



AASTU ADDIS ABABA SCIENCE AND TECHNOLOGY UNIVERSITY

College of Engineering

Department of Electrical and computer Engineering

Internship project Report on

“Implementing IPsec Tunneling for Enhanced Data Center Security and Performance.”

By:

Name of the student

ID.No

- | | |
|------------------------|-------------|
| 1. Tedros Teka | ETS 1208/13 |
| 2. Eyerusalem Desalegn | ETS0455/13 |
| 3. Eyerusalem Nigusie | ETS 0457/13 |

Supervisors:

1. University supervisor name: Mr. Yalemsew Abate
2. Industry supervisor name : Ms. Elsabet Alemayehu

*Submitted to Addis Ababa Science and technology University Department of
Electrical and Computer Engineering (communication stream)*

September, 30/ 9/2024

Addis Ababa, Ethiopia

Declaration

We Tedros Teka, Eyerusalem Desalegn, and Eyerusalem Nigusie, students of Addis Ababa Science and Technology University, declare that this report describes actual events and facts observed and performed during our two and half month internship program at IPCOM Technology Solution. We appreciate the guidance and support of our advisor, Mr. Yalmsew, and our company supervisor, Ms. Elsabet during our internship at IPCOM Technology. The internship program helped us develop our technical skills and knowledge in information technology, and we are confident that the experience gained will be useful in our future careers. We have used different sources, mentioned under the reference section, to prepare this document. We hereby declare that this report is prepared by ourselves, and our mentor has approved it by placing his signature below.

Name

Signature

1. Tedros Teka
2. Eyerusalem Desalegn
3. Eyerusalem Nigusie

Advisor's Approval

This certifies that the candidates' above statement has been accepted and is prepared for submission for presentation.

Name : Mr Yalemsew

Signature

Abstract

A network company is a specialized business that focuses on providing a range of network-related services to both corporations and individuals. These services typically include network design, installation, maintenance, and troubleshooting, ensuring that the infrastructure is robust, efficient, and tailored to meet the specific needs of clients. Additionally, the company may offer advanced network security services, such as the deployment of firewalls, intrusion detection systems, data encryption, and regular security audits to protect sensitive information from unauthorized access and cyber threats.

In addition to these core services, a network company may provide consultation and training to help organizations optimize their network performance and adopt the latest technologies. This includes advising on network scalability for future growth, disaster recovery planning, and implementing redundancy measures to minimize downtime.

The primary objective of a network company is to ensure that all clients have reliable, secure, and efficient access to their data and applications, regardless of location or device. By offering a comprehensive suite of services, these companies play a crucial role in enabling businesses to operate smoothly in today's digital world. The responsibilities and services of a network company are briefly described in this abstract.

Acknowledgment

We, Eyerusalem Desalegn, Eyerusalem Nigussie, and Tedros Teka, would like to express our deepest gratitude to AASTU's Department of Electrical and Computer Engineering for providing us the opportunity to work with this prestigious organization and gain invaluable professional and educational experiences.

We extend our sincere thanks to our company supervisors, Ms. Elsabet, Mr. Kirubel, as well as our academic advisor, Mr. Yalmsew, for their unwavering support and guidance throughout our internship program. Their expertise and encouragement have greatly enhanced our knowledge and skills in the field of information technology. We are also grateful to our hosting firm, IPCOM Technology Solutions, for welcoming us and providing a conducive environment for learning and growth.

Additionally, we wish to express our heartfelt appreciation to the SDN (Software-Defined Network), Data Center Network, and Core Network Department staff members who went above and beyond to ensure we felt at ease while working at the company. Their willingness to share their knowledge and experience significantly contributed to the development of our understanding and capabilities.

We are highly indebted to every advisor for their guidance, constant supervision, and for providing the necessary information regarding both the internship report and the completion of our work.

Finally, we would like to express our gratitude to our co-workers, friends, and parents for their kind cooperation and encouragement, which played a crucial role in the successful completion of this internship program.

Executive Summary

This report is our Internship report. It consists of five chapters in which an introduction about the company that we've been working for, IPCOM Technologies, our internship experience, internship achievements and also the project we did from the knowledge we gained during our internship, as well as conclusion and recommendations section.

The first chapter encompasses introduction and background, the work flow, the main services and customers of the company. In the second chapter our internship experience including the section of the company we were assigned to work, the executed tasks, the challenges we faced and the measures taken to overcome the challenges are mentioned. The third chapter discusses the project we did, which is IPsec VPN tunneling. It includes the objective, literature review, methodology, result and discussion of the project. The fourth chapter addresses the knowledge and skill acquired during internship. Lastly, the fifth chapter is the conclusion of the report. Finally, this report will explain how our internship progressed over the course of two and a half months, as well as what we learnt while working as an intern at IPCOM Technologies.

Table of Content

List of Figures.....	vi
List of Tables	vi
List of Abbreviation	vi.

Chapter One

1. Introduction and background of IPCOM.....	1
1.1 Brief history of IPCOM.....	1
1.2 Main product and services of IPCOM.....	1
1.3 Main customer or end users.....	4
1.4 Overall organization work flow.....	5

Chapter Two

2. Overall internship experience	7
2.1 The section of the company we had been assigned to work.....	7
2.2 The workflow of the section	7
2.3 Executed Tasks.....	12
2.4 Procedures and methods used	12
2.5 Challenges during internship	12
2.6 The measures taken to overcome the challenges.....	13

Chapter Three

3. Selected industrial project and its design procedure.....	14
3.1 Design project title	14
3.2 Short summary of the project	14
3.3 Problem statement and justification	15
3.4 Objective of the project	16
3.5 Literature review	17

3.6 Methodology	24
3.7 Result and Discussion.....	26

Chapter Four

4. Overall internship achievements and experiences.....	29
4.1 Upgrading theoretical knowledge.....	29
4.2 Practical skills Gained.....	29
4.3 Improved Industrial problem solving capability.....	29
4.4 Improved team working skills.....	30
4.5 Improved leadership skills.....	30
4.6 Understanding about work ethics.....	30
4.7 Entrepreneurship skills Gained.....	31

Chapter Five

5. Conclusion and Recommendation.....	32
5.1 Conclusion.....	32
5.2 Recommendation	33
Reference.....	34
Appendix.....	35

List of Figures

Figure 1.1: Organizational Structure.....	5
Figure 1.2: Work Flow of IPCOM.....	6
Figure 2.1: Modular Data center.....	9
Figure 2.2: Simulation of data center.....	10
Figure 2.3: Composition of Data Center facility.....	10
Figure 3.1: IP packet in IPsec Transport mode	21
Figure 3.2: IP packet in IPsec tunnel mode	22
Figure 3.3 Network Design using CISCO Packet Tracer.....	26
Figure 3.4 Test Reachability of between devices.....	27

List of Tables

Table 3.1: IP Address Planning	26
Table 3.2: IP Address Allocation of End-Devices.....	27

List of Abbreviations

AASTU - Addis Ababa Science and Technology University

DCN – Data Center Networking

IP – Internet Protocol

CISCO - Commercial and industrial security corporation

PDU - Power distribution unit

DCIM - Data center infrastructure management

LAN - Local Area network

WLAN - Wireless Local area network

CAPEX - Capital expenditure

OpEX - Operating expenses

VLAN - Virtual Local Area Network

OSI - Open system interconnection

TCP - Transmission control protocol

UDP - User datagram protocol

IPsec - Internet Protocol Security

VPN - Virtual Private Network

CLI - command line interface

IKE - Internet key Exchange

ISKMAP - Internet Security Association and Key Management Protocol

DEEL -Design Engineering and Electronic Learning

EMC -Electromagnetic Compatibility

ESP- Encapsulating Security Payload

AH -Authentication Header

MAC -Media Access Control

SSL - Secure Sockets Layer

Chapter One

1. Introduction and background of IPCOM Technologies

1.1 Brief History of IPCOM Technologies

IPCOM is a private limited company which was founded in 2010 G.C to give a complete IT solution for its clients. The company has been working on many projects for different companies that acquire them to be more experienced and fully updated with the latest technology based on the data center Designing, installation, and configuration networking devices.

The company has been working on many projects acquiring them to be more experienced and fully updated with the latest technologies. It's not the only reason that they are chosen to provide service but also the company employees including the owner are dedicated and continuously updating themselves with current technologies. In addition, they are licensed with top international certifications including CISCO, VMware, DELL-EMC, APC etc. IPCOM has partnered with top technology solution providers, to make sure its clients have the right solution they deserve. Since those solution providers are known internationally to be the best, this makes IPCOM to be among the best solution providers currently working in Ethiopia.

Vision

Become prestigious technology solutions innovating firm and to join the electronics manufacturing industry

Mission

IPCOM Technologies is committed to design and implement up to date technology by making use of the internet and in order to gear intelligence into buildings and homes.

1.2 Main product and services of IPCOM

IPCOM offers a complete life-cycle of services, including IT Supply Chain Services, Professional Services, Support and Managed Services, and IT Outsourcing Services across a comprehensive range of networking.

1. Data Center

IPCOM Technologies expertise in data centers facilities, including power and cooling optimization, Rack and Cabinets, PDUs, DCIMs, Aisle containments, structured cabling, Safety and Security Systems, allow to maximize the impact of server, storage and virtualization projects. By Using Modular Data Center, protect on-premise business applications, roll out and implement software defined data centers, simplify and speed up planning, designing and building data centers, optimize costs and performance, secure critical applications and most valuable data, monitor, automate and control the entire data center physical infrastructure with integrated DCIM.

2. Core Networking

IPCOM sees core Network Infrastructure as the platform for all business functions and communications. They provide a powerful point of differentiation through availability, flexibility, scalability, performance, and security. They can help to Design, Integrate, Manage and Secure resilient enterprise LAN and WLAN Infrastructure.

3. Virtualization

Today Virtualization has become the strategy of IT leaders. There are no more cost savings and the containment of CAPEX and OpEX. Virtualization improves business continuity and resilience, and can assist you in disaster recovery preparations. IPCOM's can help to harness the power of virtualization to reduce operational costs and improve automation. Virtualization is also moving beyond the server and storage domains. Desktop virtualization is on the fast track to mainstream adoption. Desktop virtualization helps you manage device proliferation and operate more effectively and securely in today's mobile, user-centric workspace.

4. Unified Communication

IP telephony (IPT) forms the foundation of unified communications and collaboration strategy. Migrating from a distributed, legacy telephony infrastructure to a more integrated, user-centric model abounds with pitfalls.

5. Safety and Security

Surveillance is not just about protecting assets from threats. Keeping staff and customers safe is important too and security solutions need to provide the detail required seeing things clearly.

Surveillance systems can be used to remotely monitor property and deter vandalism. A sophisticated, built-in motion detection system can generate an alarm, which automatically transmits images to security operators giving them accurate, up-to-the minute information upon which to base their decisions. Security project involves a number of stages including system design, product installation, maintenance and support. IPCOM offers a comprehensive set of tools and features that help Customers get the right solution for the purpose. They have highly skilled Engineers and Certified technicians that can take business from beginning to end to address the infrastructure needs you are embarking upon today.

6. Performance Optimization

Improving the end-to-end performance, availability and security of applications and services across communication networks. If a data center has evolved over time, it's possible that it's not making the most efficient use of computing, storage, and energy resources. IPCOM Technologies data center optimization teams can assist with data center planning, rationalization, migration, and management across on-premise, hosted, and cloud environments. They ensure that business continuities aren't interrupted and that most precious assets – data – isn't lost or rendered inaccessible, through robust backup and recovery systems and techniques.

7. IT Support Services

IPCOM Technologies proactive approach reduces risk by identifying problems before they arise. They also provide an annual maintenance support contract for your existing Data Center Power, Cooling, Fire Alarm, Network Infrastructure, Compute and Storage Server Infrastructure.

8. Building Automation Systems

Voice and Data Network, Fire Alarm and Fire Suppression Systems, Access Control and Video Surveillance Solutions, Public addressing, digital signage, water and energy saving technologies, keep pace with Internet of Things (IoT) and etc.

9. SMART Systems

SMART Classroom Solutions Provide more interactive alternatives to traditional teaching. It deals with a variety of practical teaching tools and materials for teachers including teaching games, exercises and examples that teachers can apply to their courses. The SMART as a whole brings flexibility to learning and makes learning ubiquitous. They have partnered with a range of

solution providers that deliver total Education Innovation Solutions that bring Classes to Life with Ease. They Supply, Install, educate and support SMART CLASSROOMS, they deliver technology with elegant professional installation services.

10. Consulting

IPCOM Technologies can also help to choose the right solution that suits and scales customers business growth. They can also assist with consolidating existing platforms, and realizing the operational and cost benefits promised.

1.3 Main customer or end users

The main customers of IPCOM are many private and governmental sectors/companies that need IT solutions and consultancy.

◆ **Governmental Organizations:** Public institutions, government agencies, and municipalities that, in order to operate and provide public services, require a secure and trustworthy network infrastructure.

◆ **Financial Institutions:** To manage sensitive financial transactions and data, banks, insurance organizations, and financial service providers require high-performance and secure network solutions.

◆ **Enterprises:** Huge companies and organizations in need of reliable and expandable network solutions to link their offices, data centers, and outlying areas.

◆ **Educational Institutions:** Colleges, universities, and schools that need to provide their staff, instructors, and students with fast and secure network connectivity.

1.3.1 Previous IPCOM projects

IPCOM provide IT solution to Zemen Bank with Facility Management, For Gondar University with project of Turnkey Delivery of IP Surveillance Security Camera System, for Addis Ababa 4 kilo University to establish an Open Computer Lab Facility for Medical and Health Science College project of VMware Virtual desktop Infrastructure, for Cooperative Bank of Oromia (CBO) with project called SDN-DCN and unified communication.

1.4 Overall organization work flow

1.4.1 Organizational Structure of IPCOM Technologies

The organizational structure of IPCOM can be clearly shown in the following diagram. The structure which this has made it to efficiently do its job.

The following figure shows the organizational structure used by IPCOM Technologies Trading PLC.

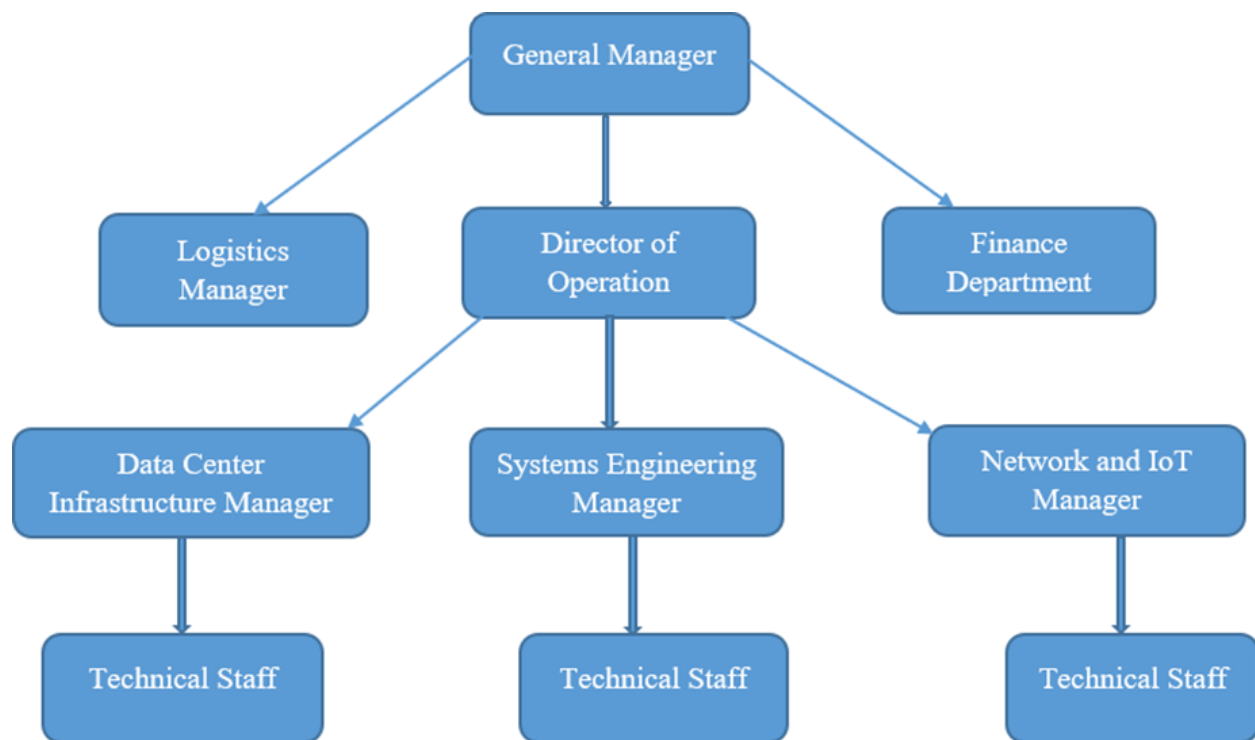


Figure 1.1 Organizational Structure

1.4.2 Work Flow of IPCOM Technologies

i. Meet and Consult

IPCOM Technologies provide expert technology advice and world class solutions, based on a deep understanding of 6 customers' business and needs. Their strategic and technical consultancy services deliver value for your business, every step of the way.

ii. Design

IPCOM Technologies utilize the latest tools and techniques from computational fluid dynamics (CFD) to 3D modeling and technical drawing to help customers understand the options and

implications of different approaches. They can do this cost effectively and against tight timescales to respond to specific project demands.

iii. Implement

Data centers and other business critical environments require expert knowledge and specialist skills. They believe innovation is key to delivering optimum performance, reducing cost and maximizing investment. Their customer focused teams deliver complex, time constrained projects successfully in new and live environments, minimizing risk. Using their design and delivery expertise, they bring together the people, processes, behaviors and tools needed to operate critical environments safely and proactively – to deliver the optimum performance.

iv. Train

IPCOM gives the skills and inspiration to keep creating great experiences. They work together with customers to deliver measurable, ongoing results based on a strong foundation of philosophy, process, collaboration and education.

v. Support

IPCOM makes it easier to operate the data center today, by maintaining performance and reducing risk and to deliver the capabilities that IT requires for the future. Their support services can significantly improve your IT performance and reduce overheads. Their approach to service interruption avoidance is through proactive monitoring and providing responsive management. Should service interruption occur, our experts are quick to respond and minimize downtime. By making data centers support their responsibility, your organization not only benefits from augmented IT support but also reduced operating costs.



Figure 1.2 Work Flow of IPCOM

Chapter two

2. Overall internship experience

2.1 The section of the company we had been assigned to work

During our internship at IPCOM Networking Company, we embarked on a journey of learning and hands-on experience in the realm of data center facility, networking, system and cyber security. The initial weeks were dedicated to building a strong foundation in networking basics. We gained an understanding of fundamental concepts such as IP addressing, subnetting, OSI model, and TCP/IP protocols. We also gained fundamental knowledge about data centers, systems, networks and cyber security. We got the opportunity to observe the datacenters of COOP bank and Ethiopia Shipping Line. This knowledge served as a crucial framework for the rest of our internship.

Another significant topic covered was virtualization, which is a cornerstone of modern data center design. The lecture introduced us to the concept of creating virtual versions of physical hardware, such as servers, storage devices, and networks. We explored different virtualization platforms and learned how they improve resource efficiency, flexibility, and scalability in networking environments. Understanding virtualization is critical as it enables the creation of scalable and secure network infrastructures, which aligns with the work we were engaged in at IPCOM.

2.2 The workflow of the section

2.2.1 Data Center Networking (DCN)

DCN is a complex arrangement of network devices such as routers, switches, interfaces, etc., that inter-connects the various computing and storage units in a data center's resource pool to ensure a high-level of performance.

In DCN there are three fundamental components that form the core of a data center network for network, server and storage infrastructure. The key concept of data center networking is the infrastructure that allows communication and connectivity within a data center environment. It involves the design, implementation, and management of networks that interconnect servers, storage devices, and other networking equipment in a data center.

Some key concepts of data center networking include:

i. High Bandwidth: Data center networks are designed to handle large amounts of data traffic with high bandwidth capabilities. This ensures efficient communication between servers and storage devices within the data center.

ii. Low Latency: Low latency is crucial in data center networks to minimize delays in data transmission. Low-latency networks enable real-time applications and improve overall system performance.

iii. Redundancy: Data center networks are built with redundancy in mind to ensure high availability. Redundant network paths and equipment help in maintaining network operation even in the event of failures

iv. Scalability: Data center networks are designed to scale easily as the demand for computing and storage resources increases. Scalable networks accommodate additional servers and devices without impacting performance.

v. Virtualization: Network virtualization is a key concept in data center networking. It enables the creation of multiple virtual networks that can be isolated and managed independently, providing flexibility and security.

vi. Traffic Segmentation: Data center networks often employ network segmentation to separate different types of traffic, such as storage, application, and management traffic. This helps in optimizing network performance and improving security.

vii. Network Security: Data center networks require robust security measures to protect sensitive data and prevent unauthorized access. Firewalls, intrusion detection systems, and encryption are commonly used to enhance network security. These are some of the key concepts in data center networking. The design and implementation of data center networks are complex and require expertise in network architecture, protocols, and technologies.

Modular data centers are designed to deal with changes in servers such as cloud computing, virtualization, centralization and high density, improve the operation efficiency of data centers, reduce energy consumption and achieve the goal of rapid expansion and zero interference.

Modular data centers are comprised of various modules with independent functions and a unified input/output interface. Modules in different compartments can make duplications for each other and a fully functional data center is established through a combination of related modules.

Modular data centers are integrated, standardized, optimized and intelligent with highly adaptable infrastructure and a computing environment of high availability.

Modular data centers will meet the urgent needs of the IT department in the future, such as standardization, module, virtual design, dynamic IT infrastructure (flexibility and high usage rate of resources), 24/7 smart operations management (process automation, smart data center), business continuity support (disaster recovery and high availability), shared IT service (inter-business and shared infrastructure, information, application), quick response to the changing needs in business (on-demand supply of resources), green data centers (energy-saving and carbon-reduction), and so on.



Figure 2.1: Modular Data center

Data center life cycle

- 1. planning**
- 2. Design**
- 3. Construction**
- 4. Operation and Maintenance**
- 5. Evaluation**

In designing data centers real-time information, simulation, and remote monitoring technologies are involved in the process which help with resource and asset management.



Figure 2.2: Simulation of data center

Composition of Data center facility

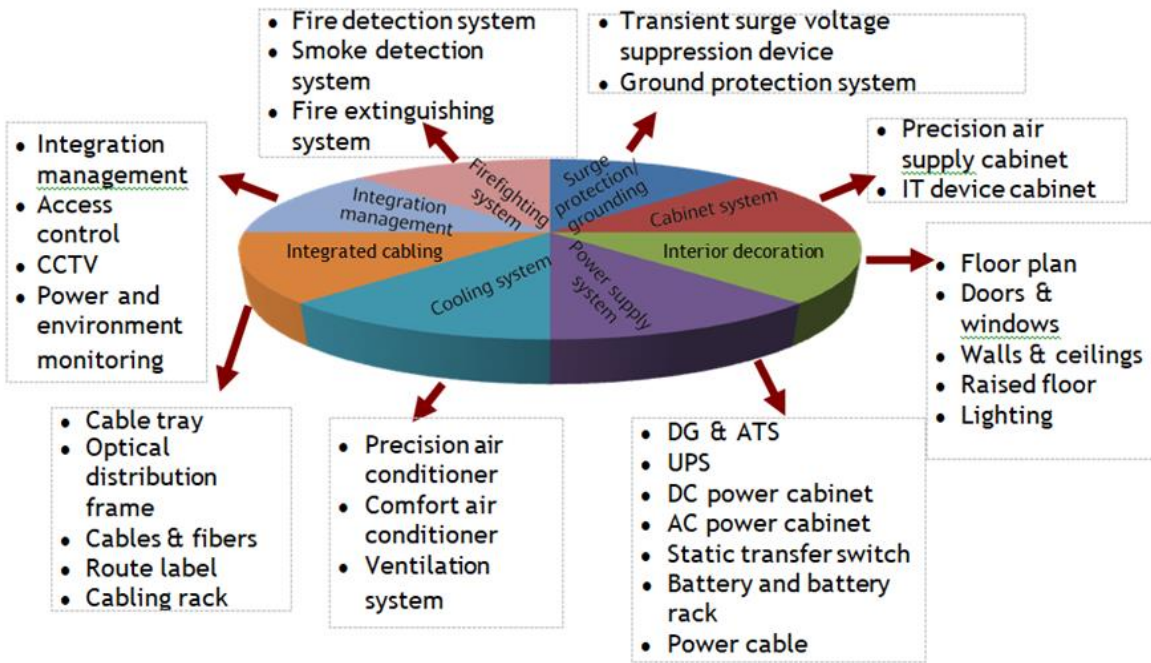


Figure 2.3 : Composition of Data Center facility

2.2.2 Core Networking

It is also called a backbone network. Because it is a central conduit designed to transfer network traffic at high speeds. Core networks focus on optimizing the performance and reliability of long-distance and large-scale data communications. They connect wide-area networks (WAN) and local area networks (LAN) altogether. While core networks provide a plethora of services, one of their key functions includes routing telephone calls across the public switched telephone network (PSTN).

2.2.3 Network Security

Network Security protects a network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection. Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

2.2.4 Virtual Networking

Virtual networking enables the communication between multiple computers, virtual machines (VMs), virtual servers, or other devices across different office and data center locations. While physical networking connects computers through cabling and other hardware, virtual networking extends these capabilities by using software management to connect computers and servers over the Internet. It uses virtualized versions of traditional network tools, like switches and network adapters, allowing for more efficient routing and easier network configuration changes. Virtual networking enables devices across many locations to function with the same capabilities as a traditional physical network. This allows for data centers to stretch across different physical locations and gives network administrators new and more efficient options, like the ability to easily modify the network as needs change, without having to switch out or buy more hardware; greater flexibility in provisioning the network to specific needs and applications; and the capacity to move workloads across the network infrastructure without compromising service, security, and availability.

2.3 Executed Tasks

At first we had orientation about the company then we attended training sessions on data center facilities. it includes

- Introduction to data center facilities
- competition of data center infrastructure
- power system of data centers
- cooling system of data centers
- data center integrated management
- data center standards
- Air conditioning system and data center Air conditioner
- monitoring system and system functions of data centers
- cloud computing
- cyber security

We also did practical work which was virtualization. and we visited data centers of coop bank and Ethiopian shipping lines to understand the practical operation of data centers.

2.4 Procedures and methods used

During our internship, we had the opportunity to engage in a variety of learning experiences that significantly enriched our understanding of the field.

One of the key components was the lectures provided by experienced professionals. These sessions covered essential procedures and methods relevant to our work, blending theoretical knowledge with practical applications. This dual approach helped solidify our understanding of complex concepts.

Additionally, we participated in site visits, which allowed us to observe real-world applications of what we learned in the classroom. These visits were invaluable; they provided context and depth to the procedures discussed in lectures, showcasing how they are implemented in practice.

Overall, the combination of lectures and hands-on experiences during site visits made the internship both educational and engaging, equipping us with skills and insights that we will carry into our future career.

2.5 Challenges during internship

- **Limited Cross-Functional Collaboration:** Networking in practice often involves collaboration with other IT teams, such as system administrators and cyber security experts. Our internship experience primarily revolved around networking tasks, and We had limited opportunities to work closely with professionals from other IT disciplines. Encouraging more cross-functional collaboration during internship
- **Adapting to new technologies:** The network solutions industry is constantly evolving, and new technologies are being introduced regularly. As an intern, we had to learn how to adapt quickly to new technologies and stay up-to-date with the latest trends.
- **Technical difficulties:** As an intern, we were not always familiar with the company's network infrastructure and software. This made it challenging for us to troubleshoot technical issues and resolve them quickly.

2.6 The measures taken to overcome the challenges

During your internship in the network solutions company, we took several measures to overcome the challenges we faced. Some of the measures include

- **Improving communication skills:** To improve our communication skills, we actively listened to our colleagues and asked questions to clarify any misunderstandings. we also learned how to communicate our ideas and thoughts clearly and concisely.
- **Staying up-to-date with new technologies:** To stay up-to-date with new technologies, we attended training sessions and workshops organized by the company. We also read industry publications and blogs to keep ourselves informed about the latest trends and developments.
- **Seeking guidance and support:** Whenever we encountered technical difficulties, we sought guidance and support from our supervisor or other experienced professionals in

the company. This helped us to learn from their expertise and resolve issues more efficiently.

- **Prioritizing tasks:** To manage my workload effectively, we learned how to prioritize tasks based on their level of importance and urgency. This helped us to meet deadlines and ensure that we completed all my tasks on time.

Chapter three

3. Selected industrial project and its design procedure

3.1 Design Project title

The project aims to address network security by using IPsec VPN tunneling, which is deployed on modular data centers of a certain company at different sites. The title of the project is “Implementing IPsec Tunneling for Enhanced Data Center Security and Performance.”

3.2 Short summary of the project

The project, titled “Implementing IPsec Tunneling for Enhanced Data Center Security and Performance,” focuses on improving the security and performance of modular data centers across multiple sites using IPsec VPN technology. By configuring site-to-site VPN tunnels through IPsec, secure communication channels are established between the data centers, ensuring data confidentiality, integrity, and protection from unauthorized access.

The implementation is carried out using Cisco Packet Tracer, where routers are configured with ISAKMP and IPsec policies to encrypt and authenticate traffic between sites. The project emphasizes the importance of strong encryption protocols (AES, SHA-256) and access control mechanisms to safeguard the data. Results demonstrate successful tunnel creation, secure communication, and minimal performance impact, proving the effectiveness of IPsec for securing distributed networks. This solution provides a scalable and robust approach to enhancing data center security.

3.3 Problem statement & Justification

The current type of data center design that the organization uses is an updated version of modular data center. Modular data centers are scalable and flexible. But there are some common problems that every data center faces. One of them is the security of the network devices data centers. The network devices such as switches, routers, firewalls facilitate the transmission of data packets. Therefore sensitive data that are transmitted between modular data centers can be accessed by unauthorized users or there might be interception.

These problems can be addressed by encapsulation and encryption of data packets using IPsec VPNs.

Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:

Confidentiality: IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key or a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key

Integrity: IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

Peer Authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

Replay Protection: The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.

Traffic Analysis Protection: A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.

Access Control: IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.

3.4 Objective of the project

General objective

The general aim of doing this project is to ensure security of network devices and protecting the data packets from unauthorized access by ensuring encapsulation and encryption between two sites.

Specific objective

Encryption is a security measure to maintain protection of data from unauthorized access. So specifically the objective of this project is to set up the IPsec VPN Tunnel by Configuring an IPsec VPN Tunnel in packet tracer, Creating an IPsec VPN Tunnel and lastly Setting up and IPsec VPN Tunnel with AES and SHA for encryption and for authentication respectively.

- 1. Network Topology Setup:** A network topology diagram is discussed that outlines the connection from a main network to a branch network via ISP, emphasizing that direct cabling isn't viable due to geographic distances. The need for secure communication through an IPsec tunnel is established, as ISP traffic is inherently untrusted.
- 2. Equipment and Configuration Steps :** The configuration requires specific equipment: a 2911 router and a 2960 switch. Following the initial setup, IP addresses must be assigned to router interfaces and computers.
- 3. Routing Protocol Configuration:** The OSPF (Open Shortest Path First) routing protocol is configured for communication between routers, followed by testing to ensure successful connectivity.
- 4. Enabling IPsec VPN Functionality:** The process begins with enabling the security technology package on the routers, which is essential for configuring IPsec VPNs.

Licensing commands and module queries are provided to ensure the security features are activities.

5. **Access Control List (ACL) Configuration:** Extended ACLs are configured on both routers to permit the relevant IP traffic that needs encryptions. The correct wildcard masking is emphasized for ACLs to function correctly.
6. **Internet Key Exchange (IKE) Configuration :** Internet Key Exchange (IKE) Phase 1 and Phase 2 configurations are detailed, including definitions for encryption and authentication using pre-shared keys. Key parameters, such as encryption algorithms and D-H groups, are specified.
7. **Transform Set and Crypto Map Configuration :** A transformation set is created followed by a crypto map that binds the operations to the ACLs. The commands needed for binding the transform set to policy and enabling crypto maps at specific interfaces are provided.
8. **Testing and Verification :** Final verification of the configuration is performed using the crypto commands to ensure the IPSec tunnel is established. Successful pings between network nodes demonstrate that encryption is operational, as reflected in IPSec security associations.

3.5 Literature review

VPN (Virtual Private Network) is referred to as an encoding and access management technology for the public network, providing private communication networks. VPN is transparent to users and appears to be using a personal circuit between users.[1]

To access all data with a high level of security, along with obtaining an excellent quality of service, Virtual Private Network (VPN) is considered as one of the optimum solutions.[2]

VPNs can use both symmetric and asymmetric forms of cryptography. Symmetric cryptography uses the same key for both encryption and decryption, while asymmetric cryptography uses separate keys for encryption and decryption, or to digitally sign and verify a signature.

Symmetric cryptography is generally more efficient and requires less processing power than asymmetric cryptography, which is why it is typically used to encrypt the bulk of the data being

sent over a VPN. One problem with symmetric cryptography is with the key exchange process; keys must be exchanged out-of-band to ensure confidentiality. [3]

A virtual private network (VPN) is an encrypted connection between two or more computers. VPN connections take place over public networks, but the data exchanged over the VPN is still private because it is encrypted.

VPNs make it possible to securely access and exchange confidential data over shared network infrastructure, such as the public Internet. For instance, when employees are working remotely instead of in the office, they often use VPNs to access corporate files and applications.

Many VPNs use the IPsec protocol suite to establish and run these encrypted connections. However, not all VPNs use IPsec. Another protocol for VPNs is SSL/TLS, which operates at a different layer in the OSI model than IPsec. (The OSI model is an abstract representation of the processes that make the Internet work).

IPSec VPN is a network security system delivering security communication between a pair of nodes. It is used to address VPN links between one and other gateways, including access protection, confidentiality, integrity security and authentication of original data etc. IPSec VPN is the standard remote access control solution of a company.[1]

A common misconception about IPSec is that it is a single protocol for providing these security services for IP traffic. In fact, IPSec is really a suite, or collection, of protocols for security defined by the IPSec working group in the IETF.[4]

The Internet Engineering Task Force (IETF) created the IP security (IPsec) protocol suite, a network-level security service that integrates IP extensions to handle network security challenges. It is made up of three primary parts: the Internet key exchange protocol (IKE), the IP authentication header (AH), and the IP encapsulating security payload (ESP) format. IPsec technology makes use of contemporary cryptographic techniques to offer strong data privacy and authentication. The network itself is safeguarded in addition to the programs that use it. Secure virtual private networks (VPNs), which are private and secure networks carved out of public or unsecured networks, are possible because IPsec is set up to prevent protocol packets from being intercepted or forged on a basic network.[5]

How do users connect to an IPsec VPN?

Users can access an IPsec VPN by logging into a VPN application, or "client." This typically requires the user to have installed the application on their device.

VPN logins are usually password-based. While data sent over a VPN is encrypted, if user passwords are compromised, attackers can log into the VPN and steal this encrypted data. Using two-factor authentication (2FA) can strengthen IPsec VPN security, since stealing a password alone will no longer give an attacker access.

How does IPsec work?

IPsec connections include the following steps:

Key exchange: Keys are necessary for encryption; a key is a string of random characters that can be used to "lock" (encrypt) and "unlock" (decrypt) messages. IPsec sets up keys with a key exchange between the connected devices, so that each device can decrypt the other device's messages.

Packet headers and trailers: All data that is sent over a network is broken down into smaller pieces called packets. Packets contain both a payload, or the actual data being sent, and headers, or information about that data so that computers receiving the packets know what to do with them. IPsec adds several headers to data packets containing authentication and encryption information. IPsec also adds trailers, which go after each packet's payload instead of before.

Authentication: IPsec provides authentication for each packet, like a stamp of authenticity on a collectible item. This ensures that packets are from a trusted source and not an attacker.

Encryption: IPsec encrypts the payloads within each packet and each packet's IP header (unless transport mode is used instead of tunnel mode — see below). This keeps data sent over IPsec secure and private.

Transmission: Encrypted IPsec packets travel across one or more networks to their destination using a transport protocol. At this stage, IPsec traffic differs from regular IP traffic in that it most often uses UDP as its transport **protocol, rather than TCP. TCP, the** Transmission Control Protocol, sets up dedicated connections between devices and ensures that all packets arrive. UDP, the User Datagram Protocol, does not set up these dedicated connections. IPsec uses UDP because this allows IPsec packets to get through firewalls.

Decryption: At the other end of the communication, the packets are decrypted, and applications (e.g. a browser) can now use the delivered data.

What protocols are used in IPsec?

In networking, a protocol is a specified way of formatting data so that any networked computer can interpret the data. IPsec is not one protocol, but a suite of protocols. The following protocols make up the IPsec suite:

Authentication Header (AH): The AH protocol ensures that data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption; they do not help conceal the data from attackers.

Encapsulating Security Protocol (ESP): ESP encrypts the IP header and the payload for each packet — unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.

Security Association (SA): SA refers to a number of protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

Finally, while the Internet Protocol (IP) is not part of the IPsec suite, IPsec runs directly on top of IP.

IPsec has two modes, transport and tunnel mode.

IPSec Transport Mode

In transport mode, an IPSec header (AH or ESP) is inserted between the IP header and the upper layer protocol header. In this mode, the IP header is the same as that of the original IP packet except for the IP protocol field, which is changed to ESP (50) or AH (51), and the IP header checksum, which is recalculated. IPSec assumes the IP endpoints are reachable. In this mode, the destination IP address in the IP header is not changed by the source IPSec endpoint; therefore, this mode can only be used to protect packets in scenarios in which the IP endpoints and the IPSec endpoints are the same. From an IPSec VPN point of view, this mode is most useful when traffic between two hosts must be protected, rather than when traffic moves from site-to-site, and each site has many hosts. The biggest challenge when using IPSec transport mode in the site-to-site model is the complexity involved in managing IPSec protection from any given host to all

the possible peer hosts. Additionally, the two hosts' IP addresses must be routable across the entire IP routing path. Due to the complexities of building an IPSec transport mode VPN from host to host, the typical VPN will use a VPN gateway to protect all the hosts from one site to all the hosts at a peer site. A typical IPSec VPN deployment occurs between sites where each site has multiple hosts behind a VPN gateway and the IPSec tunnel endpoints serve as the VPN gateway routers. With the VPN gateway protecting a set of host IP addresses, the IPSec transport mode has limited utility. IPSec transport mode can still be used for VPN connectivity if Generic Route Encapsulation (GRE) IP tunnels are used between the VPN gateways. The GRE tunnel endpoints serve as "host" endpoints. IPSec protects the GRE tunnel traffic in transport mode.

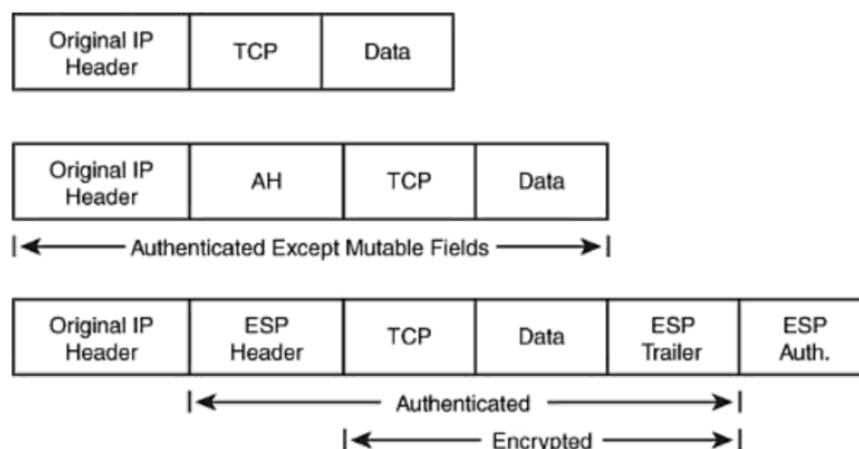


Figure 3.1 : IP packet in IPSec Transport mode

IPSec Tunnel Mode

In tunnel mode, the original IP packet is encapsulated in another IP datagram, and an IPSec header (AH or ESP) is inserted between the outer and inner headers. Because of this encapsulation with an "outer" IP packet, tunnel mode can be used to provide security services between sites on behalf of IP nodes behind the gateway router at each site.

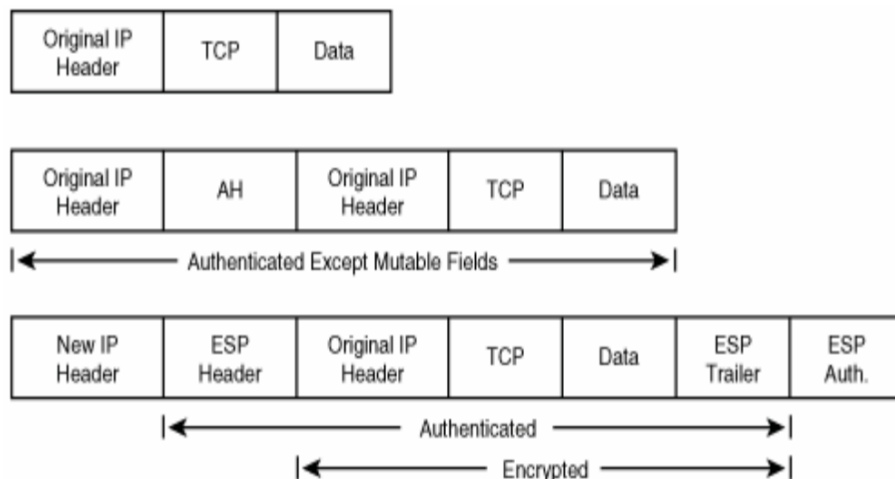


Figure 3.2 : IP packet in IPsec tunnel mode

Security Associations and IKE Operation

A security association, more commonly referred to as an SA, is a basic building block of IPsec. An SA is an entry in the SA database (SADB), which contains information about the security that has been negotiated between two parties for IKE or IPsec. There are two types of SAs:

- IKE or ISAKMP SA
- IPsec SA

Although it is common practice to use the term SA to encompass both types, it is important to make the distinction for troubleshooting purposes, because each type of SA achieves a different purpose. Both SA types are established between IPsec peers using the IKE protocol.

IKE SAs between peers are used for control traffic, such as negotiating algorithms to use to encrypt IKE traffic and authenticate peers. There is only one IKE SA between peers, and it usually has less traffic and a longer lifetime than IPsec SAs.

IPsec SAs are used for negotiating encryption algorithms to apply for IP traffic between the peers, based on policy definitions that define the type of traffic to be protected. Because they are

unidirectional, at least two IPSec SAs are needed (one for inbound traffic and the other for outbound traffic). It is possible to have multiple pairs of IPSec SAs between peers to describe unique disjoint sets of IP hosts or IP data traffic. IPSec SAs also usually have more traffic and a shorter lifetime than IKE SAs.

The establishment and maintenance of both ISAKMP/IKE SAs and IPSec SAs is a major function of the IKE protocol. The number of RFCs in the IETF IPSec working group related to key exchange and negotiation can be intimidating and confusing, as it is spread over four RFC documents: IKE (RFC 2409), ISAKMP (RFC 2408), OAKLEY (RFC 2412), and the ISAKMP Domain of Interpretation (RFC 2407). The relationships between these standards are not clearly defined in the documents themselves.

IKE operates in two phases to establish these IKE and IPSec SAs:

Phase 1 provides mutual authentication of the IKE peers and establishment of the session key. This phase creates an ISAKMP SA (a security association for IKE, sometimes referred to as an IKE SA) using a DH exchange, cookies, and an ID exchange. Once an ISAKMP SA is established, all IKE communication between the initiator and responder is protected with encryption and an integrity check that is authenticated. The purpose of IKE phase 1 is to facilitate a secure channel between the peers so that phase 2 negotiations can occur securely.

Phase 2 provides for the negotiation and establishment of the IPSec SAs using ESP or AH to protect IP data traffic.

Note

Even though we use ISAKMP and IKE interchangeably, they are different. ISAKMP defines how IPSec peers communicate, the constructs of the message exchange between the peers, and the state transitions they go through to establish their connection. ISAKMP provides the means to authenticate a peer and to exchange information for key exchange. However, ISAKMP does not define how an authenticated key exchange is done; IKE defines how the key exchange is done. [4]

3.6 Methodology

The methodology for implementing IPsec tunneling for enhanced data center security involves the following steps, executed in a simulated environment using Cisco Packet Tracer.

1. Network Design

- Define the IP addressing scheme for the data center and remote sites.
- Identify the routers that will be involved in the VPN configuration.
- Ensure proper connectivity between the sites before establishing the VPN.

2. Basic Router Configuration

- Configure interfaces with IP addresses.
- Enable necessary routing protocols (static routing protocol) for internal communication.

3. Configure IPSEC VPN

- enable security technology package
- Configure extended ACL permitting the target on each other
- Configure the IKE phase 1 ISAKMP policy on each other
- Configure the IKE phase 2 IPsec policy on each other
- Configure the crypto map

4. Set Pre-Shared Key

Define the pre-shared key for authentication.

```
crypto isakmp key YOUR_SECRET_KEY address REMOTE_IP
```

5. Configure IPSec Transform Set

Define the transform set to specify how to protect the data.

```
crypto ipsec transform-set MY_TRANSFORM_SET esp-aes esp-sha-hmac
```

6. Create Crypto Map

Create a crypto map and associate it with the transform set and remote peer.

```
crypto map MY_CRYPTOMAP 10 ipsec-isakmp
```

```
set peer REMOTE_IP
```

```
set transform-set MY_TRANSFORM_SET
```

```
match address 100
```

7. Access Control Lists (ACL)

Define an ACL to identify the traffic to be encrypted.

```
access-list 100 permit ip LOCAL_NETWORK LOCAL_SUBNET_MASK  
REMOTE_NETWORK REMOTE_SUBNET_MASK
```

8. Apply Crypto Map to Interface

Apply the crypto map to the outbound interface of the router.

```
interface INTERFACE_NAME
```

```
crypto map MY_CRYPTOMAP
```

9. Verification

Use commands like `show crypto isakmp sa` and `show crypto ipsec sa` to verify tunnel status.

Test connectivity between the sites using ping or other tools.

10. Monitoring and Troubleshooting

- Monitor the VPN tunnel for stability and performance.
- Use debug commands for troubleshooting if issues arise.

Conclusion

This methodology provides a structured approach to implementing an IPSec site-to-site VPN in a modular data center within Cisco Packet Tracer.

3.7 Result & Discussion

3.7.1 Network Design Using CISCO Packet Tracer

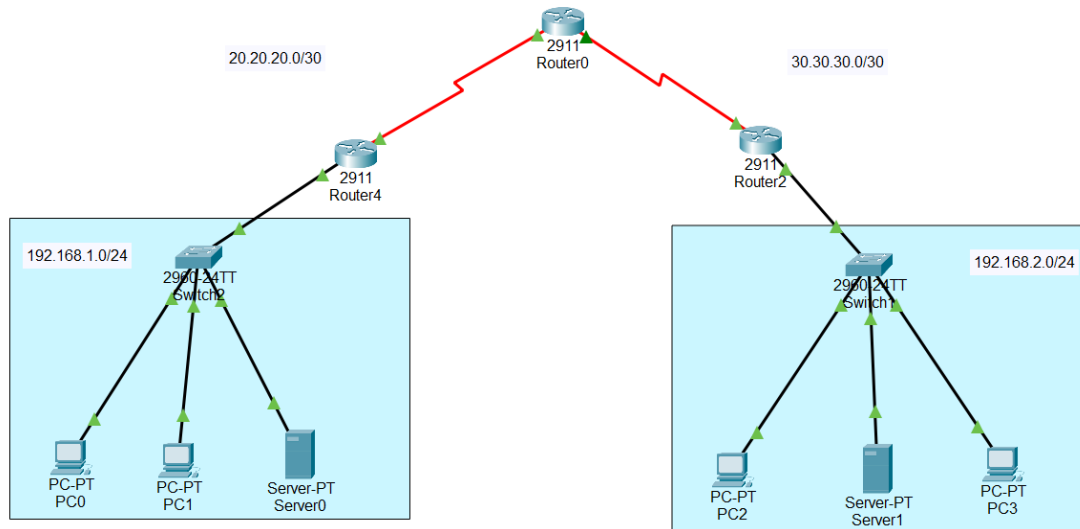


Figure 3.3 Network Design using CISCO Packet Tracer

3.7.2 IP Address planning of Design

Table 3.1 IP Address Planning

Network		
Network ID	Subnet Mask	Assigned site
192.168.1.0	/24	Site A
192.168.1.0	/24	Site B
20.20.20.0	/30	
30.30.30.0	/30	

Table 3.2: IP Address Allocation of End-Devices

	End Device	IP Address	Default Gateway	Network
Site A	PC1	192.168.1.10/24	192.168.1.1/24	192.168.1.0
	PC2	192.168.1.20/24		
	Server	192.168.1.30/24		
Site B	PC3	192.168.2.10/24	192.168.2.1/24	192.168.2.0
	PC4	192.168.2.20/24		
	Server	192.168.2.30/24		

3.7.3 Simulation Result Using CISCO Packet Tracer

Testing the Exchange of Packets between devices

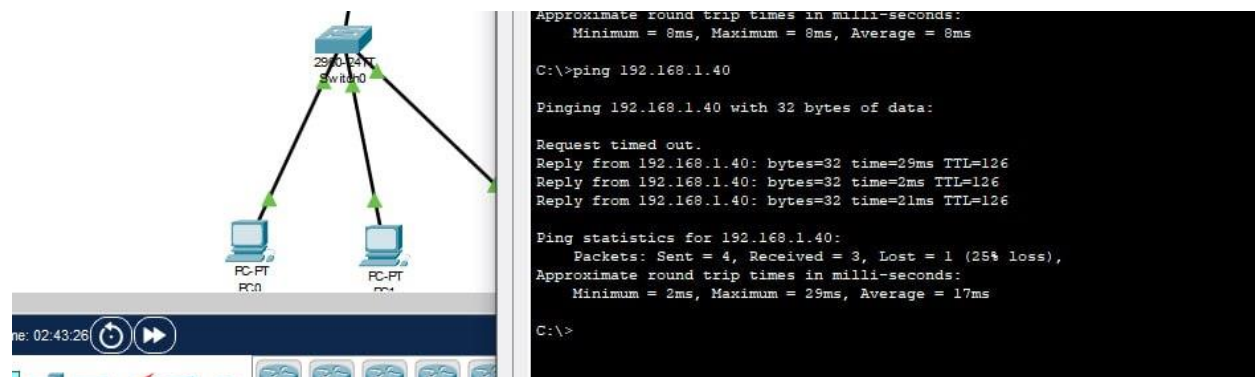
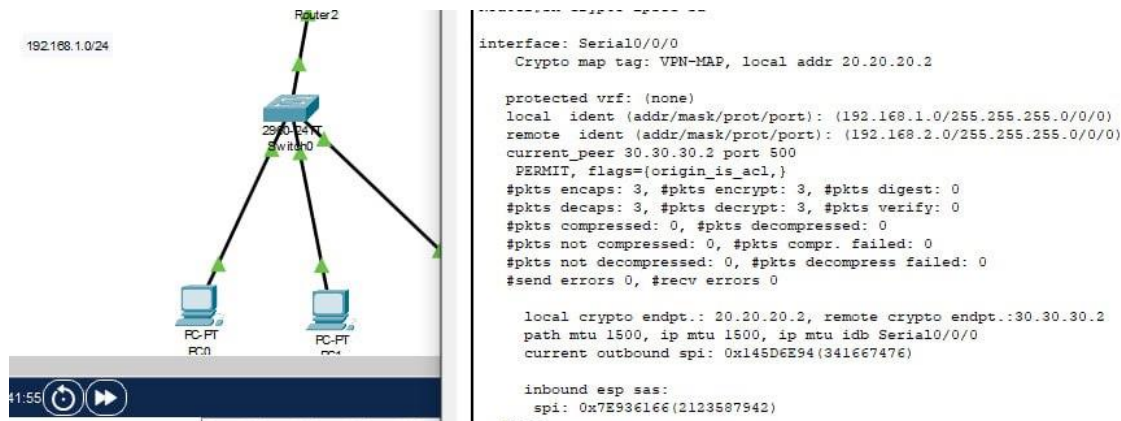


Figure 3.4 Test Reachability of between devices



Network Connectivity and VPN Tunnel Establishment

The IPsec VPN was successfully configured, and connectivity between the data center and remote sites was established. Both IKE Phase 1 and IKE Phase 2 negotiations were completed without issues, and the VPN tunnel functioned as expected. This indicates the effectiveness of the IPsec configuration, securing communications between the sites using pre-shared keys, AES encryption, and SHA-256 hashing.

Performance of Encrypted Communication

Performance testing showed minimal latency due to encryption, with a slight reduction in throughput compared to unencrypted traffic. The encryption overhead was within acceptable limits, maintaining stable performance. While encryption impacts performance, optimizations such as adjusting MTU size or faster cryptographic algorithms could further improve efficiency.

Security and Protection

Penetration testing confirmed that encrypted traffic could not be intercepted, and unauthorized access attempts were blocked. Access Control Lists (ACLs) filtered traffic effectively, allowing only authorized communication. This demonstrates that IPsec provides robust security, protecting against attacks such as packet sniffing and ensuring data confidentiality and integrity.

Scalability of the IPsec Implementation

Testing the scalability of the IPsec VPN by adding more routers and data centers proved efficient, with minimal configuration adjustments needed. The system's modular design allowed easy expansion, though managing pre-shared keys could become complex as the network grows. A transition to certificate-based authentication could simplify future scalability.

Challenges and Troubleshooting

Minor challenges, such as ACL misconfigurations and incorrect crypto map assignments, were encountered but resolved through debugging tools. This underscores the importance of accurate configuration and testing in IPsec deployments. Simulation tools like Cisco Packet Tracer helped identify issues before real-world implementation.

Chapter Four

4. Overall internship achievements and experiences

4.1 Upgrading theoretical knowledge

We have learnt a new concept that we didn't know before, which is the concept of DCN (Data Center Networking) and virtualization. It was new for us and the industry supervisors were helping us to learn new concepts, new challenging topics related to the project proposed by industry.

4.2 Practical skills Gained

It is clear and unquestionable that good practical skill is expected from an engineer. In our internship stay we have gained good practical skills in installing and troubleshooting networking equipment such as switches, cables (siemon copper and fiber optics cables) and network virtualization. In addition to this we have gained practical knowledge on data center facilities and others.

4.3 Improved Industrial problem solving capability

During our internship at ipcom technologies , we developed key problem-solving skills that enhanced our ability to tackle industrial challenges effectively. Here's a brief summary of what we gained:

- **Hands-on Experience:** We worked on real-world data center networking projects, applying theoretical knowledge to practical scenarios, and learning how to design and implement secure, scalable networks.
- **Troubleshooting Skills:** We improved our ability to identify and resolve network issues by using diagnostic tools and troubleshooting methods, ensuring optimal performance and minimal downtime.

- Collaboration: By working closely with experienced engineers, we strengthened our teamwork and communication skills, which helped us solve complex problems more efficiently.
- Adaptability: We became more flexible by learning and adapting to new technologies, tools, and methodologies, enhancing our problem-solving capabilities in dynamic environments.

These experiences equipped us with the confidence, efficiency, and technical expertise to address industrial problems successfully.

4.4 Improved team working skills

Another thing we learned throughout our internship is that teamwork has tremendous potential in overcoming any difficulty. We are all mutually reliant on one another. We worked to reach a common goal by listening to one another's thoughts, respecting one another, assisting in the understanding of various project concepts.

4.5 Improved leadership skills

This internship program has helped us on how to manage tasks and group members by observing our supervisors. From the team work we also learn how to lead our group members for every activity. we have developed skills like: -

- Building team
- Integrating team members
- Motivating team members
- Making decision
- Planning tasks

4.6 Understanding about work ethics

In the working environment there are some ethics that we have to have in the company. The work ethics we have developed in the company: -

- Obedience for manager
- Punctuality

- Honesty
- Self confidence
- Trustworthy
- Politeness
- Respectfulness

4.7 Entrepreneurship skills Gained

During our internship at ipcome technologies], we developed key problem-solving skills that enhanced our ability to tackle industrial challenges effectively. Here's a brief summary of what we gained:

- Hands-on Experience: We worked on real-world data center networking projects, applying theoretical knowledge to practical scenarios, and learning how to design and implement secure, scalable networks.
- Troubleshooting Skills: We improved our ability to identify and resolve network issues by using diagnostic tools and troubleshooting methods, ensuring optimal performance and minimal downtime.
- Collaboration: By working closely with experienced engineers, we strengthened our teamwork and communication skills, which helped us solve complex problems more efficiently.
- Adaptability: We became more flexible by learning and adapting to new technologies, tools, and methodologies, enhancing our problem-solving capabilities in dynamic environments.

These experiences equipped us with the confidence, efficiency, and technical expertise to address industrial problems successfully.

The basic entrepreneurship skills that we noted are: business planning, risk assessment, team building. A wide range of skills are seen as entrepreneurial and useful to entrepreneurs, these include both personal traits and skills:

- Communication skills and the ability to share ideas and persuade others

- The ability to work both as part of a team and independently
- Able to plan, coordinate and organize effectively
- Self-motivated and disciplined
- Innovative thinking and creativity and the ability to multitask, able to take responsibility and make decisions.

Chapter Five

5. Conclusion & Recommendation

5.1 Conclusion

This internship was really beneficial since it provided us with the opportunity to build real-life practical skills and earn work experience in addition to the academic knowledge we gained in regular studies. We gained a lot of knowledge and abilities throughout our internship by asking questions and studying our surroundings. Furthermore, we improved our interpersonal communication skills and teamwork spirit, which is an important life lesson for our future. Spending time in a work environment helped us in learning the work discipline, culture and ethics that we should reflect after we graduate and get a job. On the contrary, we have faced challenges of various forms throughout our internship period but we were able to overcome these challenges successfully which highly contributed in building our confidence and increasing our cognitive thinking ability. Furthermore, during our tenure at IPCOM Technologies, we experienced the enormous resources and infrastructure required to function as an IT and networking company. The task, the equipment, the network, and so on become more sophisticated by the day as demand rises and the system is regularly upgraded owing to new technology. Generally, from our internship experience we were able to see how the theoretical phenomenon I learnt in the regular class are related to practical applications in real life. And the development of strong teamwork skills balanced with the exercise of individual responsibility made us say that we had a successful and interesting internship experience.

5.2 Recommendation

Internship is a great way to apply the knowledge from the classroom to real-world experience. Learning is one thing, but taking those skills into the workforce and applying them is a great way to explore different career paths and specializations that suit individual interests. Therefore, we recommend the students to know internship is not time to chill, rather it is a great opportunity to learn. We recommend the students to make networks with other people. Because they may have the same interest that makes job opportunities in the future. And they have to passionately learn and practice in their company.

Reference

- [1] International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 5 Issue 2, January-February 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470 @ IJTSRD | Unique Paper ID – IJTSRD38333 | Volume – 5 | Issue – 2 | January-February 2021 Page 54: A Comparative Research on SSL VPN and IPSec VPN
- [2] K. F. Mahmmod, M. M. Azeez and M. A. Ahmed, "IPsec Cryptography for Data Packets Security within VPN Tunneling Networks Communications," *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)*, Aceh, Indonesia, 2020, pp. 1-8, doi: 10.1109/ICELTICs50595.2020.9315407.
- [3] S. Frankel, K. Kent, R. W. Ritchey, R. Lewkowski, and A. D. Orebaugh, *Guide to Ipv6 Vpns: Recommendations of the National Institute of Standards and Technology*. Createspace Independent Publishing Platform.
- [4] V. Bollapragada, M. Khalid, and S. Wainner, *IPSEC VPN design*. 2005. [Online]. Available: <https://ptgmedia.pearsoncmg.com/images/9781587051111/samplepages/9781587051111.pdf>
- [5] Arega, Kedir. (2023). Design and Implementation of an IPsec VPN Tunnel to Connect the Head Office and Branch Office of Hijra Bank. *International Journal of Systems Engineering*. 7. 9-23. 10.11648/j.ijse.20230701.12.
- [6] HCIA-Datcom V1.0 Training Material

Appendix

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ro
Router(config)#router o
Router(config)#router ospf 11
Router(config-router)#ro
Router(config-router)#router-id 2.1.2.1
Router(config-router)#ne
Router(config-router)#net
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#ne
Router(config-router)#net
Router(config-router)#network 20.20.20.0 0.0.0.3 area 0
Router(config-router)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

```
Router#
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#cr
Router(config)#crypto isa
Router(config)#crypto isakmp po
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#en
Router(config-isakmp)#encryption a
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#au
Router(config-isakmp)#authentication pr
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#ex
Router(config)#c
Router(config)#cr
Router(config)#crypto is
Router(config)#crypto isakmp key getch45 ad
Router(config)#crypto isakmp key getch45 address 20.20.20.2
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

