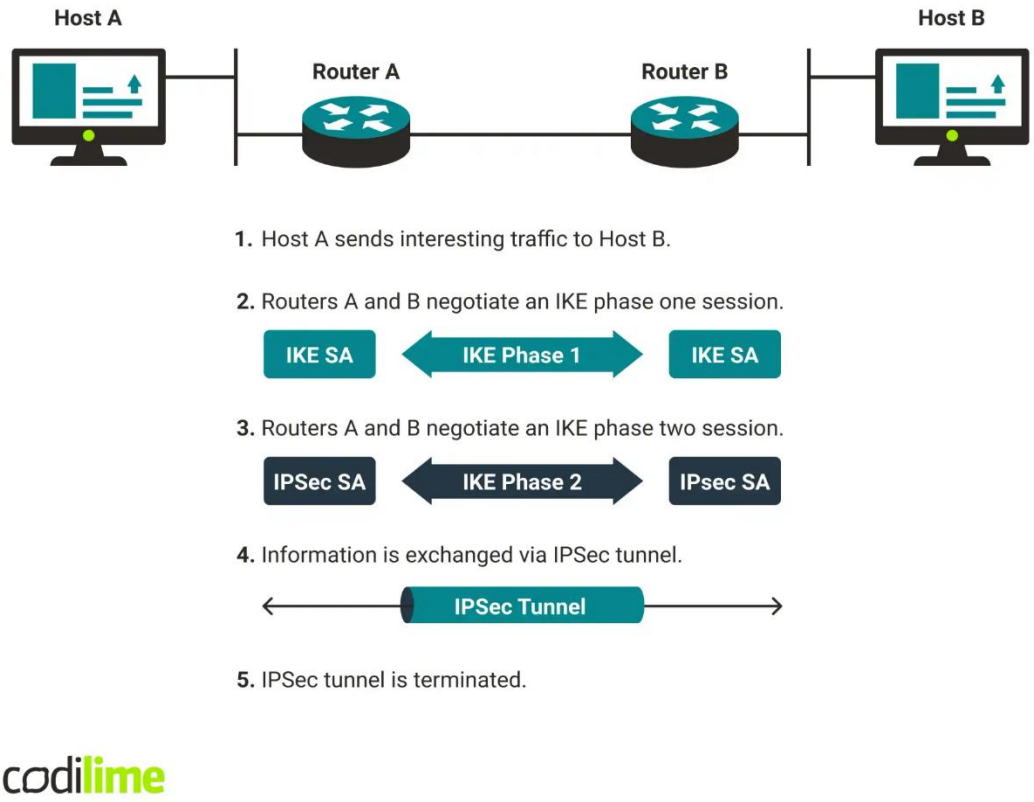


Figure 2.7 IPsec Negotiation process

2.8: IPsec protocols

IPsec is a collection of protocols that provide encryption, authentication and key management system for ensuring the VPN peers privacy, authenticity and integrity of data as the information crosses the unsecure network. IKE and IPsec are the two building blocks for the formation of the IPsec tunnel. IKE is responsible for determining identities and secrets. The IPsec tunnel is used to transport data securely via a tunnel. There are two IPsec framework protocols AH and ESP.

Authentication Header (AH)

It operates on top of IP using protocol . It is implemented in VPN communication, when confidentiality is not a major concern. In VPN communication peers AH provides the IP packets with data integrity and authentication services. It is a mechanism of verifying whether the data in transit is misused or not. It does not offer an encryption mechanism, but

all the packets are transported in clear text which is not secure. AH provides the following services:

- Authentication
- Data origin integrity
- Anti-reply protection

Encapsulating Security Payload (ESP) ESP,

It is implemented in a VPN communication, when confidentiality is a major concern. In VPN communication peers AH provides the IP packets with data integrity, confidentiality and authentication services. It offers encryption service by performing encrypting on the IP payload. Encrypting the IP packet using ESP, hides the data content, source and destination IP addresses. It performs authentication for both ESP header and inner IP packet. ESP provides the following services:

- Encryption
- Authentication
- Data origin integrity
- Anti-reply protection

2.9: IPsec Modes of Operation

IPsec security protocols, AH and ESP, can be carried out in two different modes of operation. Transport mode and Tunnel mode

Transport mode

The transport mode gives protection in the OSI layer stack from the transport layer and above. It performs protection to the data payload but it does not protect the original IP address. The original IP is used to transport the data through the Internet. Only IP packet's load that is the actual data being sent is encrypted or authenticated when it is the transport mode. There is no encryption and the original IP header remain the same. The ESP transport mode is not with the Network Address Translation (NAT), since communication is end-to-end or between hosts for example from one client to another.

Tunnel mode

When using tunnel mode, a new IP packet encapsulates the whole original IP packet, including the content and the header. A new IP header is added after the old IP header has been encrypted. When sending traffic over a public network over a secure tunnel, this mode is frequently used for Virtual Private Network (VPN). The tunnel mode gives protection to data and its source IP packet.

CHAPTER 3: Methodology

3.1: Introduction

The objective of this chapter is to delineate the strategies and tools employed to fullfil the envisioned goals of the research. The goal of this research project is to implement a Virtual Private Network (VPN) that will help remote employees of Champions Insurance company to access information securely from the main branch office in Harare. This research project will use an approachable simulation software for the design and implementation of VPN to meet its objective. This chapter will provide an overview of the research methodology, study design, and research philosophy that will be applied throughout the project.

3.2: Research design

A research design is a structured plan or blueprint that outlines the processes, procedures, and methods to be employed in conducting a research study. According to Creswell (2009), research design is important because it provides a roadmap for the research process, guides the collection and analysis of data, and ensures that the research is valid and reliable. Bryman (2008) adds that research design helps to ensure that the research is focused and systematic and that the results are meaningful and useful. In the context of Implementation of VPN, it helps to ensure that the system is developed systematically and effectively.

3.3: Requirements Analysis

Requirement analysis, according to Torkzadeh (2014), is the process of gathering, evaluating, and outlining the requirements and expectations of users. It serves as an essential first step on the road to success. Chung (2016) states that the specifications must be precise, doable, understandable, standardized, and verifiable. In the context of remote VPN, the requirements analysis considers the authentication methods for example username or password, who can access the VPN and also assess the ease of use of the VPN client software for end-users, including installation, connection, and troubleshooting processes.

This information will inform the implementation of the VPN and will ensure that it meets the needs of the users.

The documentation of the requirement analysis process can be divided into two categories which are functional requirements and non-functional requirements.

3.3.1 Functional Requirements

For a system to satisfy the demands and expectations of its users, it must have certain features, capabilities, and functionalities. These are referred to as functional requirements. These specifications outline the functions the system must have and the order in which they must be completed for it to fulfill its intended function. Functional requirements usually cover the behavior, processes, inputs, outputs, and user and system interaction aspects of the system. For the implementation of secure VPN the functional requirements are as follows:

- Support various forms of user authentication like username/password or two factor authentication.
- Implement secure Tunnelling protocols, such as OpenVPN, IKEv2/IPsec, or L2TP/IPsec, to ensure data is encrypted during transmission.
- Automatically assign IP addresses to remote users upon connection

3.3.2: Non functional requirements

Non-functional requirements are specifications that outline how a system should operate in terms of qualities unrelated to its specific functionalities. They are also known as quality attributes or system qualities. The effectiveness of the system is the main emphasis of non-functional criteria. To guarantee that the system satisfies specific performance, security, usability, and other quality standards, these requirements are crucial. Below are the non-functional requirements of the system

- Confidentiality: Ensure that all data transmitted over the VPN is encrypted
- The VPN should be compatible with various devices and operating systems (e.g., Windows, macOS, Linux, Android, iOS).
- The time taken to establish a VPN connection should be minimal to minimize user wait times.

Hardware requirements

- Laptop with core3 or above

Software requirements

- Python 3.9
- Streamlit framework
- Windows 10/11 operating system

3.4: System Development

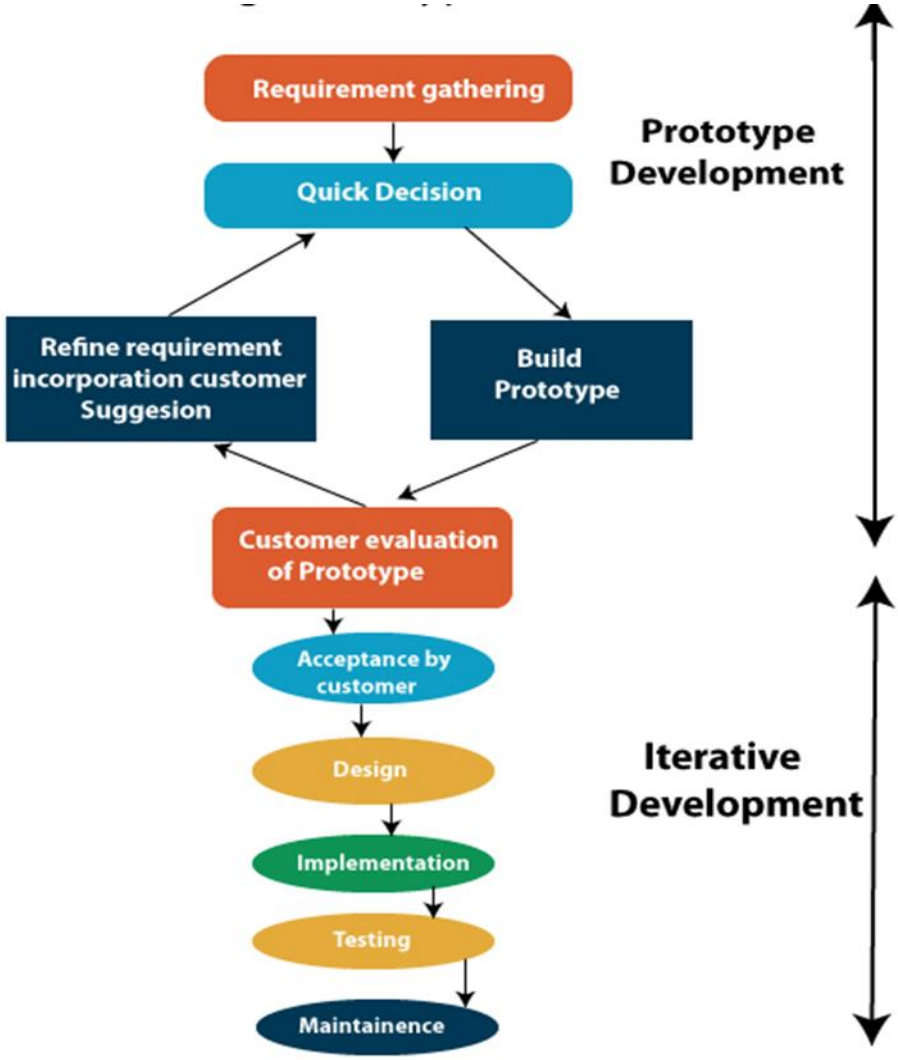
Operating within Windows 10 environment the system will be designed and simulated using Streamlit, Its a powerful Python used for creating interactive web application. The development will start by with requirements gathering, where discussion with the company's employees will inform the desired features and functionalities. The streamlit framework will then be employed to design a user friendly interface, allowing remote employees to connect to the VPN system seamlessly. Python will serve as the primary programming language for the development of Virtual private network algorithm, leveraging libraries like NLTK (Natural language tookit) and spaCy for task such as preprocessing, entity recognition and sentiment analysis. Through Streamlit system will offer functionalities such as providing secure communication between devices and application, ensures that only authorized personnel can access and transmit data and also monitor and detect threats in real time. Extensive testing will ensure the system's accuracy, efficiency and userbility before deployment in the company. User training sessions will be conducted to familiarize

Champions Insurance Company with the system's interface and functionalities. Regular maintenance and updates will be carried out to keep the system aligned with the latest advancements in VPN technology ensuring optimal performance and user satisfaction. This streamlined approach using Streamlit and Python aims to create a tailored VPN system that helps the company protect its data from unauthorised parties by encrypting data being send.

3.4.1: System Development tools

In the domain of networking, a methodology for system design serves as a framework for organizing, planning, and overseeing the methods involved in creating an information system. Numerous frameworks have been identified by researchers for various projects, each with its own set of strengths and weaknesses based on its application. Examples of these frameworks encompass the waterfall model, the spiral model, and the progressive (prototyping) model. The author has opted for the Protoype Software model, given its simplicity, as the project at hand is relatively small and constrained by a strict time frame. Through prototyping, stakeholders (such as users, IT personnel, and management) can offer input on the VPN's initial layout and features. This guarantees that the final product satisfies the users' real requirements and expectations.

Prototype model



Apart from the methodology the system was also developed using the following tools:

Python

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including structured, object-oriented and functional programming

Streamlit

Streamlit is a free and open-source framework to rapidly build and share machine learning and data science web apps. It is a Python-based library specifically designed for machine learning engineers

Dataset

A data set is a collection of data. In the case of tabular data, a data set corresponds to one or more database tables, where every column of a table represents a particular variable, and each row corresponds to a given record of the data set in question

3.5: Summary of how the system works

The user chooses a server location and starts the VPN software. Through a sequence of handshakes that authenticate the user and create a secure tunnel, the client establishes a connection with the VPN server. The data being communicated is encrypted and decrypted using encryption keys that are exchanged between the client and server.
Data Encryption: The VPN client encrypts user data prior to transmission.
Encryption jumbles the data, rendering it unintelligible to anyone who might intercept it during transmission.

Data Transmission: A secure tunnel built between the client and the VPN server transmits the encrypted data.
A packet containing the original data and the encryption header encapsulates the raw data.
Receiving Data: After the client sends the encrypted data to the VPN server, it decrypts it and sends the initial request to the correct location on the Internet.
The data is returned to the VPN server, which encrypts it before sending it back to the VPN client after receiving a response from the destination server (such as a website).

Data Decryption: The VPN client decrypts the data so the user may view and use it after getting the encrypted response from the VPN server.

3.6: System Design

The system design involves creating a robust and user-friendly platform using Streamlit and Python. The architecture begins with a user interface developed in Streamlit, providing Campions Insurance's employees with an intuitive dashboard to interact with the system. Within this interface, users can send information, which is then encrypted by cryptography algorithms implemented in Python using libraries like NLTK (Natural Language Toolkit). These algorithms perform tasks such as text preprocessing, entity recognition, and sentiment. The processed data is then used to generate comprehensive summary reports and interactive visualizations, allowing healthcare professionals to gain valuable insights quickly and effectively. The system design emphasizes ease of use, and secure communication. Additionally, the modular architecture allows for scalability and future enhancements to accommodate evolving needs and technological advancements. Through this design, the

system aims to significantly allow you to send sensitive information online because a VPN helps to protect your data. It encrypts your data and routes it through its secure servers.

3.6.1: Dataflow Diagram

Data flow diagrams (DFDs) expose relationships among and between various components of the system. A dataflow diagram is an important visual method for modeling a system's high-level detail by describing how input data is converted to output results through a continuance of functional transformations. The flow of data in a DFD is named to indicate the nature of data used. DFDs are a type of information development, and as such provides an important insight into how information is transformed as it passes through a system and how the output is displayed.

3.6.2 Proposed System flow chart

Flowcharts are an efficient way of bridging the communication divide between programmers and end users. They are flowcharts specialized in distilling a significant amount of data into comparatively few symbols and connectors.

3.7: Implementation

The implementation of the system involves a structured process using Streamlit and Python to create a functional and user-friendly platform. Beginning with the user interface developed in Streamlit, employees can easily interact with the system by entering username and password.. Python, along with NLP libraries like NLTK and spacy, powers the backend algorithms responsible for processing the data. These algorithms perform various tasks such as text preprocessing, and entity recognition. Once the data is processed, the system generates detailed summary reports and interactive visualizations. The implementation process also includes thorough testing to ensure accuracy, efficiency, and usability. User training sessions are conducted to familiarize employees with the system, ensuring smooth integration into their daily workflows. Regular updates and maintenance are integral to keeping the system aligned with the latest advancements in NLP technology. Through this implementation approach, the system aims to significantly detect security threats and ensure that only authorized people can access and transmit sensitive data ultimately improving the privacy of the company's information.

3.8: Chapter Summary

This chapter delves into the development and implementation of a VPN system aimed at detecting threats. The research project focuses on harnessing the power of Natural Language Processing (NLP) technologies, particularly using Streamlit and Python, to create a comprehensive tool for implementing a secure VPN,

CHAPTER 4: DATA ANALYSIS AND INTEPRETATIONS

4.1: Introduction

This chapter presents the critical phase of data analysis and interpretation used to assess the implementation of Virtual Private Network (VPN) over an open network. The primary purpose of this analysis is to evaluate the performance of the VPN system in terms of throughput, latency, encryption performance and security features under various configurations.

4.2: Simulation Setup

The researcher conducted simulations in a controlled environment. The parameters measured during the simulation include the following:

Throughput - it is the amount data transmitted successfully during a given time.

Latency – this refers to time taken for a packet to travel from the sender to the receiver.

Packet loss rate – This is the percentage of the amount of packet lost during transmission. Packet loss occurs when a unit of data or packet fails to reach its intended destination while being transmitted over a network.

4.3: Analysis of the Results

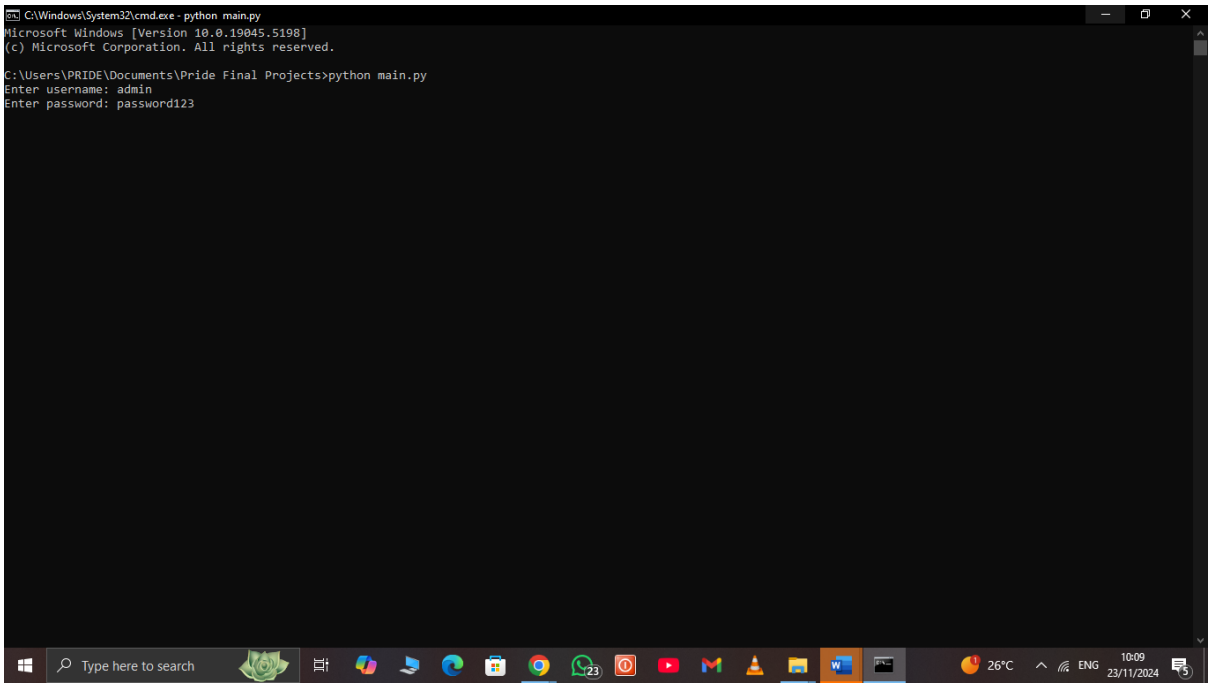


Figure 4.1; Authentication and authorisation

From Figure 1 above the system verifies the identity of the user trying to connect to the VPN. This is called authentication, this is done to ensure that only authorised users are granted access to the VPN, The authentication used in this scenario is the username and password. It

is the most straight forward form of authentication where employees can just provide a unique username and password. This ensures that the user is genuine and not a threat,

The authorisation stage grants or denies access rights to authenticated users based on predefined roles and policies. This helps to protect company's resources by ensuring that users have only access to the resources they need for their work reducing the risks of data breaches

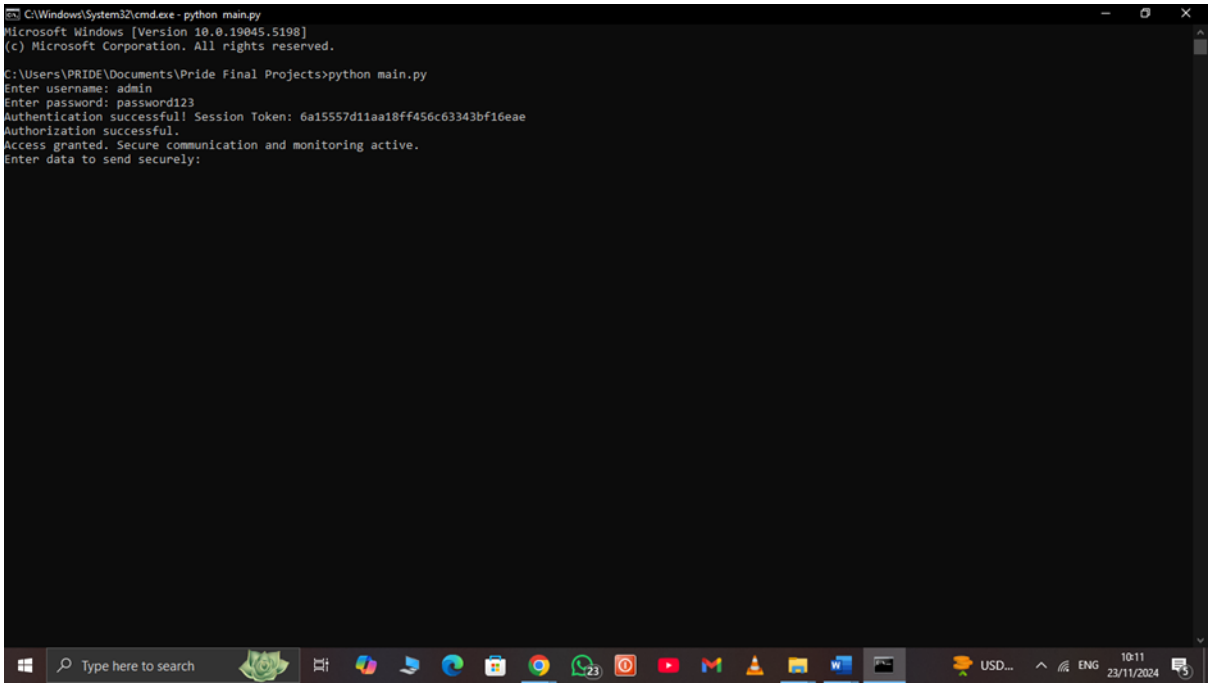


Figure 4.2: Granted access to the VPN

Session Token

After a successful authentication, the server sends a session token to the VPN client. When the VPN client has to authenticate again, it sends the session token passes server site validation test then client can continue rhe VPN session. A session token contains a unique session ID, timestamp and when the token was issued

Communication

Once granted access user can send and receive data as shown in figure 4.3 below. When a user sends data on the VPN the system encapsulate data into packets to be sent over the internet**.** The data packets are then encrypted before they are transmitted to the receiver. This encryption uses cryptographic algorithm to change the original data into an unreadable data**.**

The encrypted data is then transmitted through a secure tunnel created by a VPN protocol**.** The system uses WireGuard protocol, this is a more recent protocol known for its simplicity, speed and security while using modern cryptographic practices.

Upon reaching the receiver the data is decrypted making it readable again

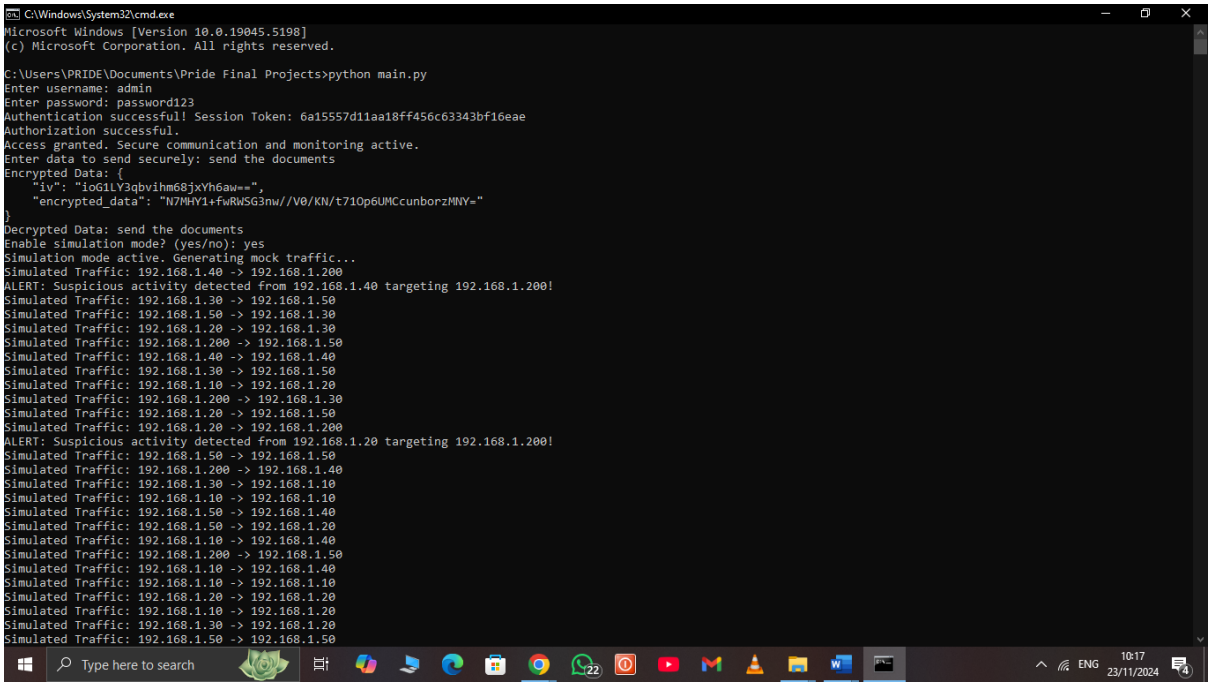


Figure 4.3: Encryption

Simulation Mode

When you switch to simulation mode the system will switch to a simulation panel where you can observe your network traffic.

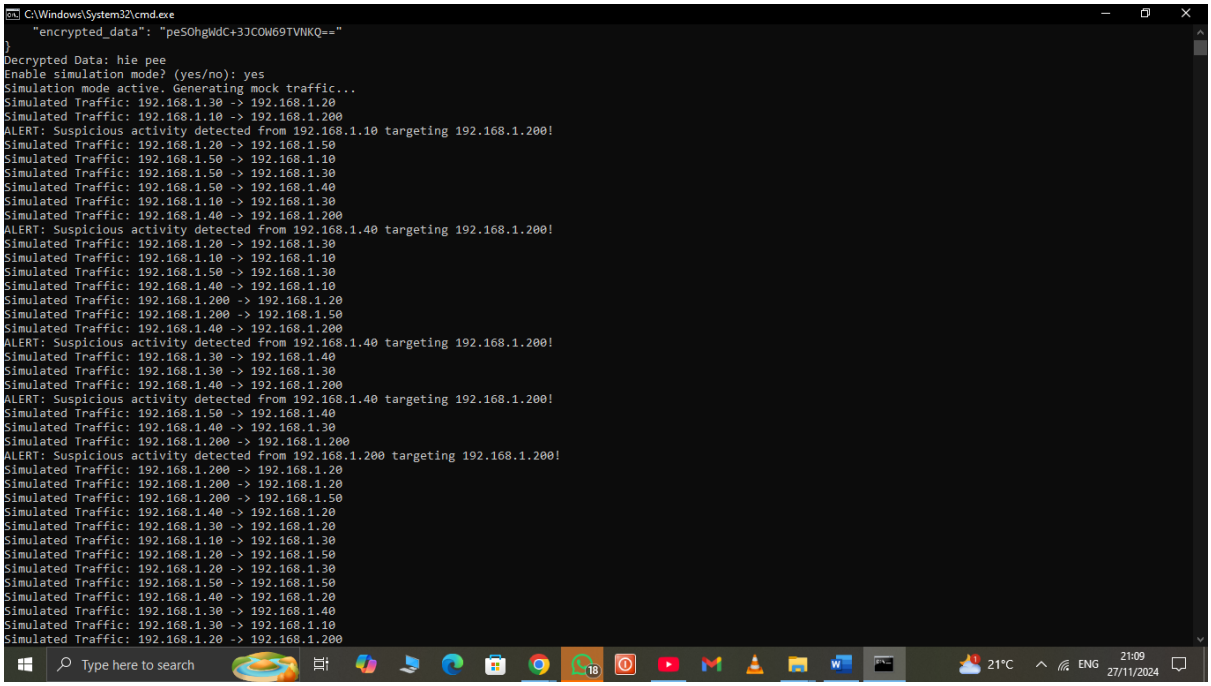


Figure 4.4: Simulation mode

Security log

The system also keep a log of all the users who connect on the VPN and threat detected during the simulation

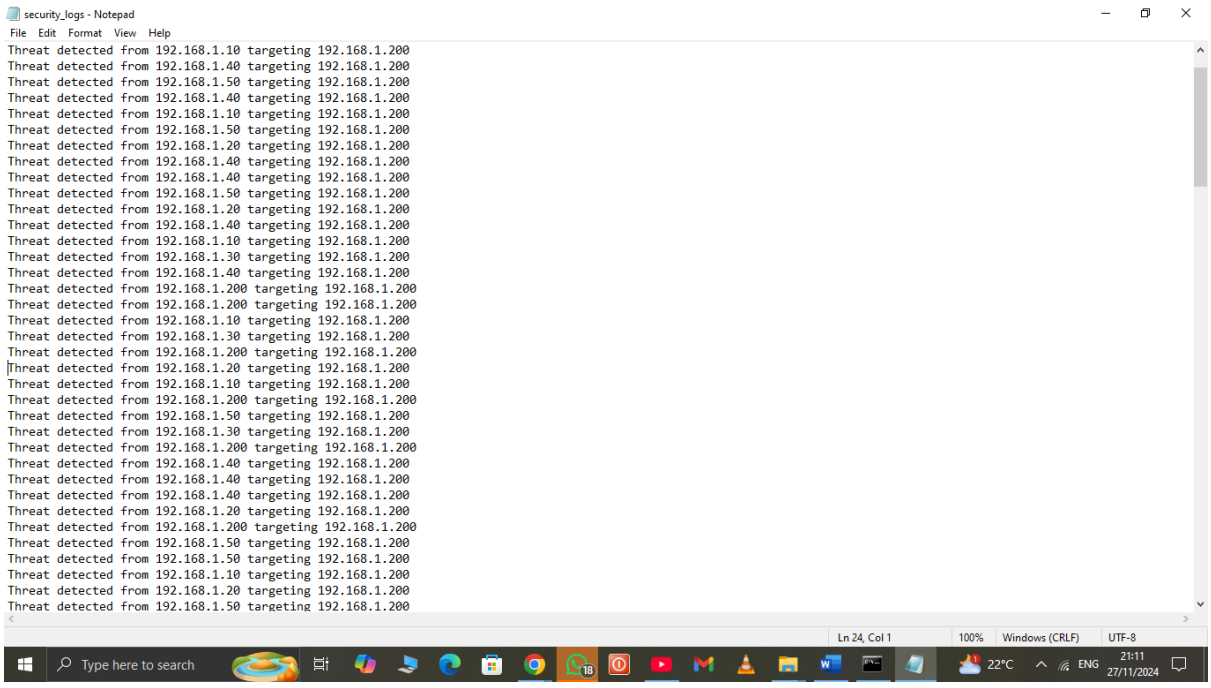


Figure 4.5: Security log

Security log helps to monitor user activity on the VPN system. It documents user connection and disconnections along with the devices utilized and user IDs. Administrators can use this to monitor users who used the VPN and when. They can also be used to monitor the length of time session are in use, logs can be used to spots irregularities in usage trends

It can detect failed login attempts. Unauthorized access attempts may be discovered in logs that monitor unsuccessful login attempts. A brute force attack may be indicated by a large number of unsuccessful login attempts in a short period of time. The security log verifies the IP addresses and timestamps of successful logins, this helps guarantee that the VPN is only being accessed by authorized users. Suspicious activity may be indicated by unusual login times or locations.

4.3: Chapter Summary

In this chapter we analyse the observations and findings from the analysis of the VPN system. Our investigations focused on the number of topics such as security features, and user experience. The VPN system demonstrated robust security protocols, including strong encryption standard (WireGuard), authentication mechanisms (password and username) and stringent access controls. Unknown IP addresses were discovered during a normal inspection of the security logs which pose as a threat to the company.

Chapter 5: RECOMMENDATIONS AND FUTURE WORK

5.1: INTRODUCTION

In this chapter we provide recommendations based on the findings and insights achieved from the study of implementation of virtual private network over an open network. Additionally, we outline potential avenues for future research and development to further enhance the efficiency and effectiveness of improving remote Virtual Private Networks.

5.2: AIMS AND OBJECTIVIES REALIZATION

Throughout this study, our primary goal was to implement a secure virtual private network for a company with offices in different locations. The implementation of the VPN project has been successfully completed, achieving the primary goal of providing secure and reliable remote access to our organization's network. This initiative has significantly enhanced our data security, ensuring that sensitive information is transmitted safely over the internet.

5.3: CONCLUSION

In conclusion, our research highlights the importance of implementing Virtual Private Network for a company with offices in different geographical locations. By implementing a secure VPN connection for Champions Insurance Company, employees can now securely transmit data mitigating risks associated with data breaches and unauthorized access. This has fortified our overall cybersecurity posture and also employees can now connect to the corporate network seamlessly, enabling enhanced productivity, especially in a hybrid work environment. However, while our study yielded positive outcomes, there is still room for further refinement and improvements of our remote VPN.

5.4: Recommendations

Based on our findings, we recommend several strategies to enhance remote Virtual Private Network. Firstly, there is a need to conduct periodic reviews of the VPN's performance and security protocols to adapt to emerging threats and evolving user needs.

User Feedback: Establishing a feedback mechanism will help to continuously improve VPN services and address user concerns more effectively.

Expansion Plans: As remote work becomes more prevalent, further examination of the VPN's capacity and features may be warranted to ensure it meets future demands effectively.

5.5: Future Work

Following the success of completion of our VPN project, a number of crucial areas will still need constant focus and improvements to guarantee the efficiency and security of our VPN services going ahead.

Performance monitoring and optimization: There is a need to set up routine performance monitoring of our VPN, particularly paying attention to pinpoint areas latency, user loads and

connection speeds. We may use this information to pinpoint areas that need work and adjust server setups and locations accordingly.

There is also a need to improve on security. Cyber dangers are always changing in nature. We will give top priority to the ongoing revision of security protocols, such as user authentication procedures and encryption standards, in order to reduce risks. One of the main priority is to implement multi factor authentication in order to improve user login security.

REFERRANCE

1. Bhosale, R., Oke, S. and Dhere, V. (2020) 'Comparative Study of VPN Protocols', *International Journal of Computer Applications*, 975, pp. 1-5. doi: 10.5120/ijca2020919301.

2. Chowdhury, M., Islam, M.N. and Ali, M.A. (2021) 'A Study on the Implementation and Security of Virtual Private Networks', *Journal of Network and Computer Applications*, 177, pp. 1-10. doi: 10.1016/j.jnca.2020.102460.

3. Gunter, D. and Koudelka, J. (2019) 'VPN Implementation and Security Concerns', *Cybersecurity: A Practical Guide to Implementation*, New York: Springer, pp. 45-60.

4. Kaur, R. and Singh, S. (2021) 'Role of VPN in Ensuring Secure Communication: An Overview', *International Journal of Computer Science Trends and Technology*, 9(3), pp. 18-24. Available at: https://www.ijcstjournal.org/paper/role-of-vpn-in-ensuring-secure-communication-an-overview (Accessed: 10 October 2023).

5. Liu, Y., Wang, G. and Zhang, X. (2020) 'Implementation of VPN and its Performance Evaluation'.

6. NIST (National Institute of Standards and Technology) (2017) *Guide to Securing the Virtual Private Network (VPN)*, NIST Special Publication 800-77.

7. Shyles, L. (2021) 'Understanding VPNs: A Technical Overview', Journal of Information Security.

8. Tiwari, A. and Kumar, S. (2021) 'Security Analysis of VPN Services: A Case Study', International Journal of Information Security.

10. Black, J. and Smith, A. (2020) *Understanding VPNs: A Comprehensive Guide*. London: Tech Press.