DECLARATION OF ORIGINALITY

NAME OF STUDENT: Bett Collins
REGISTRATION NUMBER: F17/1445/2011
COLLEGE: Architecture and Engineering
FACULTY/SCHOOL/INSTITUTE: Engineering
DEPARTMENT: Electrical and Information Engineering
COURSE NAME: Bachelor of Science in Electrical & Electronic Engineering
TITLE OF WORK: Design and implement a VPN (Virtual Private Network) for a medium office.

1) I understand what plagiarism is and I am aware of the university policy in this regard.
2) I declare that this final year project report is my original work and has not been submitted elsewhere for examination, award of a degree or publication. Where other people’s work or my own work has been used, this has properly been acknowledged and referenced in accordance with the University of Nairobi’s requirements.
3) I have not sought or used the services of any professional agencies to produce this work.
4) I have not allowed, and shall not allow anyone to copy my work with the intention of passing it off as his/her own work.
5) I understand that any false claim in respect of this work shall result in disciplinary action, in accordance with University anti-plagiarism policy.

Signature: …………………………… Date…………………………

CERTIFICATION

This report has been submitted to the Department of Electrical and Information Engineering University of Nairobi with my approval as supervisor:

Prof. M.K Mangoli

Date: …………………………………………………………………………………………….
DEDICATION

I dedicate this project to my loving mum, Florence Kirui and to my supervisor for their support and encouragement.
ACKNOWLEDGEMENTS

First and foremost, I would like to thank the Almighty God for His guidance throughout the five years of my undergraduate studies.

I would also like to acknowledge my supervisor, Prof. M.K Mangoli, for his priceless motivation, support and guidance throughout the project duration.

I extend my gratitude to all the lecturers and non-teaching staff of the Department of Electrical and Information Engineering for their contribution towards my degree.

I am also thankful to my classmates for their moral support as I did the project.
Virtual Private Networking (VPN) is a rapidly growing technology which provides secure data transmission. VPNs are an integral part of protecting company communications from unauthorized viewing, replication or manipulation. They are a vital necessity for employees who need to conduct businesses remotely in an effective and secure manner while travelling. They are also important for secure communications between the main office and branch offices. The VPN provides safe and secure communication by creating tunnels between pair of hosts.

Virtual Private network framework provides services such as: confidentiality, integrity, availability, accounting and authentication services to the packets travelling through the shared medium like the internet.

This project covers a comprehensive study of VPNs – how VPNs work, the different types of VPNs and how they are implemented. The different types of VPNs which could be implemented for a medium office include site-to-site VPN, IPsec client VPN and clientless SSL VPN. Comparisons are made among them and the most suitable one is then implemented.

**Keywords:** VPN, IPsec VPN, site-to-site VPN, clientless SSL VPN, Confidentiality, integrity, authentication, accounting.
TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION
1.1 General background........................................................................................................1
1.2 Project Objectives .........................................................................................................2
1.3 Project Goals................................................................................................................2

CHAPTER TWO: LITERATURE REVIEW
2.1 What is a VPN? ..............................................................................................................3
2.2 How a VPN works.........................................................................................................4
2.3 Types of VPN................................................................................................................5
2.4 Site-to-Site VPN...........................................................................................................5
2.5 IPsec Remote Access VPN............................................................................................7
2.6 Clientless SSL VPN......................................................................................................7
2.7 IPsec VPN Fundamentals ............................................................................................10
2.8 IPsec protocols .............................................................................................................12
2.9 IPsec modes of Operation ..........................................................................................13

CHAPTER THREE: METHODOLOGY
3.1 IPsec client VPN vs IPsec site-to-site VPN .................................................................14
3.2 Clientless SSL VPN vs IPsec client VPN .................................................................14
3.3 VPN Implementation ..................................................................................................14
3.4 Cisco packet tracer .....................................................................................................15
3.5 Network Diagram for IPsec client VPN .....................................................................17
3.6 Configuration ..............................................................................................................18

CHAPTER FOUR: RESULTS AND ANALYSIS
4.1 Testing the Remote access VPN functionality ..........................................................21

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS .....................................26

CHAPTER SIX: REFERENCES.........................................................................................27

APPENDIX
LIST OF FIGURES

Figure 2.1: Defined VPN .............................................. 4
Figure 2.2: Remote Access VPN ......................................5
Figure 2.3: Site-to-site VPN .............................................6
Figure 2.4: SSL Handshake .............................................8
Figure 2.5: IPsec negotiation process ..............................11
Figure 3.1: Packet tracer representation of company network ......16
Figure 3.2: Network diagram ..........................................17
Figure 4.1: IPsec client connection .................................21
Figure 4.2: IP configuration .........................................22
ABBREVIATIONS

VPN .................. Virtual Private Network
IPsec ................... Internet Protocol Security
SSL ...................... Secure Sockets Layer
GRE ...................... Generic Routing Encapsulation
IKE ...................... Internet Key Exchange
SA ....................... Security Association
AAA ...................... Authentication, Authorization, accounting
AH ....................... Authentication Header
ESP ...................... Encapsulation Security Payload
CHAPTER ONE

INTRODUCTION

1.1 General background

Communication play a vital role in the modern world and with the invention of internet, public data telecommunication has become cost effective and efficient. However, it is a challenge to harness this inexpensive use of this internet’s infrastructure while keeping security a top priority. The costs to a business and its reputation from stolen, manipulated or corrupted data can be devastating. Security and privacy are the major requirements for communications over the internet. The use of VPN enables companies or organizations to maintain fast, secure and reliable communications wherever their offices are located hence making VPN’s a necessity for all organizations of the modern global economy. VPN provides one of the strongest means for communication over IP network. Without adequate network security many individuals and businesses are at the risk of losing information.

Until recently, reliable communication has meant use of leased lines to maintain a Wide-Area-Network (WAN). Leased lines, ranging from ISDN (Integrated Services Digital Network, 128Kbps) to OC3 (Optical Carrier-3, 155Mbps) fiber, provided a company with a way to expand its private network beyond its immediate geographical area. A WAN has advantages over a public network, such as security, however, maintaining a WAN is expensive. Additionally, leased lines are not viable solution for organizations where workforce is highly mobile and might need to connect to corporate network remotely hence the growing importance of VPN’s.

The use of the internet, which expands day by day, increases the interest in the VPN technologies. The advantages associated with VPNs include:

- **Extended geographic connectivity** – a VPN connects remote workers to central resources, making it easier to set up global operations.
- **Improved internet security** – connection to internet makes network vulnerable to hacker attacks. VPNs solutions include firewalls and encryption measures to counteract network security threats.
- **Scalability** – A VPN allows companies to utilize the remote access infrastructure within IPSs, hence companies can virtually add unlimited amount of capacity without adding infrastructure.
- **Cost savings** – VPNs lower costs by eliminating the need for expensive long distance leased lines. A VPN needs only a relatively short connection to the internet service provider (ISP). The connection could be either a local leased line. VPN also reduces cost by reducing the long-distance telephone charges for remote access. VPN clients only need to dial up to the nearest ISP’s Access point.
1.2 Project Objectives

The main objective for this project was to establish a secure communication system for a medium-sized office with remote employees.

Since a point-to-point serial connection would not be viable, the right choice of a suitable type of VPN is crucial.

1.3 Project Goals

The goals of this project was to be able to understand the different types of VPNs, to compare them for their suitability for a medium office and to then implement the most suitable one.

The choice of a suitable type of VPN should be such that it enables travelling employees to connect and access services on the main office LAN.
CHAPTER TWO
LITERATURE REVIEW

2.1 What is a VPN?

Virtual – virtual means not real or in a different state of being. In a VPN, a private communication between two or more devices is achieved through a public network (internet). The communication is therefore virtually but not physical.

Private – private means keeping something a secret from general public. 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 – network consists of two or more devices that can freely communicate with each other. A VPN can transmit information over long distances effectively and efficiently.

Virtual Simply put, a VPN, Virtual Private Network, is defined as a network that uses public network paths but maintains the security and protection of private networks. [1]

The term VPN has been associated in the past with such remote connectivity services as the PSTN (Public Switched Telephone Network) but VPN networks have finally started to be linked with IP-based data networking. Before IP based networking, corporations had expended considerable amounts of time and resources, to set up complex private networks, now commonly called Intranets. These networks were installed using costly leased line services, Frame Relay, and ATM to incorporate remote users. For the smaller sites and mobile workers on the remote end, companies supplemented their networks with remote access servers or ISDN.

Small to medium-sized companies, who could not afford dedicated leased lines, used low-speed switched services. 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 – security. Today’s VPN solutions overcome the security factor using special tunneling 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. [6]
2.2 How a VPN works

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 PPTP (for example) after the user is authorized. 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. [6]

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

VPNs can be categorized as follows:

- Site-to-site VPN
- IPsec Remote access VPN
- Clientless SSL VPNs

2.4 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. Frame Relay, ATM, and MPLS VPNs are examples of site-to-site VPNs. [5]

There are two types of site-to-site VPNs:

- Intranet-based -- Allows a company to establish a secure connection with its remote locations.
- Extranet-based -- Allows two companies to work together via a secure connection while preventing access to their separate intranets.

One of the features of the site-to-site VPN is that hosts do not have VPN client software. Instead, they just send and receive normal TCP/IP traffic through a VPN gateway. The VPN gateway is responsible for the encryption and encapsulation of the outbound traffic. That means that there is a VPN tunnel through which communication can be established between peers over the Internet.
Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network. [6]

Basically the site-to-site VPN extends the company's network making communication easier. A good example here could be a company with branches in several remote locations.

Figure 2.3 Site-to-site VPN Tunnel: simple graphical depiction of a site-to-site VPN tunnel
2.5 IPsec Remote Access VPN

For remote access VPN connectivity with full integration into the LAN it is necessary to employ an IPsec VPN connection between a VPN Gateway and a remote client. As opposed to SSL, which operates at the application layer and is typically limited to web applications or a web portal, IPsec is a connectionless protocol that operates at Layer-3. With IPsec VPN it is possible to give the remote user full or custom access to the LAN with a user experience as if the remote user were physically connected inside the LAN. Also, it would appear to devices inside the LAN that the remote user was physically present. In other words, full network extension can be achieved. An IPsec VPN deployment is particularly necessary when the remote user needs to access applications that cannot be managed through a web portal such as an ERP or legacy software.

Although it offers more possibilities in the network, IPsec is often compared to SSL/TLS as being more complicated with increased administrative overhead. In addition to this drawback, another drawback to the IPsec Remote Access VPN approach is that the VPN client software must be installed on the remote user’s machine with administrative privileges which can hinder scalability in large scale deployments. [8]

Another challenge with IPsec VPNs can be navigating through firewalls and NAT devices that are situated between the client and the gateway. (Matei 2012) Thankfully there are tools available that can help resolve these challenges, such as NAT Traversal. Cisco’s implementation of this option is called Easy VPN Server and it is the one we chose to implement for this project. [8]

2.6 Clientless Secure Sockets Layer (SSL) VPN

By far the easiest form of VPN to implement from an end-user perspective is the clientless Secure Sockets Layer (SSL) VPN. After a remote user opens up their web browser and is successfully authenticated against a Cisco IOS SSL VPN Gateway (or other SSL VPN gateway) they are able to access web services running in their home office LAN through their browser.

Some remote services that are available via a clientless SSL VPN connection are “web servers, 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.” [12]

It is important to note that generally speaking, a clientless SSL VPN cannot be considered a permanent replacement for an IPsec client VPN or site-to-site VPN. This is due to the fact that clientless SSL VPNs typically don’t support applications such as Telnet, SNMP, ping, traceroute, FTP and IP Telephony that can’t be run through web browsers. [1] One solution to this problem is to create a SSL Tunnel VPN with a web browser. These options will be discussed in a later section.
Secure Sockets Layer (SSL) protocol

The SSL protocol was originally developed by Netscape as a way to provide secure transmission of information between a server and the company’s browser. This was done in part to try and strengthen the ability of e-commerce companies to provide their online shoppers with a safe and reliable experience.

The SSL protocol is implemented at the Transport Layer and upwards in the seven layer Open Systems Interconnection (OSI) network model. In contrast to IPsec, the layer 3 (source and destination IP address) information is not encrypted. The entire secure communications process between client and server is quite complex but can be broken down into a nine-step process. This handshake process is quite similar when using TLS. [12]

Figure 2.4 SSL Handshake: graphical depiction of the 9-step client/server Handshake

IBM’s
IBM’s WebSphere online portal, which is the source of the graphic handshake procedure representation above, also provides a short summary of the SSL handshake procedure as follows:

1) “The SSL or TLS client sends a "client hello" message that lists cryptographic information such as the SSL or TLS version and, in the client's order of preference, the Cipher Suites supported by the client. The message also contains a random byte string that is used in subsequent computations. The protocol allows for the "client hello" to include the data compression methods supported by the client.

2) The SSL or TLS server responds with a "server hello" message that contains the Cipher Suite chosen by the server from the list provided by the client, the session ID, and another random byte string. The server also sends its digital certificate. If the server requires a digital certificate for client authentication, the server sends a "client certificate request" that includes a list of the types of certificates supported and the Distinguished Names of acceptable Certification Authorities (CAs).

3) The SSL or TLS client verifies the server's digital certificate.

4) The SSL or TLS client sends the random byte string that enables both the client and the server to compute the secret key to be used for encrypting subsequent message data. The random byte string itself is encrypted with the server's public key.

5) If the SSL or TLS server sent a "client certificate request", the client sends a random byte string encrypted with the client's private key, together with the client's digital certificate, or a "no digital certificate alert". This alert is only a warning, but with some implementations the handshake fails if client authentication is mandatory.

6) The SSL or TLS server verifies the client's certificate.

7) The SSL or TLS client sends the server a "finished" message, which is encrypted with the secret key, indicating that the client part of the handshake is complete.

8) The SSL or TLS server sends the client a "finished" message, which is encrypted with the secret key, indicating that the server part of the handshake is complete.

9) For the duration of the SSL or TLS session, the server and client can now exchange messages that are symmetrically encrypted with the shared secret key.”

Unfortunately, even the SSL protocol cannot be considered entirely secure at this point, as its encryption mechanisms appear to have been cracked by the National Security Agency (NSA) in the US. According to Mike Janke, the C.E.O. of the encrypted-communications company Silent Circle, “N.S.A. developed a massive push-button scale ability to defeat or circumvent SSL encryption in virtually real time.”
2.7 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. [9] 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. [9]

*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). The implementation is divided into two phases.

**IKE Phase 1**
The first SA is created during IKE Phase 1 and is essentially a control channel. The purpose of the first phase is to establish a secure and authenticated channel that will allow secure Phase 2 negotiations to take place. [8] It also authenticates the peers.

It works at 2 modes:

- Main mode (three two-way exchanges)
- Aggressive mode

The main difference between these two is that aggressive mode will pass more information in fewer packets, with the benefit of slightly faster connection establishment.

During the first step of phase 1 the following parameters are negotiated as policy sets:

- Encryption – (DES, 3DES, AES)
- Hash – (MD5, SHA-1)
- Authentication – (Pre-shared keys, RSA signatures, RSA encrypted nonce)
- Diffie-Hellman group
- Lifetime

Once the policy set is negotiated, the second step of Phase 1 occurs when the Diffie-Hellman protocol is run in order to establish the shared keys. These shared keys will be retained and used in subsequent encryption algorithms and hashes.
The last step in IKE Phase 1 is to authenticate the peers using the negotiated hash algorithm and the shared keys obtained in the DH exchange.

**IKE Phase 2**

The purpose of IKE Phase 2 is to negotiate and establish SAs that will protect the IP traffic. The negotiation takes place over the control channel that is created in Phase 1 and the newly established shared keys from Phase 1 may also be used here. Unlike in Phase 1, the SAs in Phase 2 are unidirectional so two must be created, one in each direction. The IPsec tunnel terminates when the IPsec SAs are deleted, or when their lifetime expires.

**IKE Versions**

The IKE process as previously explained is unique to IKE version 1. There is also now an IKE version 2 in use. It is very similar to IKE version 1 but has improved on some of the challenges that were inherent in version IKEv1 and the process has been streamlined a bit. Some of the more notable differences in IKEv2 are:

- Negotiation is shorter.
- It is reduced to only one phase. Child SAs are created inside this phase
- eliminating the need for a second phase.
- NAT Traversal is built in. This feature solves some of the challenges with
- NAT/PAT that were mentioned earlier.

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

**Figure 2.5 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 51. 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, which is protocol 50, is defined in rfc4303. 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
- 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. The ESP transport mode is not with the Network Address Translation (NAT), since communication is end-to-end or between hosts.

Tunnel mode

The tunnel mode gives protection to data and the source IP packet. This original IP packet is encrypted and it is also encapsulated with a new IP packet.
CHAPTER THREE
METHODOLOGY

The three types of Remote access VPNs that can be implemented for a middle size office are:

1. IPsec Site-to-site VPN
2. IPsec client VPN
3. Clientless SSL VPN

The three will be analyzed and the most suitable among the three will be implemented for this case.

3.1 IPsec client VPN vs IPsec site-to-site VPN

The most important difference between the two is the question of mobility. The site-to-site option is stationary whereas the remote access IPsec VPN option allows for connectivity from anywhere with an internet connection.

The nature of site-to-site option between stationary routers makes mobility an impossibility. For this case we would need employees to be able to connect while travelling hence the IPsec client VPN option is a better solution.

3.2 Clientless SSL VPN vs IPsec client VPN

An IPsec client VPN requires a VPN client software to be installed at the client’s endpoint so as to be used in connecting to the main office servers. A clientless SSL VPN however uses any web browser to connect to the main office servers.

The problem with the SSL VPNs however is that they don’t support applications that can’t be run through web browsers such as ping.

Legacy software run by the company may also not be successfully adapted to a web browser and will not function correctly when accessed through a clientless SSL VPN setup.

Hence the most suitable implementation would be a remote access IPsec VPN.

3.3 VPN Implementation

The devices which are be needed to implement a remote access IPsec VPN should include following:
1. A cisco router
2. A DSL modem
3. A switch

However, at the time of doing this project the above materials could not be obtained from the department. I could not also manage to purchase them myself as they are expensive (i.e. a cisco router for example goes for over Ksh. 50,000).

I therefore resorted to implementation by use of simulation using the Cisco packet tracer software.

3.4 Cisco packet tracer

This is a cross-platform visual simulation program designed by Cisco systems that allows users to create network topologies and imitate computer networks.

Packet tracers allows students to design complex and large networks which is often not feasible with physical hardware, due to costs.

Consider a company with its network as shown in the following diagrammatic representation [cisco packet tracer used]
Figure 3.1 – packet tracer representation of a company network
3.5 Network diagram for the IPsec Client VPN

Figure 3.2 – network diagram

The above network shows a remote company employee connecting to the office router using a DSL modem.

To enable the secured connection by the remote user, the company edge router has to be configured to create the IPsec remote access VPN.
3.6 Configuration

To implement the IPsec remote access VPN in the cisco packet tracer, the command line interface (CLI) was used to enter the VPN commands into the office router.

CLI was also used to configure the other devices in the office, such as the switches, ISP router, etc.

Bulk of configurations however was on the office router as this is where the VPN was configured. The basic summary of the commands used in configuration is provided here with an accompanying short explanation of what it does.

In the appendix the detailed commands used in configuration are provided.

`aaa authentication login REMOTE local`
- This command creates the aaa authentication login user

`aaa authorization network REMOTE local`
- This command sets up the group network login
- The AAA authentication and authorization are used with the local database.

*Username VPN secret bett8746*
- This creates a user with username ‘VPN’ and secret password ‘bett8746’

`crypto isakmp policy 10`
`encryption aes 256`
`hash md5`
`authentication pre-share`
`group 2`
`lifetime 21600`
`exit`
- Defines ISEKMP policy for phase 1 negotiations.
- Sets encryption to advanced encryption standard using 256-bit key
Also sets the integrity checking mechanism (hashing) to hash md5

**Crypto isakmp client configuration group REMOTE**

*key CISCO*

*pool MYPOOL*

*exit*

- Defines the crypto isakmp group policy
- It sets the pool of ip addresses that are handed out to VPN client when they connect

**Crypto IPSec transform-set MYSET esp-aes 256 esp-md5-hmac**

- Configuration for the IPSec policies and transform sets used during IPSec negotiation
- Sets encryption to aes-advanced encryption standard and a 256-bit key
- Sets hashing to hash md5-hmac

**crypto dynamic-map DYNAMAP 10**

*set transform-set MYSET*

*reverse-route*

- Creates a dynamic map and a sequence number of 10
- The second line of command ties it to the transform-set MYSET

**crypto map CLIENT_MAP client authentication list REMOTE**

**crypto map CLIENT_MAP isakmp authorization list REMOTE**

**crypto map CLIENT_MAP client configuration address respond**

**crypto map CLIENT_MAP 10 IPSec-isakmp dynamic DYNAMAP**

- Setting up the actual crypto map itself
- Sets client authentication list and isakmp authorization list to REMOTE
- Line 3 above is a command that will respond to the network address request from client
- Line 4 ties the crypto map to the dynamic map DYNAMAP
ip local pool MYPOOL 172.16.10.150 172.16.10.200
  ➢ Creates the pool MYPOOL

interface fastEthernet 0/1

crypto map CLIENT_MAP
  ➢ This command turns on the ISAKMP

Ip dhcp pool REMOTE_POOL

    network 72.44.20.0 255.255.255.240

    default-router 72.44.20.14

    dns-server 10.10.10.1

  ➢ This sets up an ip dhcp pool for the modem connection
  ➢ This will be assigning dynamic ip addresses to the remote user
CHAPTER FOUR
RESULTS AND ANALYSIS

4.1 Testing the Remote Access VPN functionality

Verification and testing of the IPsec Remote Access VPN connection was achieved through the following:

- Using the VPN client software on the Cisco packet tracer
- Using the commands ‘show crypto isakmp sa’ and ‘show crypto IPsec sa’ which are entered onto the packet tracer’s CLI (command line interface)

Figure 4.1 IPsec client connection – confirms connection for remote user to the office router
Figure 4.2 - shows that the remote user is assigned an IP address in local LAN ip pool.
When the command prompt is used and the command `ipconfig /all` is entered, the following is seen:

**Figure 4.2 – ip configuration**

![Image of Command Prompt showing ip configuration]

This shows there is a tunnel interface created.

The other verification was using the command line interface to enter the following commands:

*Show crypto isakmp sa*

The results obtained were as shown below:

```
R1>en
R1>enable
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
    dst   src  state       conn-id slot status
    72.44.20.1 72.44.20.14   QM_IDLE 1078    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

This shows that there is an active tunnel from the remote user end to the office router.
Show crypto IPsec sa

When the above command is executed the following is obtained:

R1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: CLIENT_MAP, local addr 72.44.20.14
    protected vrf: (none)
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (172.16.10.150/255.255.255.255/0/0)
    current peer 72.44.20.1 port 500
    PERMIT, flags=(origin_is_acl,)
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 72.44.20.14, remote crypto endpt.: 72.44.20.1
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
    current outbound spi: 0x3C390185(1010368901)

    inbound esp ses:
        spi: 0x29D01ADE(701504222)
        transform: esp-aes 256 esp-md5-hmac
        in use settings = (Tunnel, )
        conn id: 2002, flow_id: FPGA:1, crypto map: CLIENT_MAP
        sa timing: remaining key lifetime (k/sec): (4525504/1435)
        IV size: 16 bytes
        replay detection support: N

    inbound ah ses:

    inbound pcc ses:

    outbound esp ses:
        spi: 0x3C390185(1010368901)
        transform: esp-aes 256 esp-md5-hmac
        in use settings = (Tunnel, )
        conn id: 2003, flow_id: FPGA:1, crypto map: CLIENT_MAP
        sa timing: remaining key lifetime (k/sec): (4525504/1435)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

    outbound ah ses:

    outbound pcc ses:
When the remote user was used to browse into the corporate intranet the following was seen:

![Web Browser Image]

Hence it is possible to access the internal web server of the office from the remote location.
CHAPTER FIVE
CONCLUSION AND RECOMMENDATIONS

Virtual Private Networks are a vital part of remote user communications across the internet due to the risks that exist when sending private information over a public internet. With the increase in online theft and hijacking of sensitive data by anonymous hackers, VPNs proves to be an effective means of securing a business’s data and therefore safeguarding reputation.

Apart from the above benefit, the importance associated with VPNs is also of so much help to businesses. VPNs have advantages such as cost savings, extended geographical connectivity and scalability which are all of great importance efficiency in running businesses.

When choosing a particular type of VPN for a business it is important to consider suitability of the VPN for that business as well as the costs to be incurred in implementation. The different types of VPNs are each suited for different types of businesses i.e. small-sized business, medium-sized business of large businesses. For our case it was a medium-sized business.

The objectives and goals of the project were thus achieved. However, the following recommendations would be of great importance for future purposes.

- Procurement of advanced Cisco routers in the department to enable actual real life implementation of the VPNs
- The department should partner with the Cisco academy so that the students can get acquainted with VPN technology.
CHAPTER SIX

REFERENCES


Switch, SW1 configuration using the packet tracer CLI (command line interface)

Switch#enable
Switch#conf t
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname SW1
SW1(config)#interface range fastEthernet 0/23 - 24
SW1(config-if-range)#
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
SW1(config-if-range)#
SW1(config-if-range)#^Z
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#wr
Building configuration...
[OK]
SW1#
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#
SW1(config)#vtp mode ?
  client   Set the device to client mode.
  server   Set the device to server mode.
  transparent  Set the device to transparent mode.
SW1(config)#vtp mode server
Device mode already VTP SERVER.
SW1(config)#
SW1(config)#vtp domain CISCO
Changing VTP domain name from NULL to CISCO

%SYS-5-CONFIG_I: Configured from console by console

SW1#wr
Building configuration...
[OK]
SW1#
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vlan 10
SW1(config-vlan)#vlan name SALES
SW1(config-vlan)#conf t
  SW1(config-vlan)#vlan 10
SW1(config-vlan)#name SALES
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name MANAGEMENT
SW1(config-vlan)#exit
SW1(config)#vlan 30
SW1(config-vlan)#name SERVERS
SW1(config-vlan)#
SW1(config-vlan)#exit
SW1(config)#^Z
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1(config)#interface range fa
SW1(config)#interface range fastEthernet 0/1 - 20
SW1(config-if-range)#swit
SW1(config-if-range)#switchport mode
SW1(config-if-range)#switchport mode acc
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switch
SW1(config-if-range)#switchport acces
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#^Z
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#wr
Building configuration...
[OK]
SW1#
Switch, SW2 configuration using the packet tracer CLI (command line interface)

SW2>enable
SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.

SW2(config)#interface range fa
SW2(config)#interface range fastEthernet 0/1 -9
SW2(config-if-range)#
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 30
SW2(config-if-range)#exit
SW2(config)#
SW2(config)#interface range fastEthernet 0/10 - 20
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 40
% Access VLAN does not exist. Creating vlan 40
SW2(config-if-range)#exit
SW2(config)#
SW2(config)#int
SW2(config)#interface range fa
SW2(config)#interface range fastEthernet 0/1 - 9
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
SW2(config-if-range)#exit
SW2(config)#
SW2(config)#interface range fastEthernet 0/10 - 20
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 30
SW2(config-if-range)#
SW2(config-if-range)#^Z
SW2#
%SYS-5-CONFIG_I: Configured from console by console

SW2#wr
Building configuration...
[OK]
SW2#show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/21, Fa0/22, Fa0/23</td>
</tr>
<tr>
<td>10 SALES</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>20 MANAGEMENT</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9</td>
</tr>
<tr>
<td>30 SERVERS</td>
<td>active</td>
<td>Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20</td>
</tr>
<tr>
<td>40 VLAN0040</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>active</td>
<td></td>
</tr>
</tbody>
</table>
1004 fddinet-default       active
1005 trnet-default         active

SW2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

SW2(config)#no vlan 40

SW2(config)#

SW2(config)#exit

SW2#

%SYS-5-CONFIG_I: Configured from console by console

SW2#show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/21, Fa0/22, Fa0/23</td>
</tr>
<tr>
<td>10 SALES</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>20 MANAGEMENT</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/5, Fa0/6, Fa0/7, Fa0/8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/9</td>
</tr>
<tr>
<td>30 SERVERS</td>
<td>active</td>
<td>Fa0/10, Fa0/11, Fa0/12, Fa0/13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/14, Fa0/15, Fa0/16, Fa0/17</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/18, Fa0/19, Fa0/20</td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>active</td>
<td></td>
</tr>
</tbody>
</table>
Router, R1 configuration

R1>enable
R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fa
R1(config)#interface fastEthernet 0/0
R1(config-if)#no ip add
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation do
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip add
R1(config-subif)#ip address
% Incomplete command.
R1(config-subif)#end
R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
%SYS-5-CONFIG_I: Configured from console by console

[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R1(config)#int
R1(config)#interface fa
R1(config)#interface fastEthernet 0/0
R1(config-if)#no ip add
R1(config-if)#no ip address
R1(config-if)#no shut
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#exit
R1(config)#interface fa
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.16.10.254 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 172.16.11.30 255.255.255.224
R1(config-subif)#exit
R1(config)#
R1(config)#interface fa
R1(config)#interface fastEthernet 0/0.30

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
R1(config-subif)#encapsulation dot
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.16.11.45 255.255.255.240
%SYS-5-CONFIG_I: Configured from console by console

R1#wr
Building configuration...
[OK]
R1#
R1#sho ip int br

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method Status</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>unassigned</td>
<td>YES unset up</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/0.10</td>
<td>172.16.10.254</td>
<td>YES manual up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/0.20</td>
<td>172.16.11.30</td>
<td>YES manual up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/0.30</td>
<td>172.16.11.45</td>
<td>YES manual up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Vlan1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
</tbody>
</table>
Remote access VPN configuration on router R1

R1(config)#aaa authen
R1(config)#aaa authentication ?
   enable   Set authentication lists for enable.
   login    Set authentication lists for logins.
   ppp      Set authentication lists for ppp.
R1(config)#aaa authentication login ?
   WORD     Named authentication list.
   default  The default authentication list.
R1(config)#aaa authentication login REMOTE local
R1(config)#
R1(config)#aaa authorization network REMOTE local
R1(config)#username VPN secret bett8746
R1(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
R1#
R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#crypto isakmp pol
R1(config)#crypto isakmp policy ?
   <1-10000>  Priority of protection suite
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#
R1(config-isakmp)#hash ?
   md5  Message Digest 5
   sha  Secure Hash Standard
R1(config-isakmp)#hash md5
R1(config-isakmp)#
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 21600
R1(config-isakmp)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#wr

R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#crypto isa
R1(config)#crypto isakmp client confi
R1(config)#crypto isakmp client configuration gr
R1(config)#crypto isakmp client configuration group REMOTE
R1(config-isakmp-group)#key CISCO
R1(config-isakmp-group)#pool MYPOOL
R1(config-isakmp-group)#exit
R1(config)#crypto ipsec transform-set MYSET esp-a
R1(config)#crypto ipsec transform-set MYSET esp-aes 256 esp-m
R1(config)#crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac
R1(config)#
R1(config)#crypto dy
R1(config)#crypto dynamic-map DYNAMAP 10
R1(config-crypto-map)#
R1(config-crypto-map)#set transform-set MYSET
R1(config-crypto-map)#rev
R1(config-crypto-map)#reverse-route
R1(config-crypto-map)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#cry
R1(config)#crypto ma
R1(config)#crypto map CLIENT_MAP client auth
R1(config)#crypto map CLIENT_MAP client authentication list REMOTE
R1(config)#crypo
R1(config)#cryp
R1(config)#crypto map CLIENT_MAP isa
R1(config)#crypto map CLIENT_MAP isakmp auth
R1(config)#crypto map CLIENT_MAP isakmp auth
R1(config)#crypto map CLIENT_MAP clien
R1(config)#crypto map CLIENT_MAP client auth
R1(config)#crypto map CLIENT_MAP isa
R1(config)#crypto map CLIENT_MAP isakmp auth
R1(config)#crypto map CLIENT_MAP isakmp authorization list
R1(config)#crypto map CLIENT_MAP isakmp authorization list REMOTE
R1(config)#cry
R1(config)#crypto map CLIENT_MAP cli
R1(config)#crypto map CLIENT_MAP client confi
R1(config)#crypto map CLIENT_MAP client configuration add
R1(config)#crypto map CLIENT_MAP client configuration address ?
   respond  Respond to network address requests from the client
R1(config)#crypto map CLIENT_MAP client configuration address respond
R1(config)#crypto map CLIENT_MAP 10 ip
R1(config)#crypto map CLIENT_MAP 10 ipsec-isakmp dy
R1(config)#crypto map CLIENT_MAP 10 ipsec-isakmp dynamic DYNAMAP
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#ip local pool
   % Incomplete command.
R1(config)#ip local pool MYPOOL 172.16.10.150 172.16.10.200
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#int
R1(config)#interface fa
R1(config)#interface fastEthernet 0/1
R1(config-if)#cryp
R1(config-if)#crypto map CLIENT_MAP
R1(config-if)#
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]

R1#show crypto isa
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status

IPv6 Crypto ISAKMP SA

R1#
R1#show crypto ips
R1#show crypto ipsec sa

No SAs found