The Libyan Academy



School of Applied Science and Engineering

Department of Electrical and Computer Engineering

Using secure Cisco network to prevent sniffing threats and IP spoofing attacks

By:
Masoud Emhemed Ahmed Aljedek

A Thesis submitted to the Department of Electrical and Computer Engineering

In partial Fulfillment of Requirements Master of Science.

Supervised By:
Dr. Abobaker Mohamed Elhouni

2016 ,Libya

Acknowledgement

I would like to express my sincere appreciation Dr. Abobaker Mohamed Alhouni , who was my supervisor and has given me tremendous advices throughout my studies and in the preparation of this thesis.

My thanks to all Staff and faculty of the department of Electrical Engineering and Computer of Libyan Academy.

On the personal side, I would like to thank my Family for support.

Also, I would like to thank my friends and Students who through their positive criticisms and contributions provided useful information for the successful completion of this work.

Preface

This research was in partial Fulfillment for the Degree of Master of Science at the Department of Electrical and Computer Engineering Section of Computer Engineering and Information Technology at Libyan Academy, Libya.

The research was performed under the supervision of Dr. Abobaker Mohamed Alhouni at Libyan Academy, May, 2016.

Abstract

The issue of security in computer network and the Internet has been a major challenge. Hackers and unauthorized users like Sniffers and Spoofers have been compromising user's information by a way of getting access to such information. It is a well-known fact that information is very vital to individuals and organization these days; hence the need to protect our data and information from unauthorized users.

In this thesis, a better understanding to Cisco network with secure routing such as researched to analyze the behavior of Cisco Routers based Firewall, Dual-Homed, Dual-Host, Dual Screened, DMZ, VLAN and VPN architectures by using intense Sniffing and Spoofing traffic.

OPNET simulation process for different scenarios for network security, were implemented and analyzed.

At last, the conclusion was made: by adding different security measures to router, protecting it against possible attacks, and increasing the network security, Dual-Homed Host is very secure to against External attacks, Screened Subnet (DMZ) is much protected from Spoofing Attacks and Sniffing Threats, because we have a Demilitarized Zone (DMZ), VPN is High security, because just encrypted packets would Tunnel Destination and it need to decryption at Destination With VLAN Technique Internal Attacks were Decreased.

Table of Contents

	Title	Page
	CHAPTER ONE	
Introduction		
1.1	Introduction…….....	1
1.2	Background …….....	2
1.3	Literature Review…….....	3
1.4	Problem Statement …….....	5
1.5	Problem Solution…….....	5
1.6	Document Overview……...	6
	CHAPTER TWO	
Network Security Threats		
2.1	Introduction…….....	7
2.2	Sniffing Threats…….....	7
2.2.1	The types of Ethernet environments'…….	8
2.2.2	Types of sniffing……...	11
2.3	Spoofing Attack…….....	15
2.3.1	IP Spoofing…….....	16
2.3.2	Types of Spoofing ……	18
	CHAPTER THREE	
Technologies Of Network Security		
3.1	System and network technology…….	24
3.1.1	Network Security ……	24
3.1.2	Developments in Network Security……..	26
3.1.3	Cisco Secure Network……..	26
3.2	Firewall Protection…….....	27
3.2.1	Classification of Firewalls Technologies……	29
3.2.2	Firewall Architectures……..	33
3.3	Virtual Private Networks (VPN) ……...	40
3.3.1	Advantages of VPNs……	42
3.3.2	Types of VPNs…….....	43
3.3.3	VPN Architectures…….....	43

3.3.4 VPN Models…… 50
3.3.5 Firewalls and VPNs……. 55

CHAPTER FOUR

Virtual LANs

4.1 Introduction…… 57
4.2 VLAN Membership……... 59
4.3 Extent of VLANs……... 61
4.4 VLAN Trunking…… 62
4.4.1 Inter-Switch Link (ISL) …….. 63
4.4.2 IEEE 802.1Q…… 64
4.5 VLAN Trunking Protocol (VTP) …… 64
4.5.1 VTP Modes…….. 65
4.5.2 Server Mode…… 66

CHAPTER FIVE

Simulation

5.1 Simulation Tools…… 68
5.2 Firewalls Simulation……..... 68
5.3 VPN Simulation…….. 77
5.4 Dual-Homed Router and Host Simulation……... 84
5.5 Screened Host / Subnet (DMZ) Simulation……. 87
5.6 VLANS Simulation…….. 93
5.7 The Libyan Academy scenario…… 98

CHAPTER SIX

Conclusions And Future Work

6.1 Conclusion…… 106
6.2 Future Work……. 108

References……. 109

List of Figures

No.	Title	Page
2. 1	Shared Ethernet	9
2. 2	Switched Ethernet	10
2. 3	Passive sniffing	12
2. 4	Active sniffing	13
2.5	Valid source IP address	16
2.6	Spoofed source IP address	17
2.7	Blind Spoofing	19
2.8	A Normal TCP Connection Request from A to B	21
2.9	Half-Open TCP Connection	21
2.10	Link state before RIP attack	23
2.11	Link state after RIP attack	23
3. 1	A Firewall-controlled access from the Internet	29
3. 2	Classification of Firewall Technologies	29
3. 3	Perimeter networks	33
3. 4	Dual-Homed Host Firewall	35
3. 5	Dual-Homed Host Firewall architecture	35
3. 6	Screened Host Firewall	37
3. 7	Screened Host Firewall architecture	37
3. 8	Screened Subnet Firewall	39
3. 9	Screened Subnet Firewall architecture	39
3. 10	Tri-Homed Host	40
3.11	Tunnel creation process for Layer 2 VPNs	45
3.12	PPTP VPN components	48
3.13	PPTP packet format	47
3.14	L2F VPN components	48
3.15	L2F packet format	48
3.16	L2TP VPN components	49
3.17	L2TP packet format	49
3.18	NAS-initiated L2TP VPN model	51
3.19	Client-initiated L2TP VPN model	53
3.20	Firewalls providing authorized access to two networks	56
3.21	VPN tunnel between two firewalls	56

4.1	Virtual LANs	58
4.2	Static VLANs	59
4.3	Dynamic VLANs	60
5.1	Firewall scenarios	70
5.2	Time Average in IP DB Query Responsewith Fire wall and without Firewall	73
5.3	Time Average in IP DB Query Traffic (Sent & Received)	73
5.4	Time Average in HTTP page Response with Fire wall and without Firewall	74
5.5	Time Average in HTTP Traffic (Sent & Received)with Fire wall and without Firewall	74
5.6	Time Average in Email Traffic (Sent & Received)with Fire wall and without Firewall	75
5.7	Time Average in Email (Download & Upload)with Fire wall and without Firewall	75
5.8	Time Average in IP Broadcast Traffic Received	76
5.9	Time Average in IP Broadcast Traffic Sent	76
5.10	VPN scenario For Libyan Academy Branches	79
5.11	VPN scenario For Internal Side of Libyan Academy – Tripoli Branch	79
5.12	Dual-Homed Router and Host Scenario	86
5.13	Screened Host	89
5.14	Screened Subnet With DMZ	91
5.15	ping from External Station #1 to Internal Server #2 with Ping Pattern	92
5.16	change the default route of Internal Station #1 pointing to 190.30.30.1	93
5.17	VLAN scenario	95
5.18	Email Downloaded / Upload and average Ftp Download /Upload	96
5.19	Switch A Traffic forwarded / Received and average in Switch A Traffic forwarded / Received	97
5.20	Switch B Traffic forwarded / Received and average in Switch B Traffic forwarded / Received	97
5.21	Switch C Traffic forwarded / Received and average in Switch C Traffic forwarded / Received	98
5.22	The Libyan Academy scenario Architecture	99

5.23	The Libyan Academy scenario Simulation	100
5.24	Main Branch **(**Tripoli) Simulation	100
5.25	Mesurata Branch Simulation	101
5.26	Bengazi Branch Simulation	101
5.27	DB Jitter	103
5.28	DB Packet end to end delay	103
5.29	DB Traffic Received (packet/sec)	104
5.30	Traffic Send (packet/sec**)**	104
5.31	Traffic Forwarded (bits/ sec) with VLAN and without VLAN	105
5.32	average point- to – point delay (sec)	105

List of Tables

No.	Title	Page
5.1	Supported Services	71
5.2	Servers Profiles	81
5.3	Ping response times(VPN)	83
5.4	Network components (Dual Homed Router Host)	85
5.5	Ping's success (Dual-Homed Router and Host)	87
5.6	Components of Screened Network	89
5.7	Comparison between Effect Firewall and VPN on DBQoS	104
6.1	The parametric security of (Dual-Homed and Dual-Homed Host)	107
6.2	The parametric security of (Screened Host and Screened DMZ).	107

List of Abbreviations

Symbol	Description
ARP	Address Resolution Protocol
CWSI	Works For Switched Internetworks
DMZ	Demilitarized Zone
DNS	Domain Name System
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IEEE	Institute Of Electrical Nnd Electronics Engineers
IMAP	Internet Message Access Protocol
IP Sec	Internet Protocol Security
ISL	Inter-Switch Link
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Logical Control Protocol
NCP	Network Control Protocol
NNTP	Network News Transfer Protocol
OSI	Open Systems Interconnection
POP	Post Office Protocol
QOS	Quality of Service
RIP	Routing Information Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
Telnet	Terminal emulation protocol
VLAN	Virtual local area network
VMPS	Virtual Membership Policy Server
VPN	virtual private network
VTP	Virtual Trunking Protocol

1.1. Introduction

The first common terms in network security are the Threats, people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses. The Attacks and the threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the end points, such as servers and desktops.

New threats to networked computers appear almost daily. There are a number of basic threats, which can be categorized based on the goals and purposes of the attacks. Certain threats specifically target the packet while it is in the route. Sniffing is one of these threats that are monitoring the data over network; Spoofing is type of attacks that are fooling the hosts to obtain information by appearing to be a legitimate entity.

To prevent the threats and attacks we should identify the risks to the network resources and data. The intent of a risk analysis is to identify the components of the network, evaluate the importance of each component, and then apply an appropriate level of security. This analysis helps to maintain a workable balance between security and required network access.

Cisco Network security refers to all the measures, software and hardware implementations that together protect the integrity and privacy of information flow. A network security focuses on controlling the network traffic and usage. There are many techniques for providing network security such as Packet Filtering that protect the packets from the threats.

1.2. Background

In order to send and receive data across the Internet networks, protocols to govern these operations are needed. The principle method of communication is the TCP/IP; which transmit the data as packets. Packets are composed of two basic components: A header portion that contains the necessary information to route the packet and a payload portion that contains the data. Each Internet packet on the Internet carries a destination address and a return address. Normal network applications provide legitimate source addresses.

TCP/IP protocol suite is not perfect. There exist a number of serious security flaws inherent in the protocol design in most of TCP/IP implementation. It does not generate or maintain stat information about the packets during delivery. The network attackers just utilize these security holes to perform various network attacks.

Several types of network attacks have been found, each of them utilizes one or more security vulnerabilities in the TCP/IP protocol specification or some well-known weakness in the implementations of TCP/IP.

1.3. Literature Review

- Obunadike Georgina and Tyokyaa K. Richard from Federal University Dutsinma , Nigeria, Department of Mathematical Sciences and IT, Presented research with title " Optimization of Computer Network for Efficient Performance " [1] in 2015.

- Rajni Ranjan Singh and Deepak Singh Tomar from Maulana Azad National Institute of Technology, Bhopal, India, Presented research with title " Network Forensics: Detection and Analysis of Stealth Port Scanning Attack " [2] in 2014, proposed system correctly identifies crafted scans injected into real traffic.

- Dr. Abdul-Bary R. Sulaiman and Omar Kh. Salih Alhafidh from College of Electronic Engineering, Computer and Information Dep. University of Mosul , Iraq, Presented research with title " Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering " [3] in 2014 , studying the Performance measures such as delay variation, delay, page response time, throughput, and packet drop for different types of traffics in their movement using OPNET modeler simulation.

- Hussein A. Mohammed and Adnan Hussein Ali from Electrical & Electronics Engineering Techniques College – Baghdad, Presented research with title" Effect of some Security Mechanisms on the QOS VoIP Application using OPNET " [4] in 2013, studying the effect some of the Security Mechanisms on the VoIP Qos. In this work, simulation tool OPNET Modeler version 14.0 is used to implement the

proposed network (VoIP Network). The proposed network is a private network for a company with two locations.

- Mohammad Z. Ahmad, Mustafa I. Akbas, Damla Turgut from University of Central Florida Baghdad, Presented research with title" Design and development of a simulation environment in OPNET using High Performance Computing " [5] in 2013, studying How to simulate environment and the generation of initial simulations where data can be gathered that depicts some of the trade-offs needed to make intelligent decisions regarding the design and deployment of simulation federations.

- An Engineer Sparsh Mittal, Department of Electronics and Communications From Indian Institute of Technology, Presented research with title" OPNET: An Integrated Design Paradigm for Simulations " [6] in SEPTEMBER 2012, He survey and review prominent fields where OPNET has been applied and compare it with other existing simulators.

- Some of Engineers of Computer department of BUID University, UAE, Dubai Presented research with the title " Sniffing Attacks Prevention and Detection Techniques in Wired and Wireless Local Area Networks (LAN) " [7] in 2011, in this research, evaluated the most famous security solutions and classifying them according to their efficiency against detecting or preventing the types of Address Resolution Protocol [ARP] Spoofing attacks.

1.4. Problem Statement

The threats to computer networks appear almost daily. There are a number of threats, which can be categorized based on the goals and method of the attacks.
The Attacks and the threats use a variety of tools, scripts, and programs to launch attacks on networks. Certain threats specifically target the packet while it is in the route. Sniffing is one of these threats that are monitoring and cache the data over network if it is not encrypted ; Spoofing is type of attacks that are fooling the hosts to obtain data on the networks .

1.5. Problem Solution

To prevent sniffing and spoofing with Cisco technology we should identify the risks to the network components and apply an appropriate level of security of Cisco routers of our network by make control access to block malicious packets of attacker and Apply Proxy to disable all interested services and programs probably used from some sniffers .

Also, configure VPN between the branches to encrypt all data traveling on network that the sniffers can catch it and restrict Telnet Access and SNMP ports if no need to use.

Also, divide internal network users to separate LANs depending on (Services, Departments to limitation possibility of access)by Configuring VLAN technology.

1.6. Document Overview

The rest of this document is outlined as follows:

Chapter two presents the Types of Network Security Threats that infect the packet when computers are connected in network environment these types cover Sniffing and Spoofing.

Chapter three covered the Technologies of Network Security (Firewall & VPN).

Chapter four I discussed The Technology of VLAN s and presented VLAN types and protocols.

Chapter Five presented the Simulation of Network Security and covered the implementation and analysis of results.

In the **final chapter**, we discussed the result, drew conclusion and recommended areas for future research.

2.1. Introduction

Threats to the security of computer networks have been issue since computer began to be used widely by the general public. Nowadays, any computer or network that is connected to the Internet is at risk. In this chapter we will focus on threats that infect the packet while it is in the router.

2.2. Sniffing Threats

A sniffer is program and/or device that monitor data traveling over a network. Sniffer can be used for legitimate activities, e.g. network management, as well as for illegitimate activities, e.g. stealing information found on a network. Sniffers are available for several platforms, both commercial and open source variations. Some of the simplest packages use a command line interface and dump captured data onto the screen, while sophisticated ones use GUI and graph traffic statistics; they can also track multiple sessions, and offer several configuration options [8].

Network utilization and monitoring programs often use sniffers to gather data necessary for metrics and analysis. It is important to note, however, that sniffers do not generally intercept or alter captured data.

The sniffer works through Ethernets most common way of networking computers. A computer connected to the LAN has two addresses. One is the MAC address that uniquely identifies each node in a network and stored on the

network card itself. The MAC address is used by the Ethernet protocol while building “frames” to transfer data to and from a system. The other is the IP address. This address is used by the applications. The data link Layer uses an Ethernet header with the MAC address of the destination machine rather than the IP address. The Network layer is responsible for mapping IP network addresses of the MAC address as required by the data link Protocol. It initially looks for the MAC address of the distinction machine in a table, usually called the ARP cache. If no entry found for the IP address, an ARP broadcast of a request packet goes out to all machines on the local sub-networks. The machine with that particular address responds the source machine with its MAC address. This MAC address then added to the source machines ARP cache. The source machine, in all its communications with the destination machine, then uses this MAC address.

2.2.1. The types of Ethernet environments’

There are two basic types of Ethernet environments’, and sniffers work slightly differently in both these environments.

The two types of Ethernet environments are:

- **Shared Ethernet:**

In a shared Ethernet environment, all hosts are connected to the same bus and complete amongst each other for bandwidth. In this environment, all the other machines receive packets meant for one machine. Thus, when machine 1 wants to talk to machine 2 as shown in Fig(2.1) , it sends a packet out on the

network with the destination MAC address of machine 2 along with its own source MAC address. The other machines in the shared Ethernet (machine 3 and machine 4) compare the frames destination MAC address with their own, if they do not match, the frame is discarded. However, a machine running a sniffer ignores this rule and accepts all frames. Sniffing in a shared Ethernet environment is totally passive and hence difficult to detect.

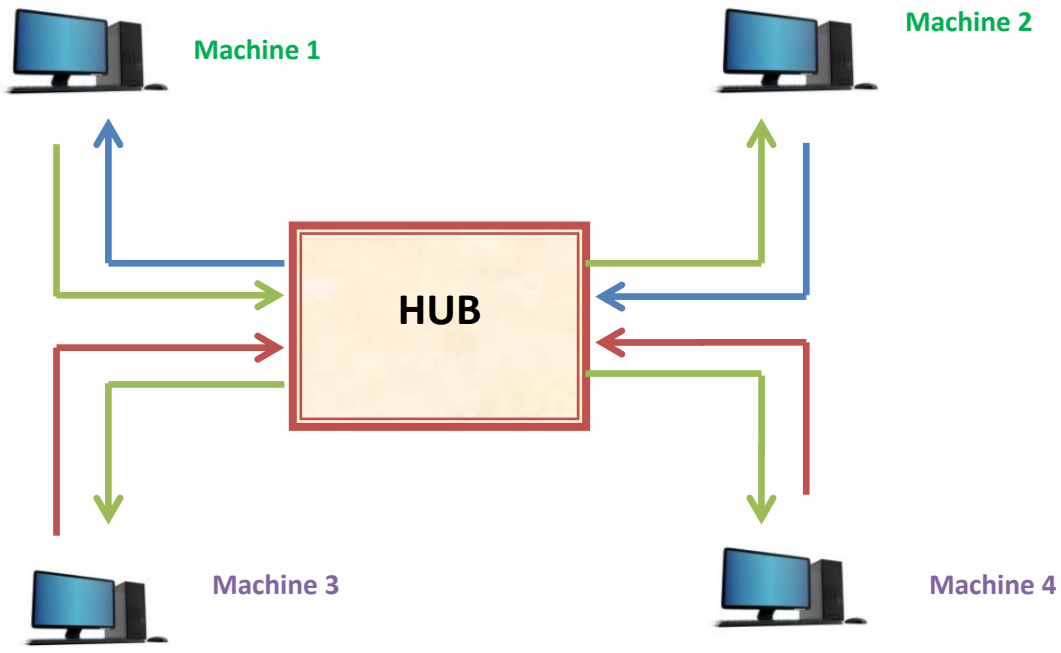


Figure (2.1)-Shared Ethernet

- **Switched Ethernet:**

An Ethernet environment in which the hosts are connected to a switch instead of a hub is called a switched Ethernet. The switch maintains a table keeping track of each computer's MAC address, and the physical port on which that MAC address is connected, and delivers packets destined for a particular machine.

The switch is a device that sends packets the destined computer only and does not broadcast it to all the computers on the network. This results in better utilization of the available bandwidth and improved security. Hence, the process of putting the machine NIC into promiscuous mode to gather packets does not work.

As a result, many people think that switched networks are totally secure and immune to sniffing. However, this is not true. Though the switch is more secure than a hub, sniffing the network is possible using the modules as following:

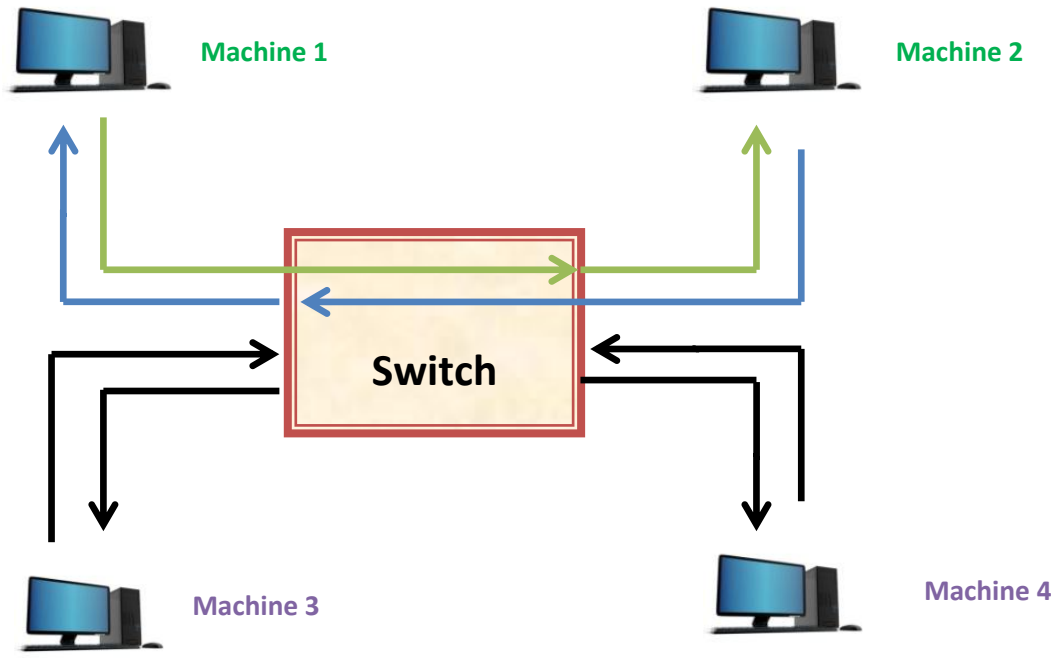


Figure (2.2)-Switched Ethernet

2.2.2. Types of sniffing

There are two types of sniffing:

- **passive sniffing:**

In passive sniffing, as a sniffer gathers packets at the Data Link layer, it can potentially grab all the packets on the LAN of the machine running the sniffer program. This is because a network with a hub implements a broadcast medium shared by all systems on the LAN. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. If an attacker runs a sniffer on one system on the LAN. He can gather data sent to and from any other system on the LAN. The majority of sniffer tools are ideally suited to sniff data in a hub environment. These tools are called passive sniffers because they passively wait for the data to be sent before capturing it. These sniffers are efficient at silently gathering data from the LAN.

In passive sniffing, the intruder gets access to the network by any of the following methods:

- By compromising the physical security.
- Using a Trojan horse.

Trojans can be used as a carrier to install sniffers on the target machine. For instance, the back orifice server has a plug-in known as "Butt Trumpet" that the attacker after installation of the server. Once the attacker recognizes that the victim's system has been compromised, he can then install a packet sniffer and use it to sniff the network.

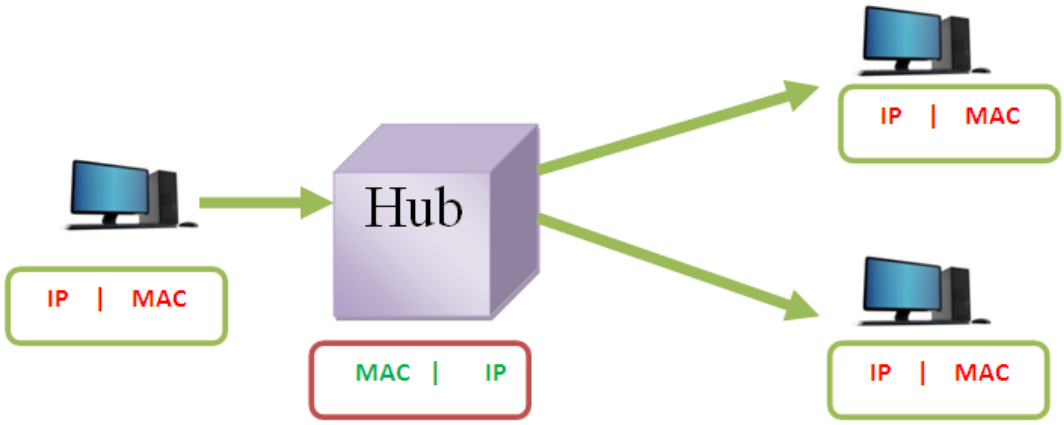


Figure (2.3)- Passive sniffing

A packet sniffer is seldom the only tool used for an attack. This is because a sniffer can only work it a common collision domain. Common collision domain is the sector of the network that is not attacked by the hub. In that sector, all devices can watch traffic that is not switched or bridged. As a sniffer gathers packets at the data link layer, it can potentially grab all packets on the LAN of the machine running the sniffer program.

- **Active sniffing:**

One countermeasure against passive sniffing is to replace the network hub with a switch. Unlike a hub-based network, switched Ethernet does not broadcast all information (other than actual broadcast or multicast packets) to all systems on the LAN. The switch regulates the flow of data between its ports by

actively monitoring the MAC address on each port, which assists it in passing data only to its intended target.

The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping. In addition, a switch looks at the MAC address associated with each frame passing though it and sends the data to the required port.

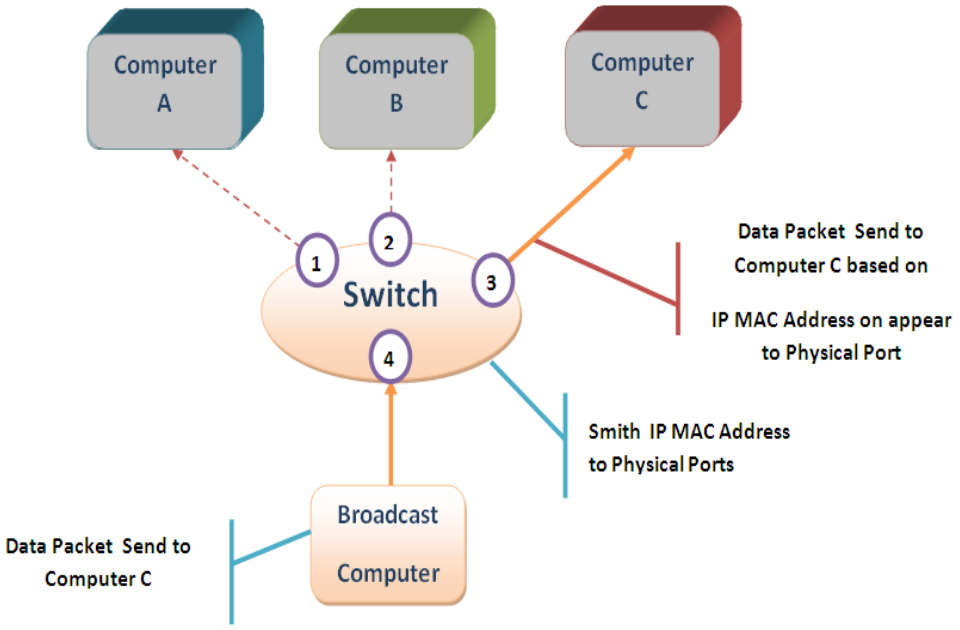


Figure (2.4)-**Active sniffing**

This switch thereby, limits the data that a passive sniffer. If there is a passive sniffer can gather and If it is activated on a switched LAN, the sniffer will be able to see data going to end from one machine to another than an actual broadcast or multicast packet.

Switched networks have been developed to accomplish the necessity of more band width, not for the necessity of secure networks. Since the evolution was not driven by security needs, there are ways to circumvent this network posture and sniff the traffic.

The sniffers for a switched LAN actively inject traffic into the LAN enable sniffing of the traffic. This is what is known as "active sniffing" ,and the methods used in this attack include:

- ARP Spoofing.
- MAC Flooding.
- MAC Duplicating.

2.3. Spoofing Attacks

The basic protocol for sending data over the Internet network and many other computer networks is the Internet Protocol (IP). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response.

Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. It should come as no surprise .then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques. IP spoofing is one of the most common forms of on-line camouflage. In IP spoofing , an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by spoofing the IP address of that machine.

In certain cases, it might be possible for the attacker to see or redirect the response to his own machine. The most usual case is when the attacker is spoofing an address on the same LAN or WAN.

2.3.1. IP Spoofing

In computer networking, the term of IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.

In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system. In essence, the attacker is fooling (spoofing) the distant computer into believing that ,They are a legitimate member of the network.

The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system [9].

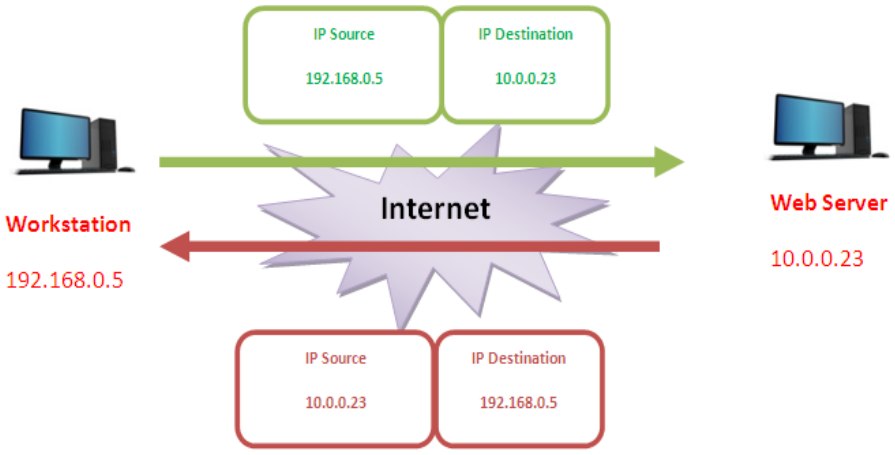


Figure (2.5) -Valid source IP address

In this Figure Valid source IP address, illustrates a typical interaction between a workstation with a valid source IP address requesting web pages and the web server executing the requests. When the workstation requests a page from the web server the request contains both the workstation's IP address (i.e. source IP address 192.168.0.5) and the address of the web server executing the request (i.e. destination IP address 10.0.0.23). The web server returns the web page using the source IP address specified in the request as the destination IP address, 192.168.0.5 and its own IP address as the source IP address, 10.0.0.23.

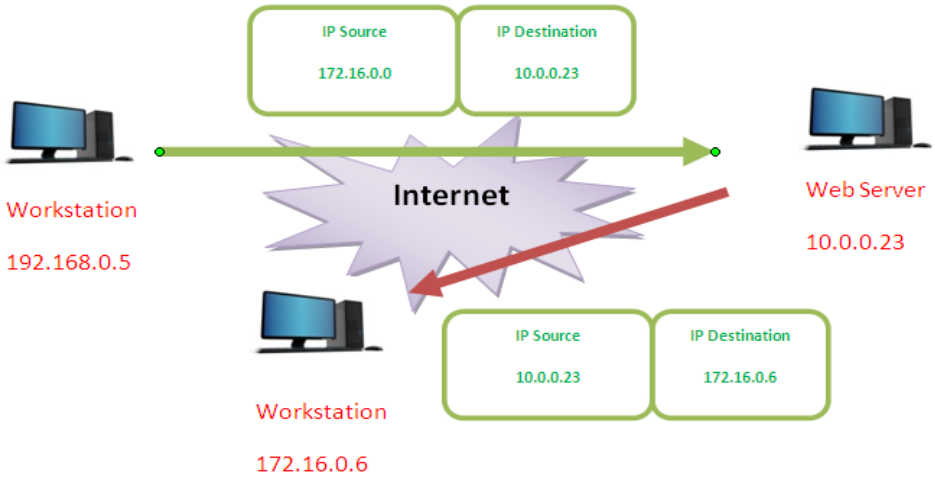


Figure (2.6) - Spoofed source IP address

In this Figure Spoofed source IP address, illustrates the interaction between a workstation requesting web pages using a spoofed source IP address and the web server executing the requests. If a spoofed source IP address (i.e. 172.16.0.6) is used by the workstation, the web server executing the web page request will attempt to execute the request by sending information to the IP address of what it believes to be the originating system (i.e. the workstation at

172.16.0.6). The system at the spoofed IP address will receive unsolicited connection attempts from the web server that it will simply discard [10].

2.3.2. Types of Spoofing

There are a few variations on the types of attacks that successfully employ IP spoofing. Although some are relatively dated, others are very pertinent to current security concerns.

- **Non-Blind Spoofing**

This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be calculated, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the DataStream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using the spoofing, the attacker interferes with a connection that sends packets along the subnet.

- **Blind Spoofing**

This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days.

Usually the attacker does not have access to the reply, abuse trust relationship between hosts. For example: Host C sends an IP datagram with the address of some other host (Host A) as the source address to Host B. Attacked host (B) replies to the legitimate host (A) shows in Fig (2.7) [10].

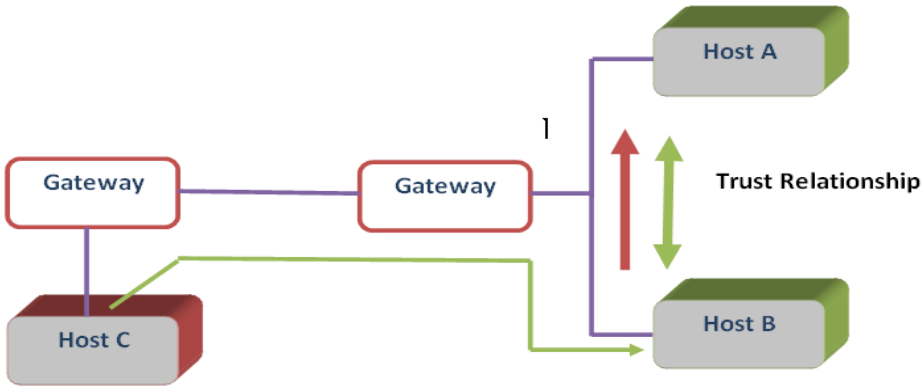


Figure (2.7)- Blind Spoofing

- **Hijacking an Authorized Session**

An attacker who can generate correct sequence numbers can send a reset message to one party in a session informing that party that the session has ended. After taking one of the parties' offline, the attacker can use the IP address of that party to connect to the party still online and perform a malicious act on it. The attacker can thus use a trusted communication link to exploit any system vulnerability.

Keep in mind that the party that is still online will send the replies back to the legitimate host, which can send a reset to it indicating the invalid session, but by that time the attacker, might have already performed the intended actions. Such

actions can range from sniffing a packet to presenting a shell from the online host to the attacker's machine [11].

- **Man in the Middle Attack**

Both types of spoofing are forms of a common security violation known as a man in the middle (MIM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by “spoofing” the identity of the original sender, who is presumably trusted by the recipient.

- **Denial of Service Attack**

The connection setup phase in a TCP system consists of a three-way handshake. This handshake is done by using special bit combinations in the "flags" fields. If host A wants to establish a TCP connection with host B, it sends a packet with a SYN flag set. Host B replies with a packet that has SYN and ACK flags set in the TCP header. Host A sends back a packet with an ACK flag set, finishing the initial handshake. Then hosts A and B can communicate with each other, as shown in Fig (2.8).

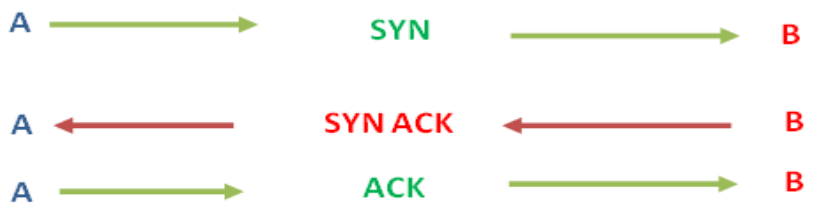


Figure (2.8) - A Normal TCP Connection Request from A to B

The three-way handshake must be completed in order to establish a connection. Connections that have been initiated but not finished are called half-open connections. A finite size data structure is used to store the state of the half-open connections. An attacking host can send an initial SYN packet with a spoofed IP address, and then the victim sends the SYN-ACK packet and waits for a final ACK to complete the handshake. If the spoofed address does not belong to a host , then this connection stays in the half-open state indefinitely, thus occupying the data structure. If there are enough half-open connections to fill the state data structure, then the host cannot accept further requests, thus denying service to the legitimate connections in this Fig (2.9).



Figure (2.9)-Half-Open TCP Connection

IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against – denial of service attacks. Since crackers are concerned only with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions.

Rather, they wish to flood the victim with as many packets as possible in a short amount of time. In order to prolong the effectiveness of the attack, they spoof source IP addresses to make tracing and stopping the denial of service attacks as difficult as possible.

When multiple compromised hosts are participating in the attack, all sending spoofed traffic; it is very challenging to quickly block traffic.

- **Attacks Concerning the Routing Protocols**

A host can send spoofed RIP packets in order to "inject" routes into a host. This is easy to implement, it only requires IP/UDP spoofing. On a LAN with RIPv2 passwords have to be used for updating routes, but plaintext passwords are used and the plaintext passwords can be sniffed.

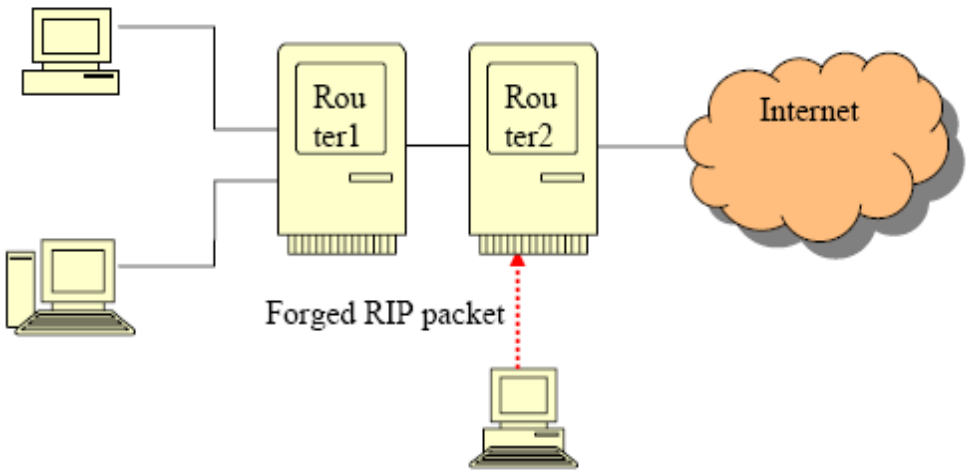


Figure (2.10) - Link state before RIP attack [10].

Attacker sends a forged RIP packet router 2 (Fig 2.10) and says it has the shortest path to the network that router1 connects. Then all the packets to that network will be routed to attacker (Fig 2.11). The attacker can sniff the traffic.

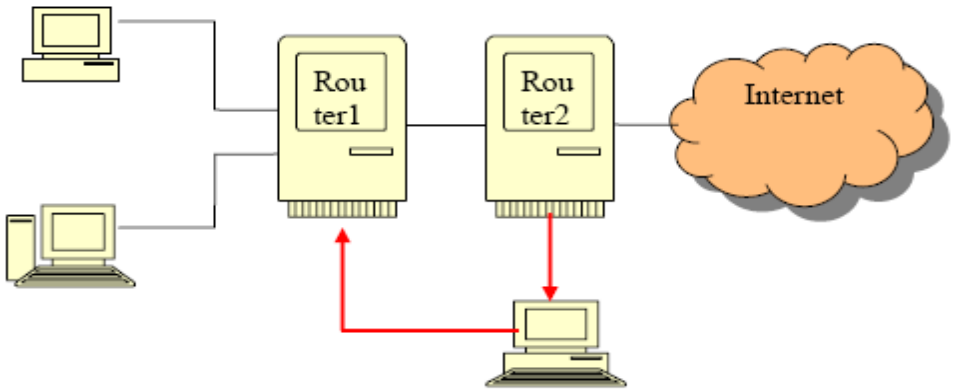


Figure (2.11) - Link state after RIP attack [10].

3.1. System And Network Technologies.

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet.

There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses" planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

Internet threats will continue to be a major issue in the global World as long as information is accessible and transferred across the Internet Different defense and detection mechanisms were developed to deal with these attacks.

3.1.1. Network Security

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

There exists a “communication gap” between the developers of security technology and developers of networks.

Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development.

The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed process. There isn’t a methodology to manage the complexity of security requirements.Secure network design does not contain the same advantages as network design [12].

When considering network security, it must be emphasized that the whole network is secure.Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack.
A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered

1- Access – authorized users are provided the means to communicate to and from a particular network
2- Confidentiality – Information in the network remains private
3- Authentication – Ensure the users of the network are who they say they are.

4- Integrity – Ensure the message has not been modified in transit

5- Non-repudiation – Ensure the user does not refute that he used the network

3.1.2. Developments in Network Security

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems.

1-Hardware Developments

Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely impacting security.

2- Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, VPN, intrusion detection, and much more [13].

3.1.3. Cisco Secure Network

Effective network security demands an integrated defense-in-depth approach. The first layer of a defense-in-depth approach is the enforcement of the fundamental elements of network security. These fundamental security elements form a security baseline, creating a strong foundation on which more advanced methods and techniques can subsequently be built.

The Cisco Security Framework (CSF) is a security operational process model aimed at ensuring network, and service, availability and business continuity. Security threats are an ever-moving target and the CSF is designed to identify current threat vectors, as well as track new and evolving threats, through the use of best common practices and comprehensive solutions [13].

The CSF is built upon two fundamental objectives, under the premise that one cannot control what one cannot see or measure :

•Gain Total Visibility

•Identify, monitor, and correlate system-wide events

•Assure Complete Control

Harden network infrastructure, isolate hosts and services, and enforce security policies.To achieve this total visibility and complete control, multiple technologies and capabilities are used throughout the network to gain visibility into network activity, enforce network policy, and address anomalous traffic. Network infrastructure elements such as routers and switches are leveraged as pervasive, proactive policy monitoring and enforcement agents [14].

3.2. Firewall Protection

Firewall is a necessity in most corporations. For most of these corporations, the Internet is the virtual backbone of their enterprise network, interconnecting an organization’s corporate network and those of its business partners and customers. The Internet also provides an inexpensive way to link branch offices, telecommuters, and mobile workers to the corporate network. Unfortunately، linking a corporate network to the Internet exposes it to the outside world.

This protection is provided by implementing appropriate network access control policies and using firewalls to enforce them. A firewall is a security system that controls access to a protected network, such as a private corporate network. The network is being protected from an untrusted public network, such as the Internet. As a result, a firewall is located so that every access request from a public network to the protected network must pass through the firewall, eliminating the need for individual protection of every server and host in the protected network.

The permits of firewall to provide authentication and other security services to remote users in order to prevent unauthorized users from logging in to the network [12].

For a firewall to be effective, Organizations first need to define their network security policy. A network security policy identifies the resources that need protection and the threats against them. It then defines how they can be used and who can use them, and stipulates the actions to be taken when the policies are violated.

A policy is a set of rules against which arriving packets are tested. Examples of such rules include what IP traffic the organization wants to allow into its network, what source addresses should be excluded from the network, and what destination addresses within the network can be accessed from outside the network. Specifications to be taken include accept packet and reject packet. The firewall is responsible for filtering traffic according to the security policy.

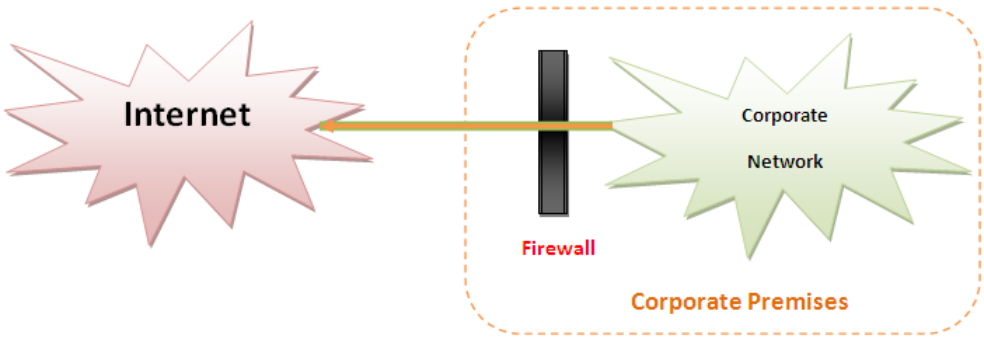


Figure (3. 1) - Firewall-controlled access from the Internet.

3.2.1. Classification of Firewalls Technologies.

Firewalls can be classified into three basic Technologies: packet filters, proxy servers (which include application gateways and circuit-level gateways), and stateful packet filters [15].

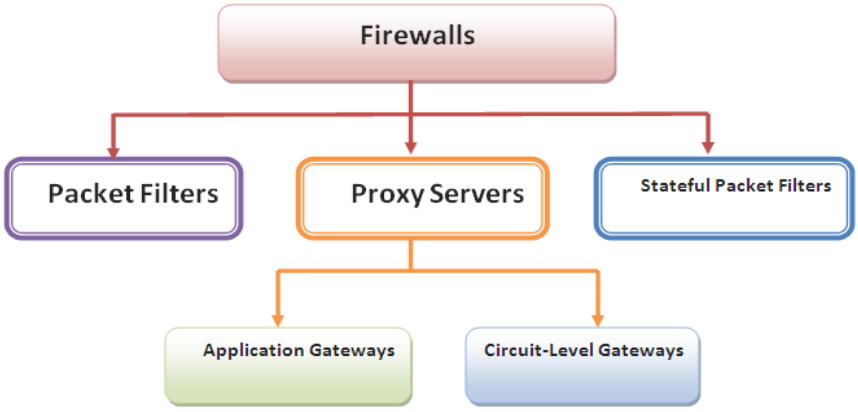


Figure (3.2) -Classification of Firewall Technologies.

1- Packet Filters

A packet filter is a firewall that inspects each packet for user-defined filtering rules to determine whether to pass or block it. For example, the filtering rule might require all Telnet requests to be dropped. Using this information, the

firewall will block all packets that have a port number 23(the default port number for Telnet) in their header. Filtering rules can be based on source IP address, destination IP address, Layer 4 (that is, TCP/UDP) source port, and Layer 4 destination port. Thus, a packet filter makes decisions based on the network layer and the transport layer.

Packet filters are fast and can be easily implemented in existing routers. Unfortunately, they are the least secure of all firewalls. One disadvantage of packet filters is that they have no logging facility that can be used to detect when a break-in has occurred. Also, a packet filtering firewall grants or denies access to the network according to the source and destination addresses and the source and destination ports. Unfortunately, these ports can be spoofed. As a result, anyone can access network resources once access has been granted to an authorized user.

2- Proxy Servers

A proxy service is an application that redirects users' requests to the actual services based on an organization's security policy. All communication between a user and the actual server occurs through the proxy server. Thus, a proxy server acts as a communications broker between clients and the actual application servers. Because it acts as a checkpoint where requests are validated against specific applications, a proxy server is usually processing intensive and can become a bottleneck under heavy traffic conditions.

Proxy servers can operate at either the application layer or the transport layer. Thus, there are two classes of proxy servers: application gateways, which operate at the application layer; and circuit-level gateways, which operate at the transport layer.

- **Application Gateways**

An application gateway is a proxy server that provides access control at the application layer. It acts as an application-layer gateway between the protected network and the entrusted network. Because it operates at the application layer, it is able to examine traffic in detail; therefore, it is considered the most secure type of firewall. It can prevent certain applications, such as FTP, from entering the protected network. It can also log all network activities according to applications for both accounting and security audit purposes.

Application gateways can also hide information. Since all requests for services in the protected network pass through the application gateway, it can provide network address translation (or IP address hiding) functionality and conceal IP addresses in the protected network from the Internet by replacing the IP address of every outbound packet (that is, packets going from the protected network to the Internet) with its own IP address.

Network address translation also permits unregistered IP addresses to be freely used in the protected network because the gateway will map them to its own IP address when the users attempt to communicate with the outside world.

- **Circuit-Level Gateways**

A circuit-level gateway is a proxy server that validates TCP and UDP sessions before allowing a connection or circuit through the firewall. It is actively involved in the connection establishment and does not allow packets to be forwarded until the necessary access control rules have been satisfied.

A circuit-level gateway is not as secure as an application gateway because it validates TCP and UDP sessions without full knowledge of the applications that use these transport services. Moreover, once a session has been established, any application can run across that connection. This behavior exposes the protected network to attacks from intruders. Unlike a circuit-level gateway, an application gateway can differentiate the applications that need to be blocked from those that can be allowed to pass-through the gateway.

3- Stateful Packet Filters

Although the application gateway provides the best security among the preceding firewalls, its intensive processing requirement slows down network performance.

A stateful packet filtering gateway attempts to provide tight security without compromising performance. Unlike the application gateway, it checks the data that passes through at the network layer but does not process it.

The firewall maintains state information for each session, where session states include a combination of communication phase and the endpoint application state. When a stateful packet filtering gateway receives data packet, it checks the packet against the known state of the session. If the packet deviates from the expected session state, the gateway blocks the rest of the session.

3.2.2. Firewall Architectures

Firewall architecture refers to the manner in which firewall components are arranged to provide effective protection against unauthorized users. It is usually defined after the network security policy has been defined because it is supposed to be a model that enforces the security policy.

The network security policy is enforced at defensible boundaries within the network called perimeter networks. A corporate network usually contains multiple perimeter networks that can be classified into three groups: the outermost perimeter network, one or more internal perimeter networks, and the innermost perimeter network.

The outermost perimeter network provides a boundary between corporate resources (that need to be protected) and external resources (resources the corporation cannot control). Internal perimeter networks represent boundaries within the corporate network that need additional security [16].

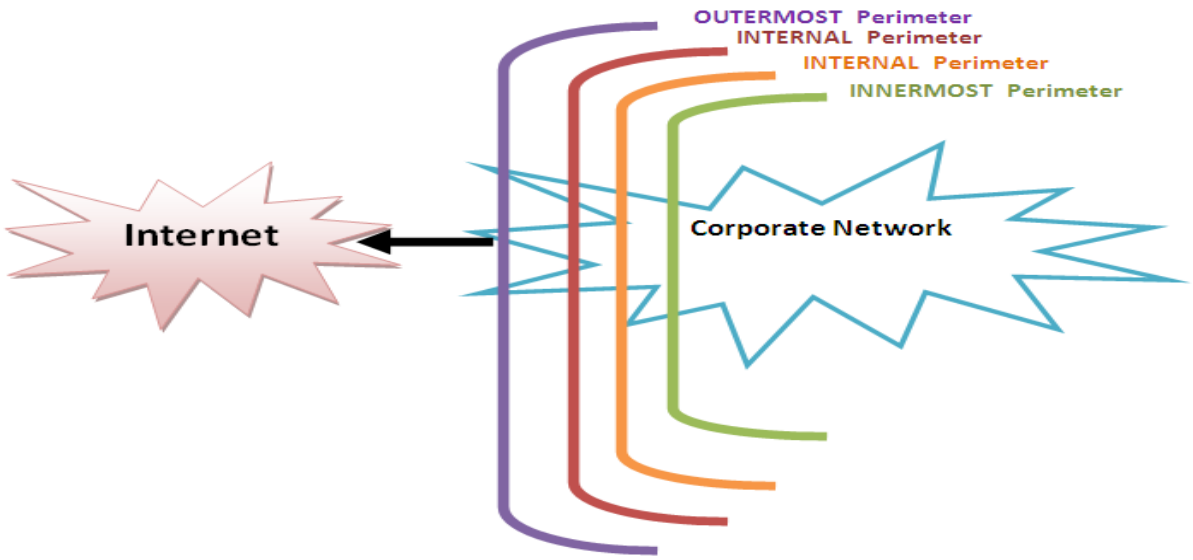


Figure (3.3) - Perimeter networks.

Not all networks have three levels of perimeter networks. Organizations need to configure their firewalls to meet their network security policy. The following section discusses the three most commonly used firewall architectures.

1- Dual-Homed Host Firewall

A dual-homed host firewall is a type of the multi-homed host firewall. In the dual-homed host firewall, the host (which provides the firewall functionality) has two interfaces: One interface is connected to the private network and the other interface is connected to the Internet (or some other untrusted network). Thus, all IP traffic from the Internet must pass through the firewall before arriving at a host in the private network. Similarly, an internal host can communicate with external hosts (that is, hosts in the Internet) via the dual-homed host.

Direct communication that bypasses the dual-homed host is blocked. This means that the IP forwarding capability of the dual-homed host is disabled to ensure that IP packets from one network are not being directly routed to the other network. The dual-homed host cannot operate as a router. However, disabling IP packet forwarding ensures that the Internet and the private network are logically disconnected so that even when system problems occur the firewall cannot fail open. Data can only pass-through the firewall via its application proxies, not through the operating system layer [17].

The dual-homed host can be used to completely block access to the private network when it provides proxy services (such as Telnet, FTP and HTTP), the server providing the particular service is located between a packet filtering router,

which may be present, and the dual-homed host. This arrangement prevents intruders from accessing systems protected by the dual-homed host.

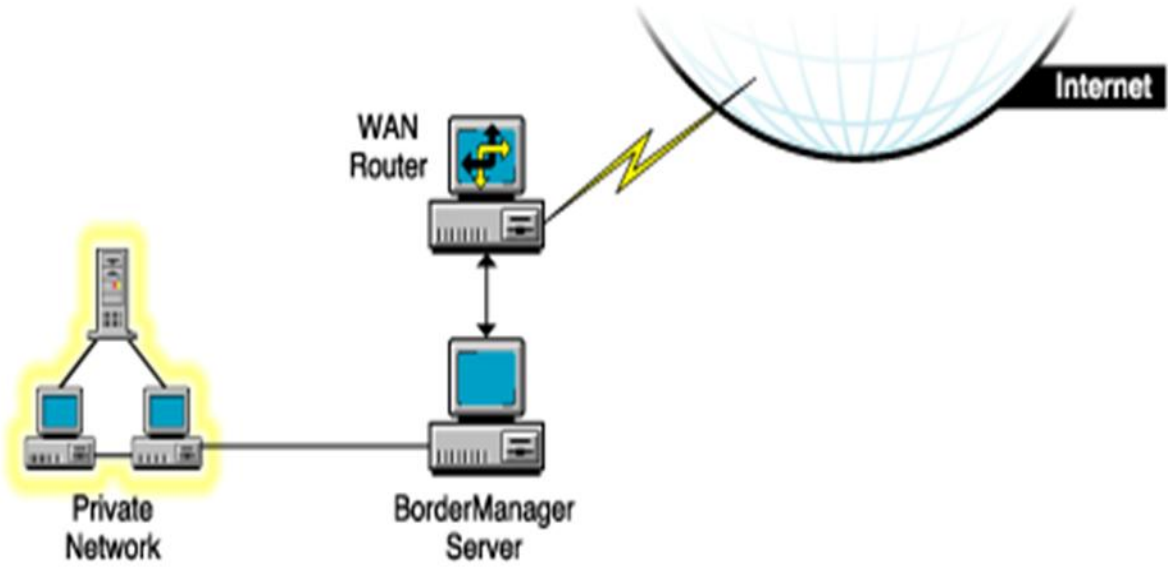


Figure (3. 4) - Dual-Homed Host Firewall [17].

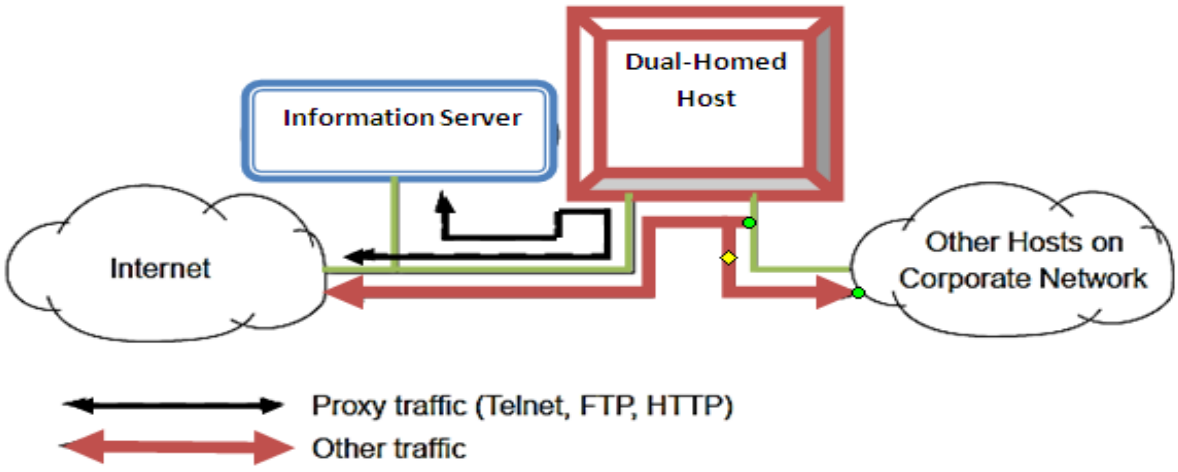


Figure (3.5)-Dual-Homed Host Firewall architecture.

2- Screened Host Firewall

Unlike the dual-homed host firewall architecture, which allows the host firewall to be connected to two networks, the screened host firewall architecture allows the host providing the firewall (called a bastion host)to connect only to the private network. A separate screening router is placed between the host and the Internet. Thus, the screened host firewalls a combination of a packet filtering router and an application gateway.

The screening router performs a packet filtering function and is configured so that the bastion host is the only host in the private network that can be accessed from the Internet. Extra security can be provided in the screening router by configuring it to block traffic to specific ports on the bastion host.

The screening router may be configured to permit or block connections between internal hosts and the Internet. Its basic function is to filter traffic classes that have been defined as security risks in the security policy before they arrive at the bastion and other internal hosts. Since the bastion host is the most exposed host in the private network, it is usually the most protected host. Generally, there are two or more bastion hosts in a network.

One of the advantages of this architecture is that a public information server providing FTP, Telnet, and HTTP services can be placed on the network segment between the screening router and the bastion host. If stronger security is desired, the bastion host can be configured to run proxy services that require both internal and external users to access the information server through the bastion host. In fact, one of the main functions of the bastion host is to act as a proxy server for various services including FTP, HTTP, Telnet, DNS, and SMTP.

One of the problems with the screened host firewall architecture is that once an attacker breaks through the bastion host, all the hosts in the private network are exposed to the attacker. In a dual-homed host firewall, however, it is impossible to pass through the dual-homed host without a corresponding proxy server. Unlike the dual-homed host firewall, the screened host firewall requires the screening router and the bastion host to be configured [18].

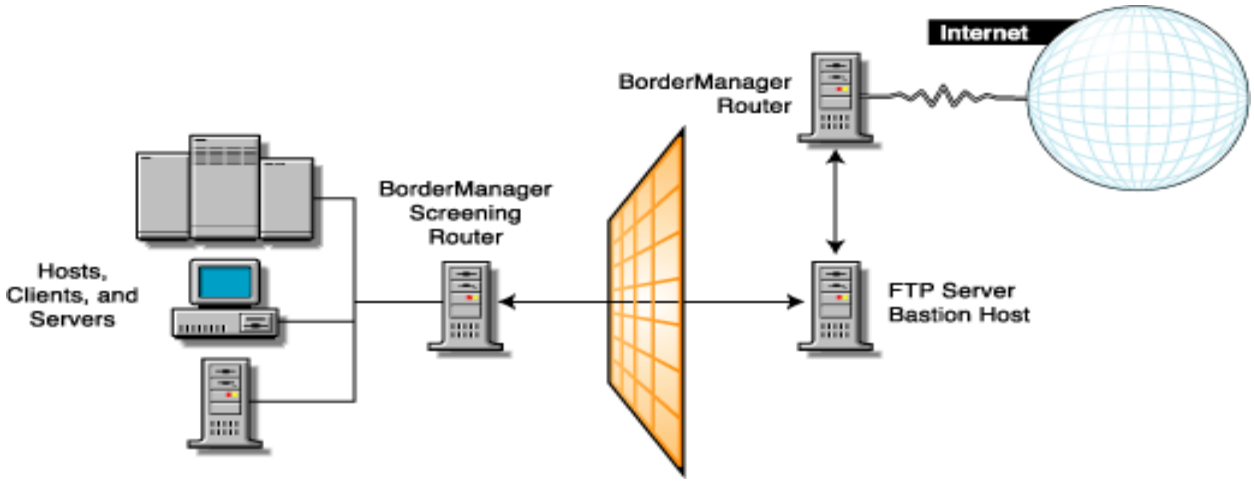


Figure (3.6) - Screened Host Firewall [17].

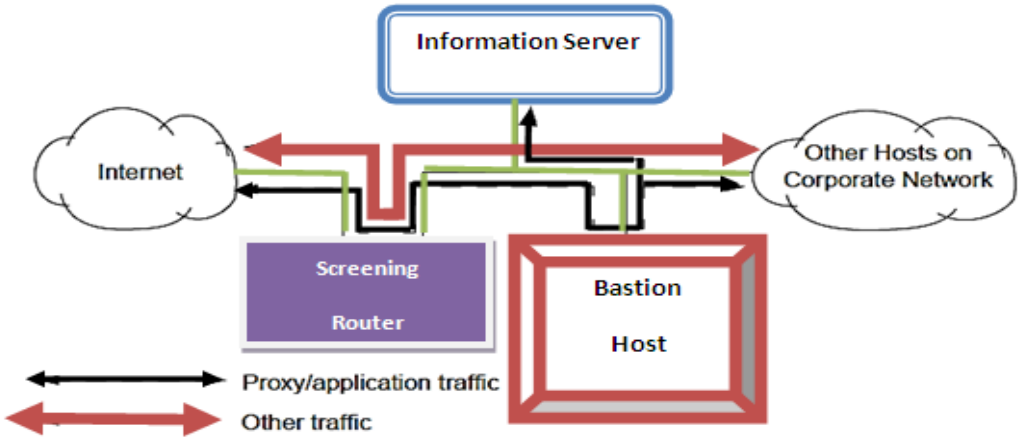


Figure (3.7) -Screened Host Firewall architecture.

3- Screened Subnet Firewall

The screened subnet firewall can be considered an extension of the screened host firewall. Like the screened host firewall, it uses a screening router (called the outer or external router) and a bastion host. However, this firewall, which is also called the Demilitarized Zone (DMZ), creates an extra layer of security by adding a perimeter network that further isolates the private network from the Internet. The firewall defines a DMZ demarcated by the outer router and an internal router, where the latter is placed closer to the private network than the outer router. The DMZ is an inner screened subnet bounded by the internal router and the outer router.

The DMZ can be considered an isolated network between the private network and the Internet. The outer router protects the network from external attacks by restricting access to systems in the DMZ. It also blocks traffic to the Internet from unauthorized sources in the private network.

The internal router manages DMZ access to the private network by passing only traffic from the bastion host to the hosts in the private network that are not in the DMZ, and vice versa.

For an attack to reach any internal host located outside the DMZ, it must break through both routers. In addition, the architecture reveals only the DMZ network to the outside world and keeps the private network hidden [19].

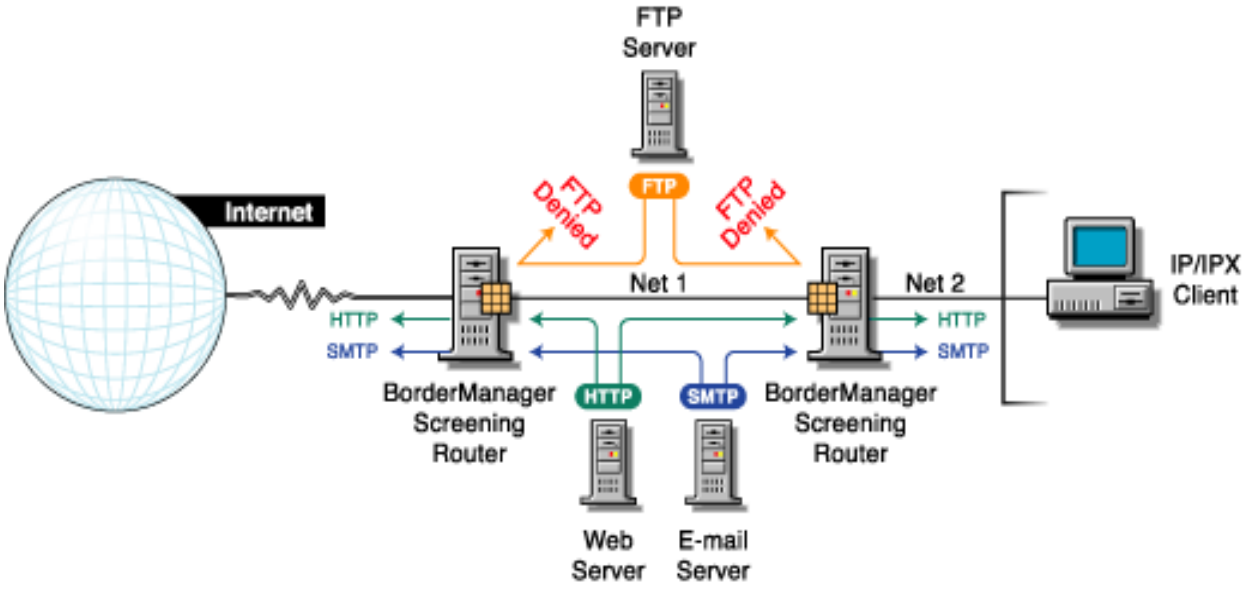


Figure (3.8) -Screened Subnet Firewall [17].

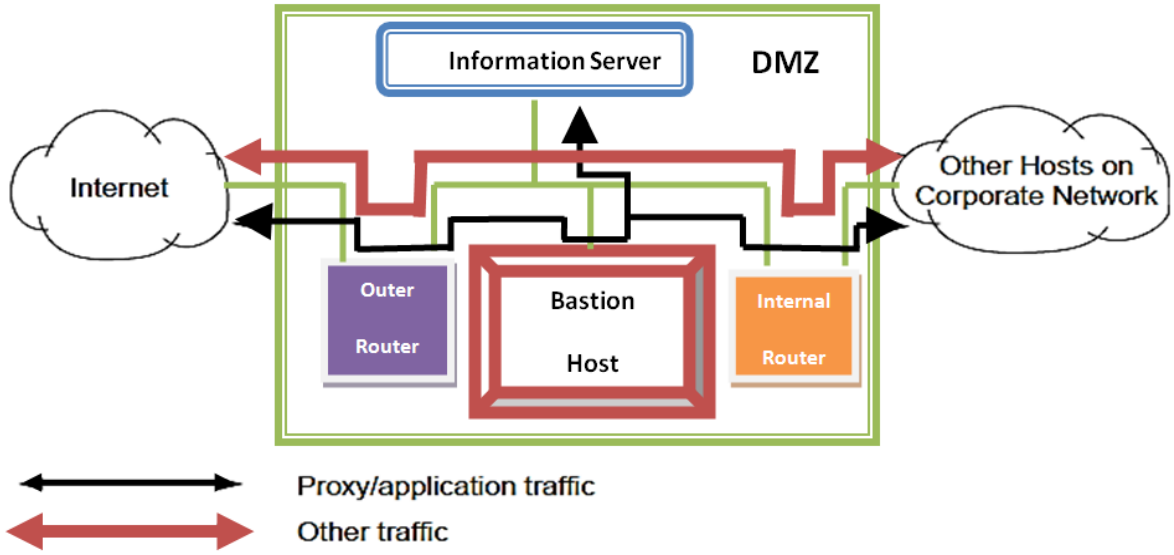


Figure (3.9) -Screened Subnet Firewall architecture.

4- Tri-Homed Hosts

A tri-homed host combines elements of a screening router and a screened host, thereby overcoming the limitations of each. Security is centered on the screening routers by using interfaces for the Internet, the intranet, and the subnets

that contain the bastion hosts and application servers. An example of a tri-homed host is shown in the following Fig (3.10).

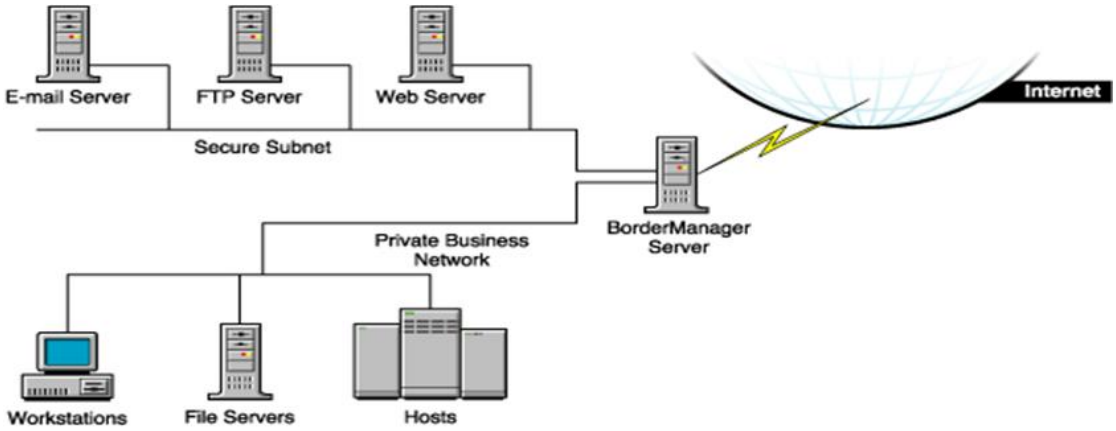


Figure (3.10) - Tri-Homed Host [17].

3.3. Virtual Private Networks (VPN)

A virtual private network (VPN) provides a secure connection between a sender and a receiver over a public non-secure network such as the Internet. A secure connection is generally associated with private networks. (A private network is a network that is owned, or at least controlled via leased lines, by an organization), a VPN can transform the characteristics of a public non-secure network into those of a private secure network. VPNs reduce remote access costs by using public network resources. Compared to other solutions, including private networks، a VPN is inexpensive.

VPNs are not new. In fact, they have been used in telephone networks for years and have become more prevalent since the development of the intelligent network. Frame relay networks, which have been around for some time, are VPNs. Virtual private networks are only new to IP networks such as the Internet.

The goal of a VPN is to provide a secure passage for users' data over the non-secure Internet. It enables companies to use the Internet as the virtual backbone for their corporate networks by allowing them to create secure virtual links between their corporate office and branch or remote offices via the Internet. The cost benefits of VPN service have prompted corporations to move more of their data from private WANs to Internet based VPNs.

A VPN uses data encryption and other security mechanisms to prevent unauthorized users from accessing data, and to ensure that data cannot be modified without detection as it flows through the Internet. It then uses the tunneling process to transport the encrypted data across the Internet.

Tunneling is a mechanism for encapsulating one protocol in another protocol. In the context of the Internet, tunneling allows such protocols as IPX, AppleTalk, and IP to be encrypted and then encapsulated in (IP.Similarly), in the context of VPNs, tunneling disguises the original network layer protocol by encrypting the packet and enclosing the encrypted packet in an IP envelope. This IP envelope, which is an IP packet, can then be transported securely across the Internet. At the receiving side, the envelope is removed and the data it contains is decrypted and delivered to the appropriate access device, such as a router.

Simply put, a corporation is creating a private tunnel through the Internet for the secure delivery of its data. The tunnel enables the corporation to create a virtual WAN, within the Internet.

VPNs also provide quality of service (QoS) guarantees, which usually specify an upper bound on the average packet delay in the network. The guarantees may also include specification of a lower bound on the bandwidth available to the user. These guarantees are developed through service level

agreements (SLAs) with the service provider. Most service providers have their own private backbone IP networks.

Therefore, they are in a better position to meet QoS guarantees. However, such networks do not provide the global coverage as the Internet. Sometimes a service provider makes private peering arrangements with other service providers, whose private IP networks cover more area. This arrangement allows the service provider to hand off its high-priority traffic (that is, traffic with stringent QoS requirements) to networks with a guaranteed QoS instead of putting such high-priority traffic on the Internet where delay is unpredictable.
We can define a VPN by the following relationship [20] :

VPN = Tunneling + Security + QoS Guarantees

3.3.1. Advantages of VPNs

As stated earlier, VPNs are inexpensive; they provide remote and mobile user with access to the corporate network at the price of a local call. VPNs also provide the framework for corporate intranets and extranets. Corporations can exploit the global nature of the Internet and use VPNs to link all branch offices into private networks called intranets. A corporation can make certain sections of its intranet accessible to its vendors and strategic partners by means of the extranet. VPN tunnels permit non-routable protocols to be delivered to specific LAN segments in the corporate intranet. In this way, VPNs enable legacy applications to use the intranet [18]. VPNs have also contributed significantly to the increased use of private IP addresses.

3.3.2. Types of VPNs

Currently there are three types of VPNs. While their goal is to leverage the Internet as a private enterprise backbone network, each of them addresses the needs of a different interest group in the enterprise.
The three types of VPNs are as follows:

1. Access VPNs provide remote users such as road warriors (or mobile users), telecommuters, and branch offices with reliable access to corporate networks.

2. Intranet VPNs allow branch offices to be linked to corporate headquarters in a secure manner.

3. Extranet VPNs allow customers, suppliers, and partners to access corporate intranet in a secure manner.

3.3.3.VPN Architectures

A VPN consists of our components: a VPN client, a network access server(NAS), a tunnel terminating device (or VPN server), and a VPN protocol. In atypical access VPN connection, a remote user (or VPN client) initiates a PPP connection with the ISP's NAS via the public switched telephone network (PSTN).

An NAS is a device that terminates dial-up calls over analog (basic telephone service) or digital (ISDN) circuits. The NAS is owned by the ISP, and is usually implemented in the ISP's POP. After the user has been authenticated by the appropriate authentication method, the NAS directs the packet to the tunnel that connects both the NAS and the VPN server. The VPN server may reside in the

ISP's POP or at the corporate site, depending on the VPN model that is implemented. The VPN server recovers the packet from the tunnel, unwraps it, and delivers it to the corporate network [21].

There are four tunneling protocols used to establish VPNs, and three are extensions of the Point-to-Point Protocol (PPP):

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- IP Security (IPSec) Protocol Suite

When both PPTP and L2F were submitted to the IETF, the organization decided to combine the features of both protocols into a common tunneling protocol, which is now L2TP. The Layer 2 Tunneling Protocol was in the draft stage at this time.

The four protocols can be classified broadly into two groups: Layer 2tunneling protocols and Layer 3 tunneling protocols. PPTP, L2F, and L2TP are Layer 2 tunneling protocols, while IPSec is a Layer 3 tunneling protocol.

- **Layer 2 Tunneling Protocols**

Layer 2 tunneling protocols operate at the data link layer (or Layer 2). They encapsulate Layer 3 packets in Layer 2 PPP before encapsulating them in IP.
They use the security provided by PPP. Thus, they perform user authentication using existing PPP authentication protocols, namely PAP and CHAP. No specific

provision is made for data encryption, which may be performed by the user prior to requesting VPN service.

A client initiates a PPP connection by dialing up the NAS, which is typically implemented in the ISP's POP. The client then uses the logical control protocol (LCP) negotiation to establish the PPP connection. Once the PPP connection is established, the NAS uses either PAP or CHAP to authenticate the client. If the authentication is successful, the NAS attempts to open a PPP connection to the VPN server using LCP negotiation. The VPN server will authenticate the NAS using PAP or CHAP. The client and the VPN server will then use the network control protocol (NCP) to negotiate the network layer protocol. This completes the tunneling process.

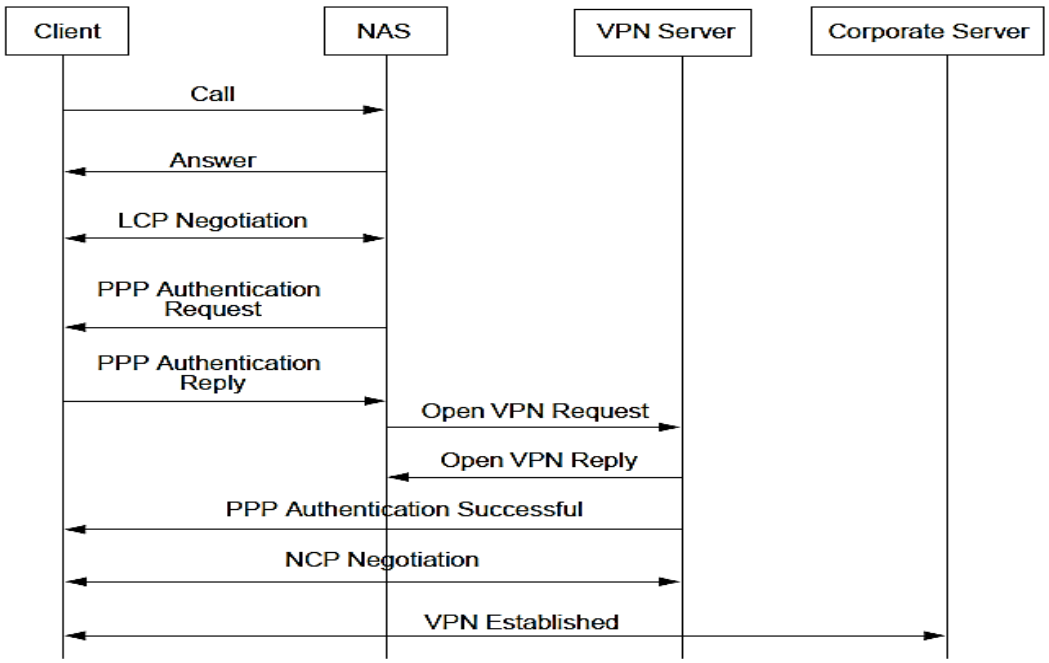


Figure (3.11) -Tunnel creation process for Layer 2 VPNs [20].

1- PPTP

PPTP is a protocol developed by Microsoft and a group of network equipment vendors including Ascend Communications and 3Com. It permits IPX, NetBEUI, and IP packets to be encapsulated inside IP packets, enabling non-IP applications to run over the Internet. As an extension of PPP, it handles only point-to-point connections; it does not support point-to-multipoint connections. More importantly, PPTP is an IP-centric protocol that is designed only for IP networks.

In PPTP, the NAS that allows the remote user to initiate a VPN call is called the PPTP access concentrator (PAC), and the VPN server is called the PPTP network server (PNS).

PPTP does not provide packet-by-packet encryption. Instead, it relies on PPP's native encryption capability in PAP and CHAP. A PPTP packet is encapsulated in Generic Routing Encapsulation (GRE), which is then carried over IP. PPTP separates the control and data channels into a control stream that runs over TCP and a data stream that runs over GRE. The PPP payload consists of the data and its TCP and IP headers.

PPTP is a proprietary protocol, but most VPNs to date are based on this protocol. PPTP uses TCP, which allows it to support flow control. It also supports a rate control mechanism that limits the amount of data in transit, minimizing the need for retransmission due to dropped packets. This results in better use of the bandwidth.

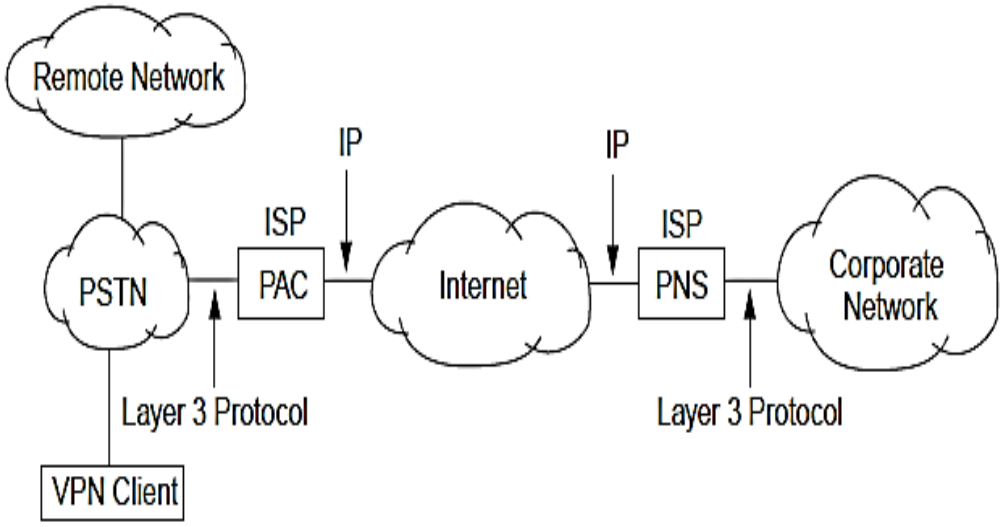


Figure (3.12) - PPTP VPN components [20].

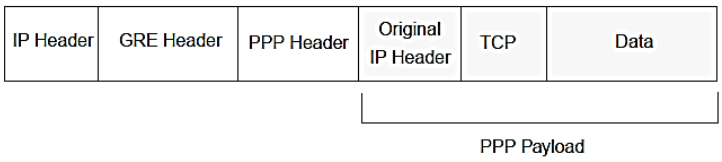


Figure (3.13) - PPTP packet format [20].

2- L2F

L2F is a proprietary protocol that was developed by Cisco Systems. It is protocol-independent and can run over X.25, frame relay, and ATM networks. It supports private IP, IPX, and AppleTalk, and uses UDP for Internet tunneling.L2F defines many connections within a tunnel, allowing a tunnel to support many connections.

In L2F, the VPN server is called the Home Gateway. L2F uses PPP for dial-up user authentication. However, it also supports other authentication schemes including RADIUS and TACACS+.

Unlike PPTP, L2F defines its own encapsulation header, which is not dependent on IP and GRE. This capability permits L2F to work in different types of networks. The SLIP/PPP payload is encapsulated in an L2F packet with an L2F header and an optional L2F checksum as the trailer.

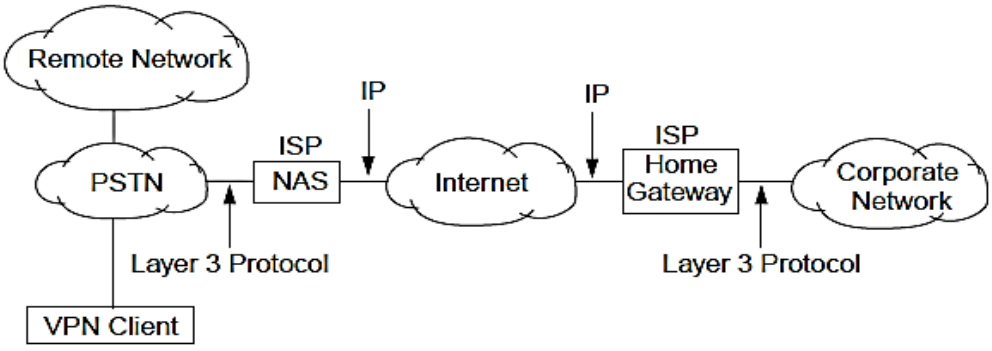


Figure (3.14) - L2F VPN components [20].

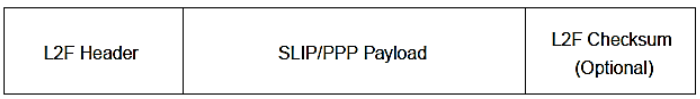


Figure (3.15) - L2F packet format [20].

3- L2TP

As stated earlier, L2TP combines the features of PPTP and L2F. Unlike PPTP, which runs over TCP, L2TP runs over UDP and does not use GRE. Because many firewalls do not support GRE, L2TP is more firewall-friendly than PPTP. In L2TP, the NAS is called the L2TP access concentrator (LAC) and the VPN server is called the L2TP network server (LNS).

L2TP uses PPP dial-up links and, as a result, also uses PAP and CHAP for authentication. However, it allows the use of RADIUS for user authentication. L2TP permits multiple tunnels to be created between the same pair of end-points, allowing the user to create different tunnels with different qualities of service between the same end-points. L2TP is supported by many vendors, and is expected to be the predominant protocol once it becomes a standard. L2TP relies on IPSec to perform data encryption. If L2TP discovers that IPSec is not supported at the remote end, it uses the less secure PPP encryption.

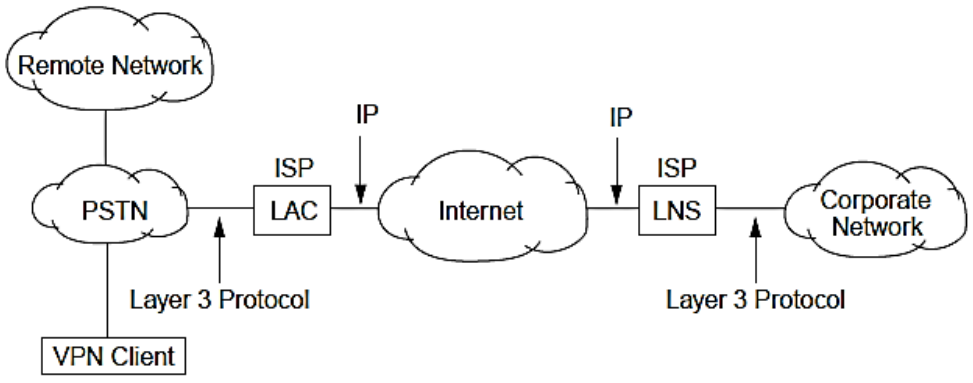


Figure (3.16) - L2TP VPN components [20].

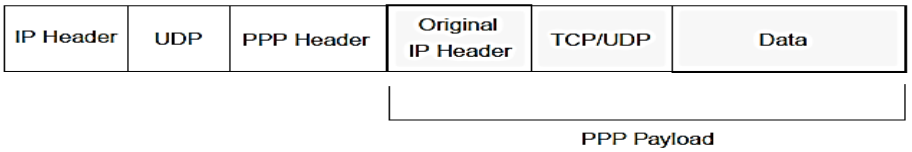


Figure (3.17) - L2TP packet format [20].

3.3.4.VPN Models

There are two ways to implement Layer 2 VPNs, which are referred to as the NAS-initiated VPN, and the client-initiated VPN. In both models, the VPN client initiates a remote dial-up to the ISP's POP.

1- NAS-Initiated VPN

In NAS-initiated VPN, a VPN client initiates a dial-up session with the ISP's NAS. The NAS assigns the user an IP address independent of the user's IP address for the local network. The NAS is responsible for tunneling the packet through the Internet to the VPN server. Thus, the VPN connection extends only between the NAS and the VPN server.

A NAS-initiated VPN is also called a compulsory VPN because the client does not participate in its creation and is compelled to use it. All encryption occurs between the NAS and the VPN server and the two functional entities form the end-points of the tunnel. A compulsory VPN is created without the user's consent, meaning that the VPN is transparent to the user. One of the advantages of the NAS-initiated VPN is that it can support multiple connections, which reduces the overhead associated with establishing one VPN for each connection. However, the connection between the client and the NAS occurs outside the tunnel, making the VPN vulnerable to attacks.

This model can also be considered an out-sourced VPN in which the ISP manages the remote access needs of a corporation. It is particularly useful in those environments where the information technology staff is not equipped to handle VPN management [22].

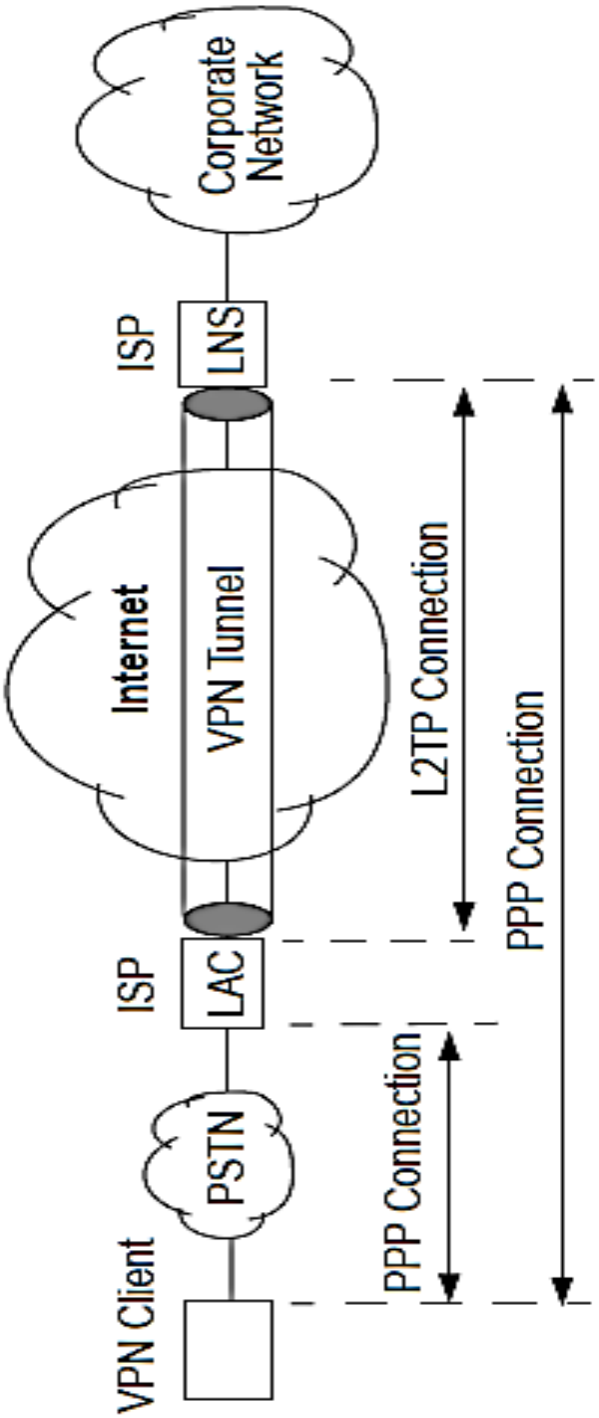


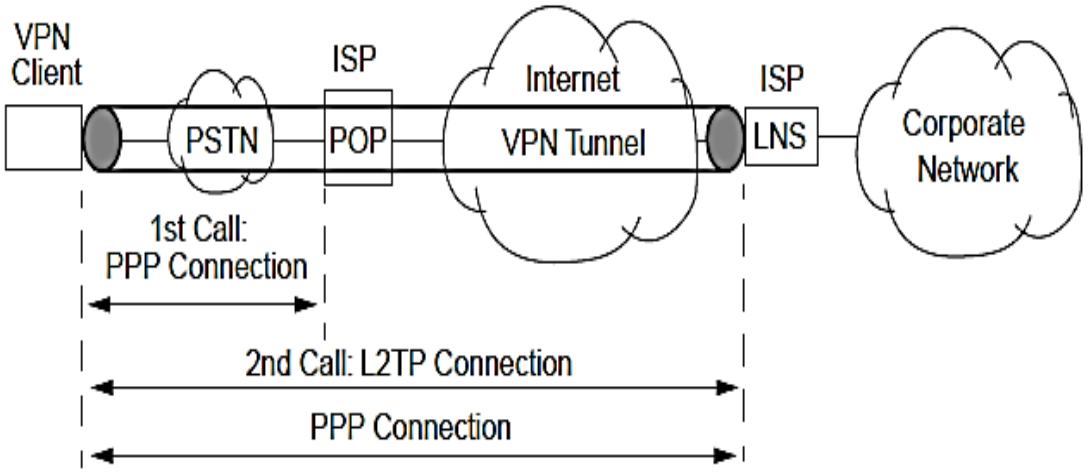
Figure (3.18) NAS-Initiated L2TP VPN model [20].

2- Client-Initiated VPN

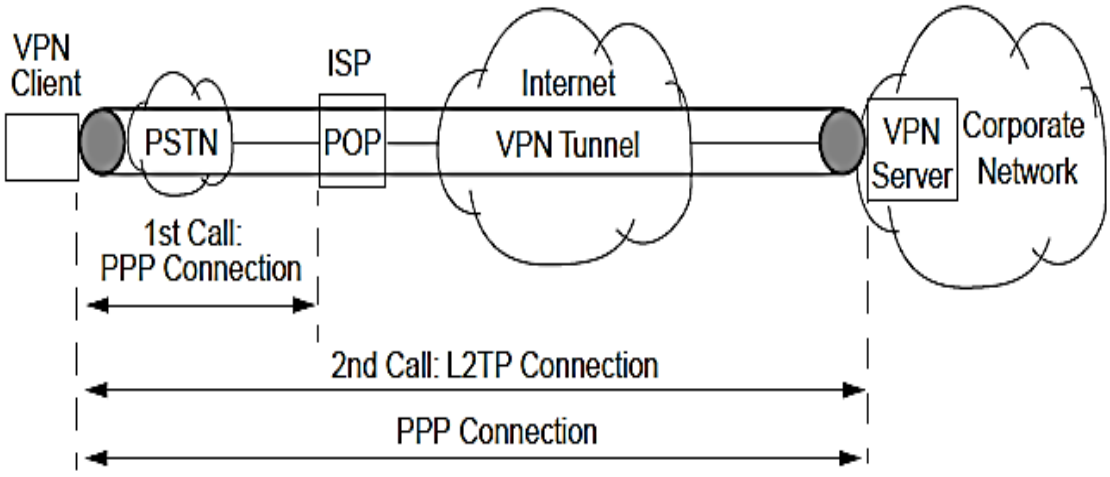
n a client-initiated VPN, the VPN client is VPN-enabled (that, the VPN software is already installed). The VPN client dials up the ISP's local POP to establish a PPP session. Then, using the Internet connection, the client establishes a VPN connection with the VPN server. In this model, the tunnel extends from the VPN client to the VPN server. The NAS is not involved in the tunnel establishment. A client-initiated VPN is also called a voluntary VPN because the user determines when and where to establish the VPN. The user is responsible for the necessary encryption between the client and the VPN server.

The VPN server may reside in either the ISP's network or in the corporate network. If the VPN server resides in the ISP's network, the contents of the tunnel are delivered to the corporate network via the WAN that the corporate router uses to access the ISP's POP. This WAN may be a frame relay network or an ISDN network. If the VPN server resides in the corporate network, the tunnel extends from the client directly into the corporate network.

In the case where the VPN server resides in the corporate network, the VPN is essentially managed in-house [22].



(a) VPN server in ISP network



(b) VPN server in corporate network

Figure (3.19) Client-initiated L2TP VPN model [20].

The client-initiated model permits remote users with VPN-enabled clients to dial into any ISP's POP and establish a tunnel to the corporate network. The ISP's POP is not required to be VPN-enabled; that is, the NAS functionality does not need to be available at the POP. In the NAS-initiated model, the ISP's POP must have NAS functionality. Unlike the NAS-initiated model, the client initiated model does not bind a corporation to any one ISP; it permits a corporation to change ISPs without changing its addressing scheme. The client-initiated model does not lend itself easily to hacker intrusion. The model does not require a company to hand its authentication database over to the ISP. Since a company controls both ends of the tunnel, it can impose any desired requirement for user authentication to prevent unauthorized users
from gaining access to its resources. In the NAS-initiated model, a company is required to give its authentication database to the ISP. Thus, a hacker can penetrate the ISP under a false identity.

NAS-initiated VPN permits VPN clients to support tunneling without software or hardware upgrades. However, the model requires the ISP to manage both the addressing and authentication processes. A corporation may have to restructure its addressing scheme to match the ISP's scheme. Also, the ISP must be constantly informed of changes in the network.

A Layer 3 VPN, such as IPSec, is more suited to the NAS-initiated model because it is designed primarily to provide security between a router and a firewall. In general, the NAS functionality is implemented in a router and the VPN server functionality is implemented in a firewall. IPSec is an integral part of IPv6. Thus, unless a VPN client is running IPv6, it may not be economical for a legacy end-station implementing VPN client functionality to be equipped to provide the IPSec protocol stack. It may be more economical for the ISP's NAS to provide IPSec.

3.3.5. Firewalls and VPNs

Firewalls and VPNs go hand in hand. Many firewall products provide encrypted firewall-to-firewall tunnels. In particular, it was stated that application gateways provide IP address hiding by encapsulating one IP packet in another. This, by our definition, is the tunneling associated with VPNs.
Firewalls control access to corporate network resources and establish trust between the user and the network.

VPNs are created to provide privacy between two sites; there is usually no trust between the two sites. A combination of firewalls and a VPN establishes trust and provides privacy between the two sites. This approach provides more security than using either firewalls at both sites or a VPN between the two sites.

In the past, firewall products provided only firewall security service. However, many new firewall products now support VPN functionality. As stated earlier, both firewall functionality and VPN functionality are needed to establish effective security control.

A firewall provides access control to a protected network, protecting a company's private network from an untrusted public network. Every access request from a public network to the protected (that is, corporate) network must pass through the firewall. Different types of firewalls and firewall architectures have also been discussed.

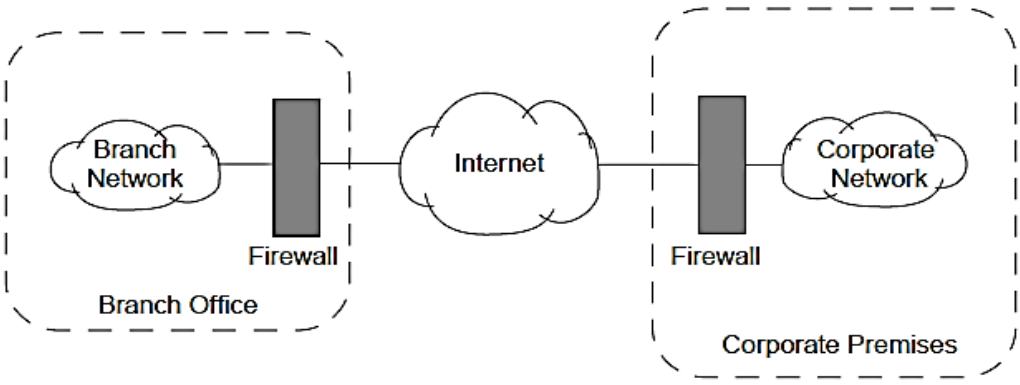


Figure (3.20) -Firewalls providing authorized access to two networks.

A virtual private network (VPN) provides secure connections using a public on-secure network, such as the Internet. VPNs reduce remote access costs by using public network resources that can be shared by many users. VPN technology has enabled companies to build intranets to link branch offices to the corporate network. Furthermore, the technology enables companies to deploy extranets that securely link corporate networks to those of their strategic partners, suppliers, and special customers.

VPNs are used in conjunction with firewalls to provide more comprehensive security protection for an organization. Firewalls control access to corporate network resources, establishing trust between the user and the network.

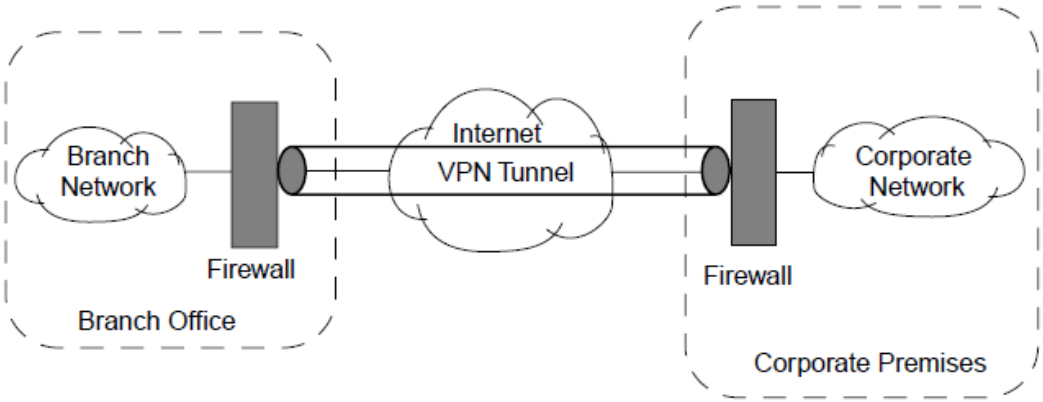


Figure (3.21) - VPN tunnel between two firewalls.

4.1. Introduction

A fully Layer 2 switched network is referred to as a flat network topology. A flat network is a single broadcast domain in which every connected device sees every broadcast packet that is transmitted.

As the number of hosts on the network increases, so does the number of broadcasts. Due to the Layer 2 foundation, flat networks cannot contain redundant paths for load balancing or fault tolerance. However, a switched network environment offers the technology to overcome flat network limitations. Switched networks can be subdivided into virtual LANs (VLANs), each of which is a single broadcast domain.

All devices connected to the VLAN receive broadcasts from other VLAN members. However, devices connected to a different VLAN will not receive those same broadcasts because is made up of defined members communicating as a logical network segment. A VLAN can have connected members located anywhere in the campus network, as long as VLAN connectivity is provided between all members. Layer 2 switches are configured with a VLAN mapping and provide the logical connectivity between the VLAN members.

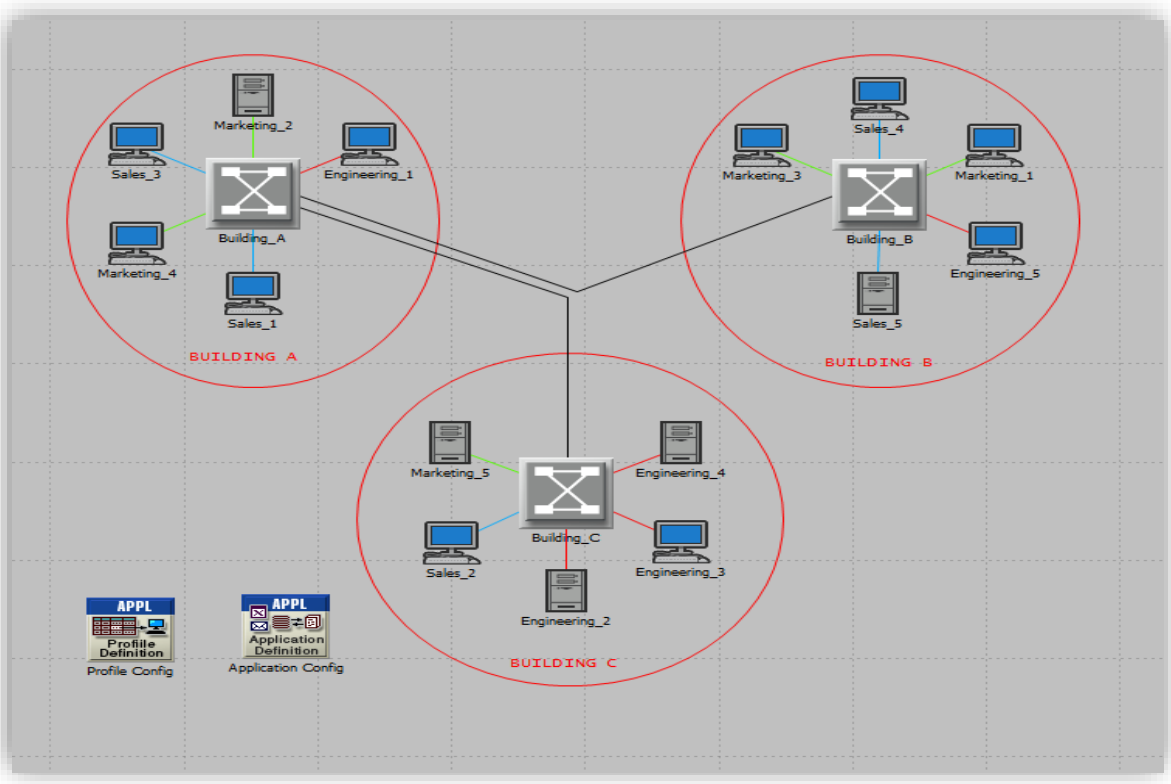


Figure (4.1) -**Virtual LANs**

4.2. VLAN Membership

When a VLAN is provided at an access layer switch, an end user must be able to gain membership to it.

Two membership methods exist on Cisco Catalyst switches: static VLANs and dynamic VLANs.

- **Static VLANs** offer port-based membership, where switch ports are assigned to specific VLANs. End user devices become members in a VLAN based on which physical switch port they are connected to.

No handshaking or unique VLAN membership protocol is needed for the end devices; they automatically assume VLAN connectivity when they connect to a port. The static port-to-VLAN membership is normally handled in hardware with application specific integrated circuits (ASICs) in the switch. This membership provides good performance because all port mappings are done at the hardware level with no complex table lookups needed [23].

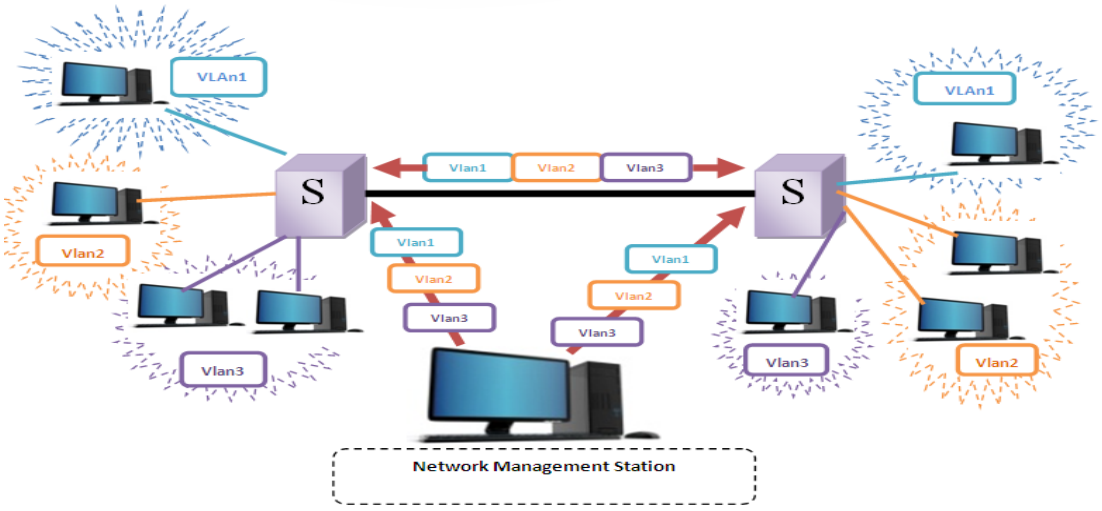


Figure (4.2) –Static VLANs

- **Dynamic VLANs** are used to provide membership based on the MAC address of an end user device.

When a device is connected to a switch port, the switch must query a database to establish VLAN membership. A network administrator must assign the user's MAC address to a VLAN in the database of a VLAN Membership Policy Server (VMPS).

With Cisco switches, dynamic VLANs are created and managed through the use of network management tools like Cisco Works 2000 or Cisco Works for Switched Internetworks (CWSI). Dynamic VLANs allow a great deal of flexibility and mobility for end users, but require more administrative overhead.

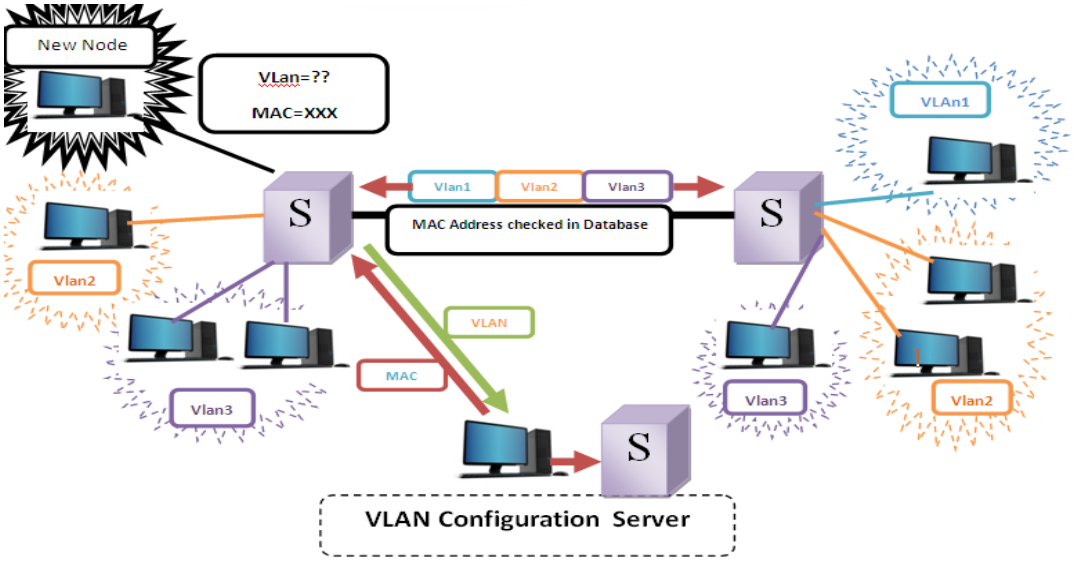


Figure (4.3) -Dynamic VLANs

4.3. Extent of VLANs

The number of VLANs that will be implemented on a network is dependent on traffic patterns, application types, segmenting common workgroups, and network management requirements. However, consideration must be given to the relationship between VLANs and the IP addressing schemes. Cisco recommends a one-to-one correspondence between VLANs and IP subnets, which means that if a Class C network address is used for a VLAN, then no more than 254 devices should be in the VLAN. Cisco also recommends that VLANs not extend beyond the Layer 2 domain of the distribution switch, i.e., the VLAN should not reach across the core of a network and into another switch block. This is designed to keep broadcasts and unnecessary movement of traffic out of the core block. VLANs can be scaled in the switch block by using two basic methods: end-to-end VLANs and local VLANs [24].

- End-to-end VLANs span the entire switch fabric of a network and are also called campus-wide VLANs. They are positioned to support maximum flexibility and mobility of end devices. Users are assigned to VLANs regardless of their physical location. This means that each VLAN must be made available at the access layer in every switch block. End-to-end VLANs should group users according to common requirements, following the 80/20 rule. Although only 20 percent of the traffic in a VLAN is expected to cross the network core, end-to-end VLANs make it possible for all traffic within a single VLAN to cross the core. Because all VLANs must be available at each

access layer switch, VLAN trunking must be used to carry all VLANs between the access and distribution layer switches.

- In the modern network, end users require access to central resources outside their VLAN. Users must cross into the network core more frequently, making the end-to-end VLANs cumbersome and difficult to maintain. Most enterprise networks have adopted the 20/80 rule. Local VLANs deployed in this type of network. Local VLANs are designed to contain user communities based on geographic boundaries, with little regard to the amount of traffic leaving the VLAN. They range in size from a single switch in a wiring closet to an entire building. Local VLANs enables the Layer 3 function in the campus network to intelligently handle the inter-VLAN traffic loads. This provides maximum availability by using multiple paths to destinations, maximum scalability by keeping the VLAN within a switch block, and maximum manageability.

4.4. VLAN Trunking

When using VLANs in networks that have multiple interconnected switches, you need to use VLAN trunking between the switches. With VLAN trunking, the switches tag each frame sent between switches so that the receiving switch knows to what VLAN the frame belongs. End user devices connect to switch ports that provide simple connectivity to a single VLAN each. The attached devices are unaware of any VLAN structure .A trunk link can transport more than one VLAN through a single switch port. A trunk link is not assigned to a specific VLAN. Instead, one or more active VLANs can be

transported between switches using a single physical trunk link. Connecting two switches with separate physical links for each VLAN is also possible.
In addition, trunking can support multiple VLANs that have members on more than one switch. Cisco switches support two trunking protocols, namely, Inter-Switch Link (ISL) and IEEE 802.1Q [25].

4.4.1. Inter-Switch Link (ISL)

Cisco created ISL before the IEEE standardized a trunking protocol. Thus, ISL is a Cisco proprietary solution and can be used only between two Cisco switches. ISL fully encapsulates each original Ethernet frame in an ISL header and trailer. The original Ethernet frame inside the ISL header and trailer remain sun changed. The ISL header includes a VLAN field that provides a place to encode the VLAN number.

By tagging a frame with the correct VLAN number inside the header, the sending switch can ensure that the receiving switch knows to which VLAN the encapsulated frame belongs. Also, the source and destination addresses in the ISL header use MAC addresses of the sending and receiving switch, as opposed to the devices that actually sent the original frame.

4.4.2. IEEE802.1Q

After Cisco created ISL, the IEEE completed work on the 802.1Q standard. 802.1Q uses a different style of header to tag frames with a VLAN number than the ISL. It does not encapsulate the original frame, but adds a 4-byte header to the original Ethernet header. This additional header includes a field with which to identify the VLAN number. Because the original header has been changed, 802.1Q encapsulation forces are calculation of the original FCS field in the Ethernet trailer, because the FCS is based on the contents of the entire frame. 802.1Q also introduces the concept of a native VLAN on a trunk. Frames belonging to this VLAN are not encapsulated with tagging information. In the event that a host is connected to an 802.1Qtrunk link, that host will be able to receive and understand only the native VLAN frames.

4.5. VLAN Trunking Protocol (VTP)

Administration of network environments that consists of many interconnected switches is complicated .Cisco has developed a propriety solution to manage VLANs across such networks using the VLAN Trunking Protocol (VTP) to exchange VLAN configuration information between switches. VTP uses Layer2 trunk frames to exchange VLAN information so that the VLAN configuration stays consistent throughout a network. VTP also manages the additions, deletions, and name changes of VLANs across multiples witches from a central point, minimizing misconfigurations and

configuration inconsistencies that can cause problems, such as duplicate VLAN names or incorrect VLAN type settings.

VTP is organized into management domains or areas with common VLAN requirements. A switch can belong to only one VTP domain. Switches in different VTP domains do not share VTP information .Switches in a VTP domain advertise several attributes to their domain neighbors. Each advertisement contains information about the VTP management domain, VTP configuration revision number, known VLANs, and specific VLAN parameters .The VTP process begins with VLAN creation on a switch called a VTP server. VTP floods advertisements throughout the VTP domain every 5 minutes, or whenever there is a change in VLAN configuration. The VTP advertisement includes a configuration revision number, VLAN names and numbers, and information about which switches have ports assigned to each VLAN. By configuring the details on one or more VTP server and propagating the information through advertisements, all switches know the names and numbers of all VLANs [25].

4 .5.1. VTP Modes

To participate in a VTP management domain, each switch must be configured to operate in one of three modes. These modes are: server mode, client mode, and transparent mode.

4.5.2. Server Mode

Server mode is the default mode. In this mode, VTP servers have full control over VLAN creation and modification for their domains. All VTP information is advertised to other switches in the domain, while all received VTP information is synchronized with the other switches. Because it is the default mode, server mode can be used on any switch in a management domain, even if other server and client switches are in use .This mode provides some redundancy in the event of a server failure in the domain.

- **Client Mode**

Client mode is a passive listening mode. Switches listens to VTP advertisements from other switches and modify their VLAN configurations accordingly. Thus the administrator is not allowed to create, change, or delete any VLANs. If other switches are in the management domain, a new switch should be configured for client mode operation. In this way, the switch will learn any existing VTP information from a server. If this switch will be used as a redundant server, it should start out in client mode to learn all VTP information from reliable sources. If the switch was initially configured for server mode instead, it might propagate incorrect information to the other domain switches. Once the switch has learned the current VTP information, it can be reconfigured for server mode [25].

- **Transparent Mode**

Transparent mode does not allow the switch to participate in VTP negotiations. Thus, a switch does not advertise its own VLAN configuration, and a switch does not synchronize its VLAN database with received advertisements. VLANs can still be created, deleted, and renamed on the transparent switch. However, they will not be advertised to other neighboring switches. VTP advertisements received by a transparent switch will be forwarded on to other switches on trunk links.

5.1. Simulation Tools

Simulation is the process of testing a designed model on a platform which imitates the real environment. It provides the opportunity to create, modify and study the behavior of proposed design so that one can predict its strengths and weakness before implementing the model in real environment. One of the popular simulators used to simulate the data networks is OPNET Modeler.

OPNET provides several modules for the simulation comprising a vast universe of the protocols and network elements .It has gained popularity in academia as it is offered for free of cost to institutions and it is also obtained as a student version. The user doesn't need to have any programming knowledge in order to use OPNET; the user can directly concentrate on building and analyzing model from simulation. The main feature of OPNET is that it provides various real-life network configuration capabilities that make the simulation environment close to reality .The advantages of OPNET compared to other simulators include GUI interface, comprehensive library of network protocols and models, graphical interface to view the results, availability of documentation for the user to develop the network models etc.

5.2. Firewalls Simulation

Firewalls are a network access control system that divides a network that we presume it is secure from a network that may be unsecure. Although it can control the incoming and outgoing traffic, the most common usage of firewalls is to control the ingoing traffic.

- **Network Firewalls (packet filtering)**

Routers can control the IP packets that go across them by accepting/denying traffic according to policies affecting to protocol headers (IP, ICMP, UDP, TCP, ..). We can analyze source/destination addresses and ports, protocol types, packet contents and size, etc. There are two general policies:

a) Accept all packets except for a finite set of cases.

b) Deny all traffic except for a finite set of cases.

Each packet reaching the device will look up the filtering rules and stop at the first match, and after that will make the decision of either denying or accepting the traffic.

- **Proxies (Application Gateways)**

They behave as Application-level retransmission devices. Network users establish a communication with the proxy, thus dividing the source-destination connection in two independent connections (source-firewall and firewall-destination). The proxy server manages the requested connections.

This technology has a slower performance than network firewalling because it is working on the upmost OSI layer. It is usual to use both firewalls at the same time.

Lab Scenarios

We have two **Scenarios**, each one with its own network (LAN1 and LAN2 “Mesrata "), trying to access a database server "Tripoli" where a database with

user's information is stored, and an e-mail and HTTP servers "Tripoli". At the same time, some Users are using illegal Access and multimedia downloading, and so slowing the Internet link performance or hacking the data. The Branches are requesting to set up a Firewall to avoid multimedia traffic in order to decrease the mean database access time to a 1 sec threshold.

- **Creating the Scenario (packet filtering)**

1. Open OPNET IT Guru Academic Edition: (File_New Project) using these parameters (use default values for the remainder):

• Project Name: Libyan _Academy_ Firewall
• Scenario Name: No Firewall
• Network Scale: Campus
• Size: 100x100 meters

2. Network creation:

Create the scenario of Figure (5.1)with the components that are used.

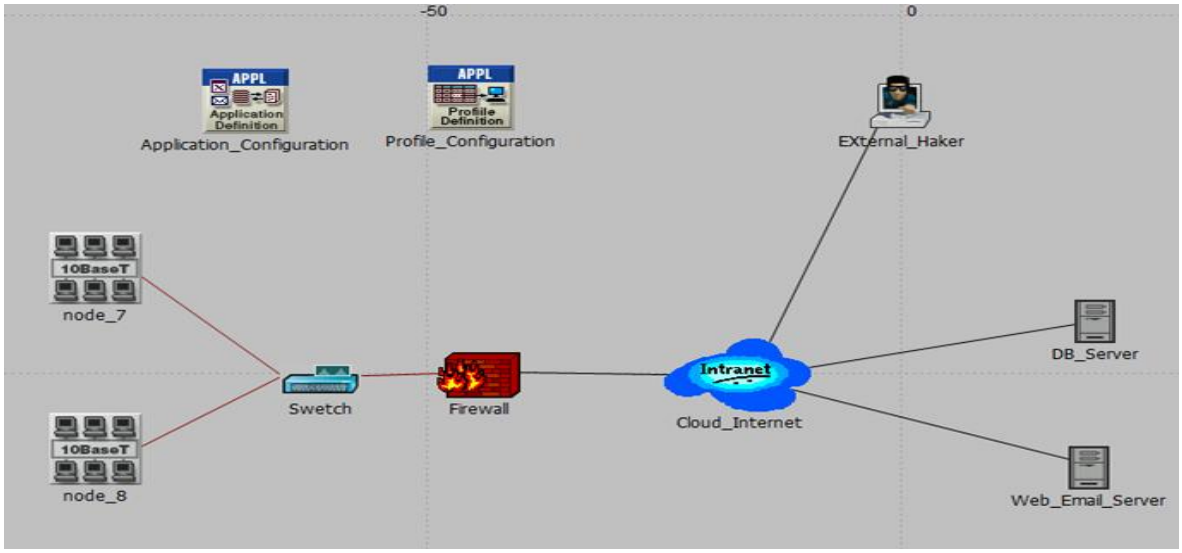


Figure (5.1) - Firewall scenario.

3. Setting up the Application Config control:

Select the Application Config control, and Change the application load afterwards: HTTP: Permits HTTP (Light Browsing) and Email: Permits Email (Low Load).

4. Setting up the Firewall:

with first scenario permits the traffic and the attributes to modify Address and Subnet Mask: Auto Addressed on all rows of IP Routing Parameters_Interface Information and IP Routing Parameters_Loopback Interfaces.

Config the routing protocol OSPF: OSPF and Parameters Interface Information the unique router interfaces Type: Broadcast. Set Point to Point.

Proxy Server Information (corresponds to Application Remote Login, necessary for Database access)_Proxy Server Deployed: Yes, this ensures that database traffic has the right to pass.

5. Setting up multimedia as attacker:

We have to modify the Application: Supported Services, by setting the parameters .

6. Setting up the DB Server and Web and Email Server:

This server Supported Services have to be set as seen in the Table below:

Table (5.1) - Supported Services

Server	Supported Services
DB Server	DB
Web And Email Server	Http Email

7. Configuring the Branch LANs:

For LAN 1 And LAN 2 we will Use (non-deployed branches use default parameters). This configuration will use 250 workstations for each and every LAN (Number of Workstations), 5 of them will be doing web browsing, 5 will be using email, 50 attempting to connect to the database and 9 using multimedia Servers illegally (Application: Supported Profiles).

8. Internet-Firewall link configuration:

9. Configuring the simulation statistics:

- **Creating the second scenario (Proxy)**

The second scenario is a duplicate of the first, but with some router rules avoiding particular packets from / to multimedia and data services. Later on we will see how this decreases the internet link throughput and database access time fair enough below the 1 second limit. Must leave all the values as they are, except the Proxy Server Information _ row 8 (Application Voice data) as multimedia, **using Proxy Server Deployed: No**.

- **Firewall Results**

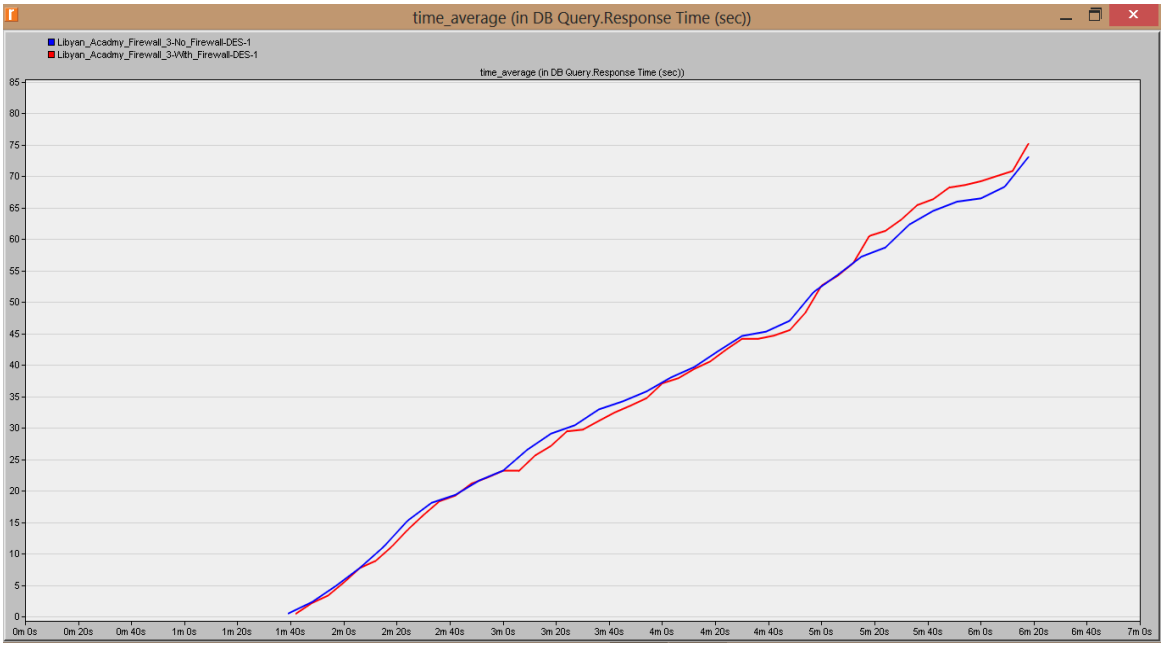


Figure (5.2)- Time Average in IP DB Query Response with Fire wall and without Firewall

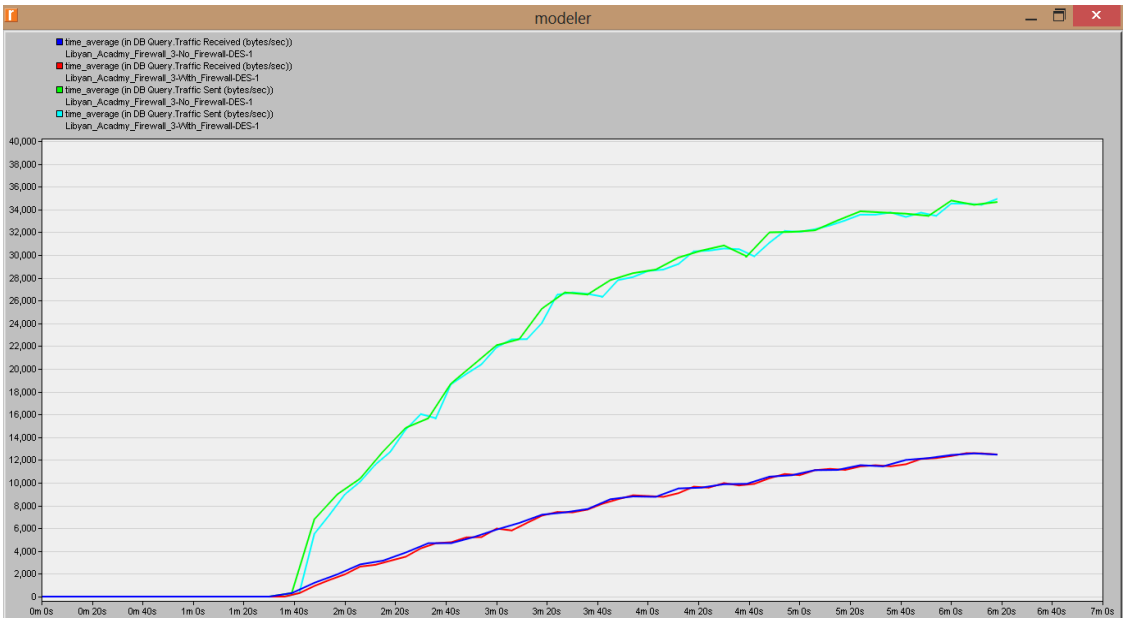


Figure (5.3)- Time Average in IP DB Query Traffic (Sent &Received)

The Fig (5.2) and Fig (5.3) give the Time Average in IP DB Query Response and average numbers of packets and bytes send and received in IP Data base Traffic. By the end of simulation it is observed that No-Firewall model gives more throughput than the Firewall model.

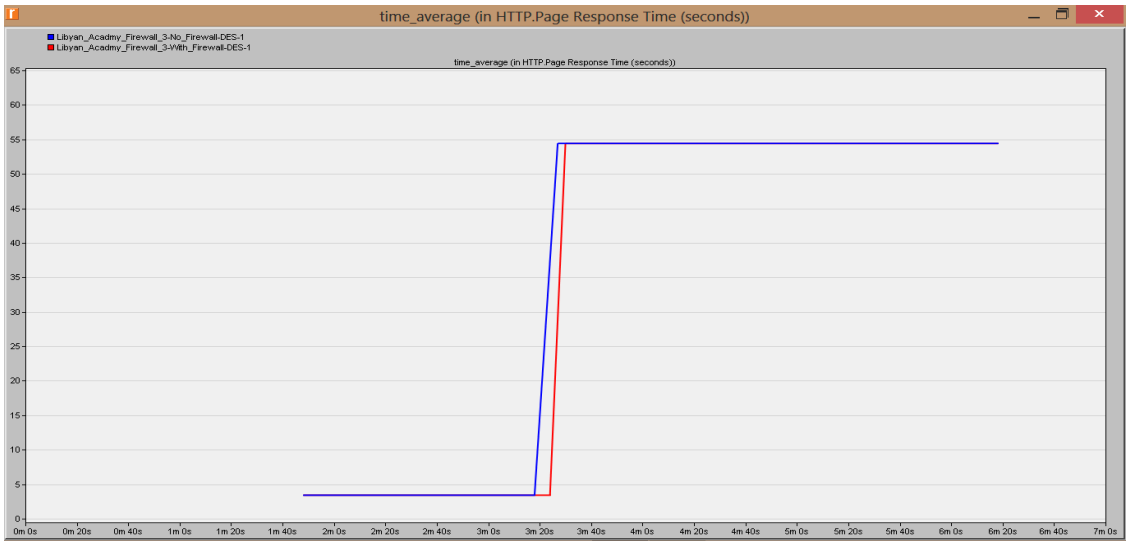


Figure (5.4)- Time Average in HTTP page Response

with Fire wall and with out Firewall

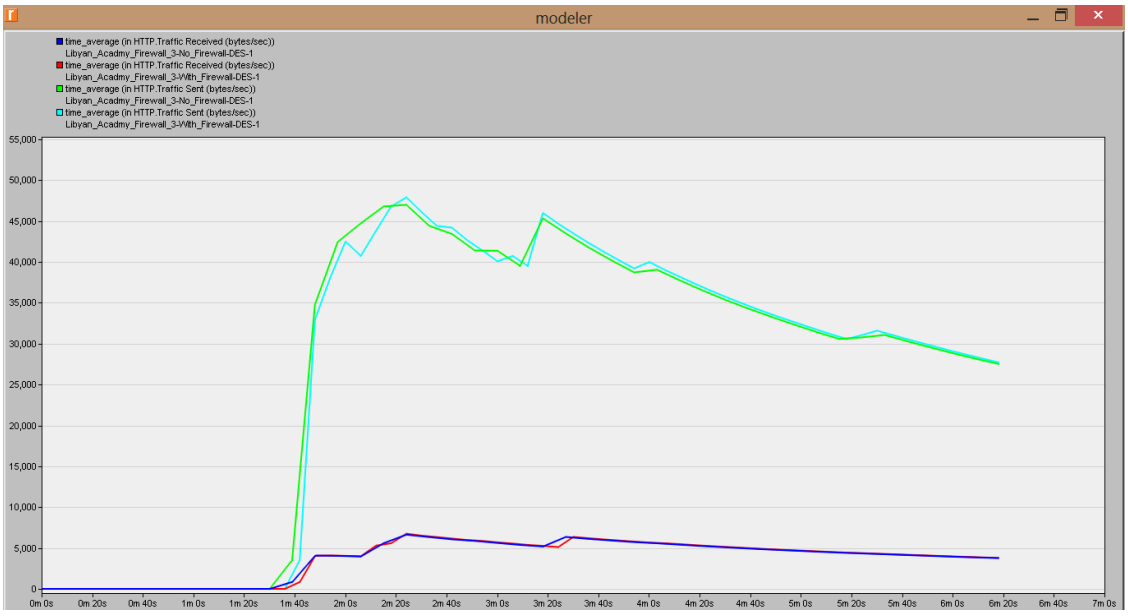


Figure (5.5)- Time Average in HTTP Traffic (Sent &Received)

with Fire wall and with out Firewall

The Fig (5.4) and Fig (5.5) give the Time Average in HTTP page Responseand average numbers of packets bytes send and received in HTTP Traffic. By the end of simulation it is observed that No-Firewall model gives more throughput than the Firewall model.

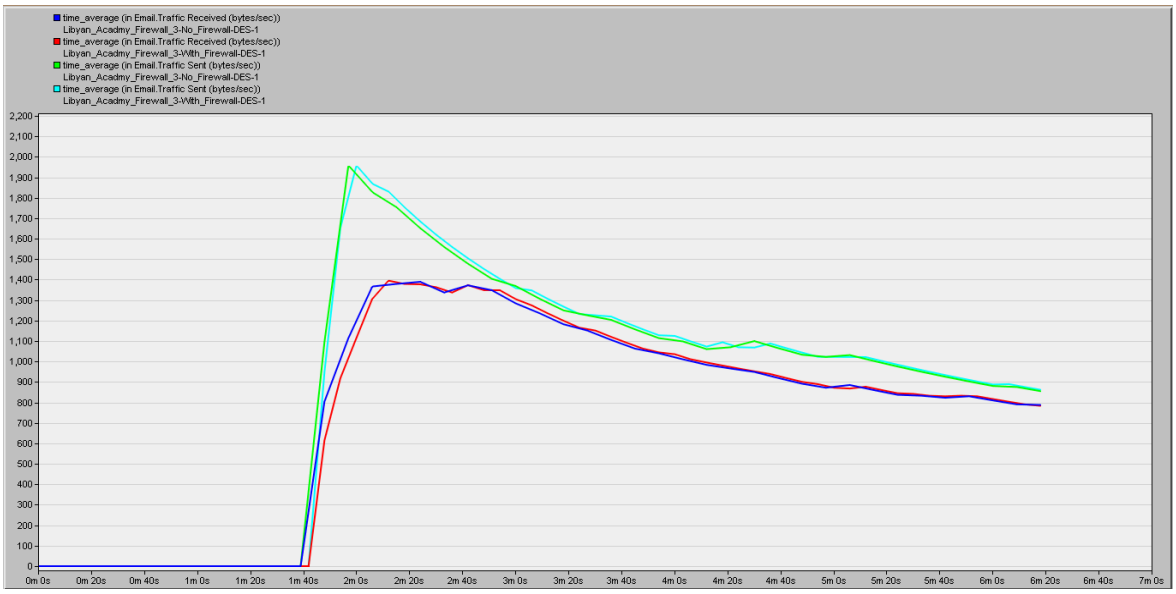


Figure (5.6)- Time Average in Email Traffic (Sent &Received)

with Fire wall and with out Firewall

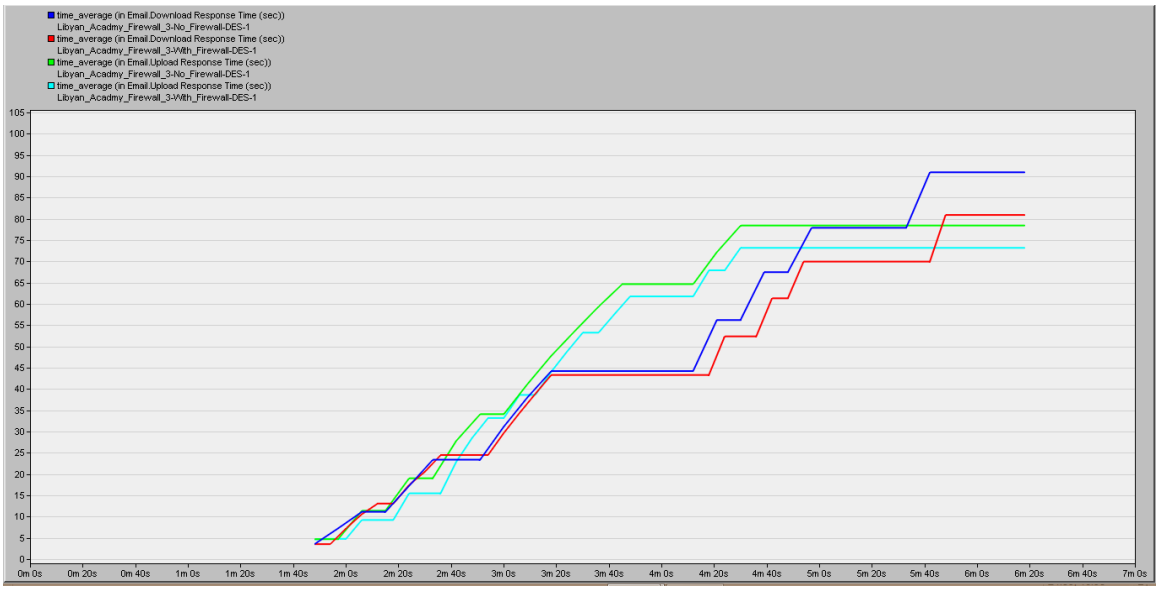


Figure (5.7)- Time Average in Email (Download & Upload)

with Fire wall and with out Firewall

The Fig (5.6) and Fig (5.7) give the Time Average in Email Traffic Response and average numbers of packets bytes send and received in Email Traffic and Time Average in Email (Download & Upload) . By the end of simulation it is observed that No-Firewall model gives more throughput than the Firewall model.

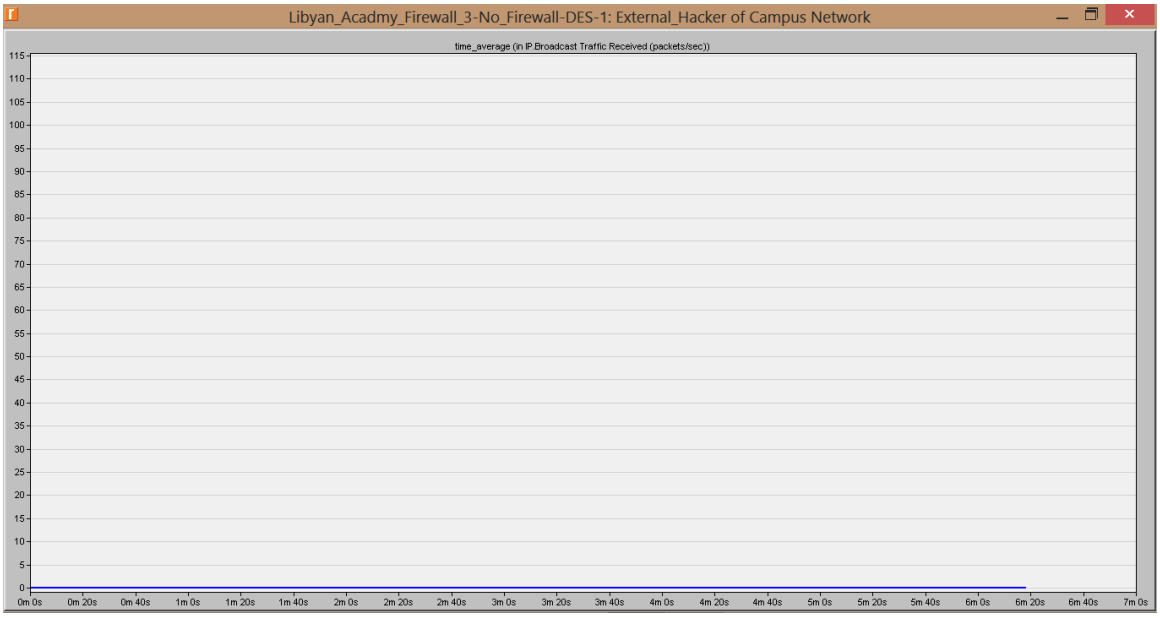


Figure (5.8)- Time Average in IP Broadcast Traffic Received.

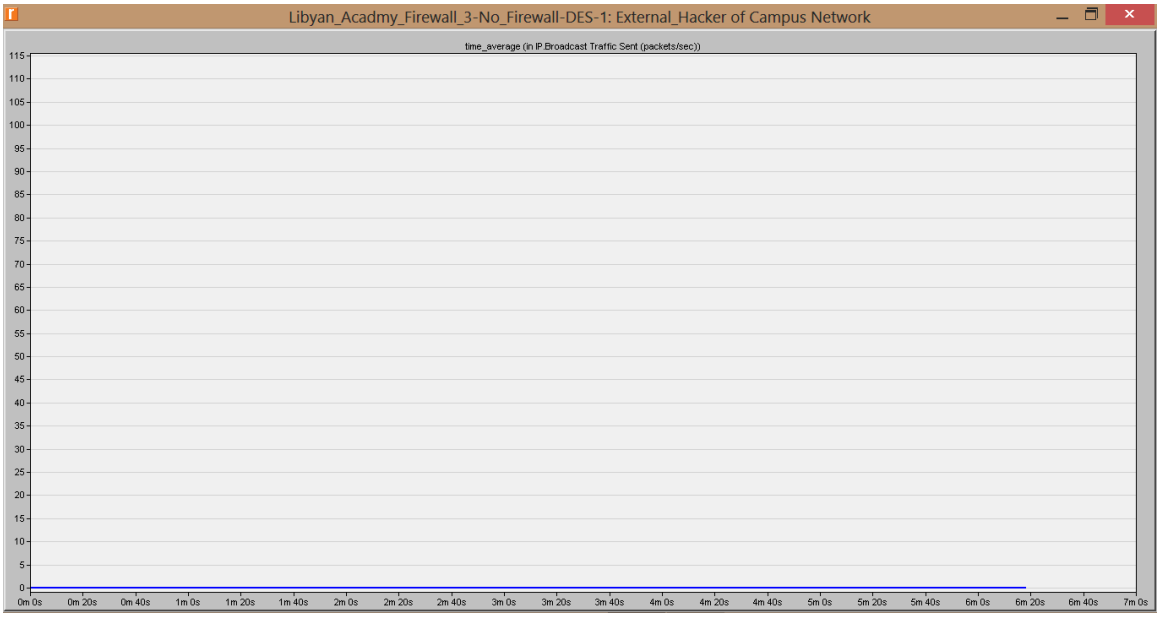


Figure (5.9)- Time Average in IP Broadcast Traffic Sent.

The Fig (5.8) and Fig (5.9) give Time Average in IP Broadcast Traffic for Attacker Response and average numbers of packets bytes send and received with Firewall model.

5.3. VPN Simulation

Point-to-Point Tunneling Protocol (PPTP) is a set of communication rules that allow by Libyan Academy to extend its corporative network using private tunnels through a public network as the Internet. As a result, users of branches have the same impression as if they were working with a WAN of their own, and they don't need to rent a private owned wide area communication line. However, the security is granted in a non-secure environment as the Internet is. This kind of connection is a Virtual Private Network (VPN).

PPTP is an extension of the PPP protocol (Point-to-Point Protocol). Users of branches can use an ISP provider to connect to a server of The Libyan Academy at the Internet.

VPNs use IP tunnels (*tunneling*), point-to-point virtual links between any two stations. The virtual link is created at the input router when the destination IP address is given. When the input router wants to transmit an IP packet using the virtual link, it encapsulates the packet into an IP datagram. The source and destination addresses of the IP datagram are those of the routers in between doing the encapsulation and desencapsulation.

A PPP client user will establish a call with an ISP (Internet Service Provider), the Front End Processor (FEP). The security of this connection is granted. The FEP and the PPP Client will negotiate a VPN tunnel with a remote PPTP Server

(Remote Access Server, RAS). The two peers are the Tunnel Source and Tunnel Destination. The Tunnel Destination is always a remote PPTP Server.

Lab scenario

VPNs is using to achieve communication security when communicating with the central site of The Libyan Academy, and to use the Internet infrastructure as well, in order to have lower cost. This communication scheme has the Tunnel Source at the FEP.

- **Creating the scenario**

1. Open a Project in OPNET IT Guru Academic Edition (File_ New Project) with these parameters (use default values for the remainder**):**

• Project Name: Libyan Academy _VPN

• Scenario Name: No VPN

• Network Scale: Choose From Maps. Pick up the map of North Africa.

2. Deploying devices and controls in the scenario:

Place the components upon the grid as seen Figure (5.10) and Figure (5.11) shows the network created with the components.

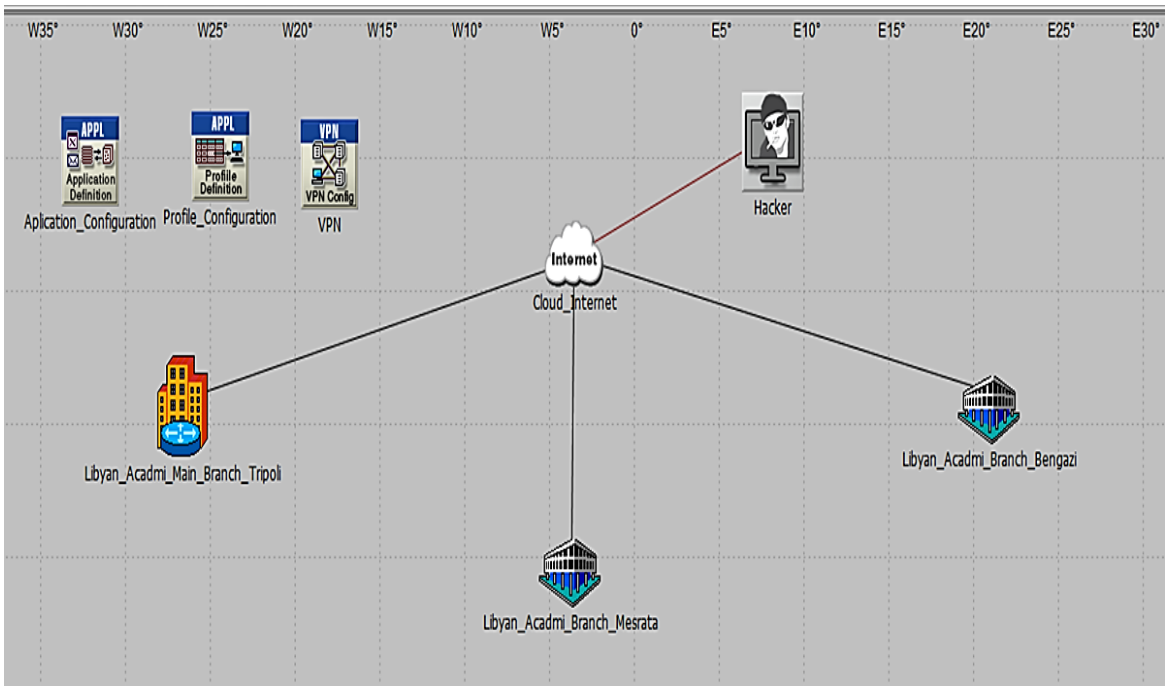


Figure (5.10) - VPN scenario For Libyan Academy Branches.

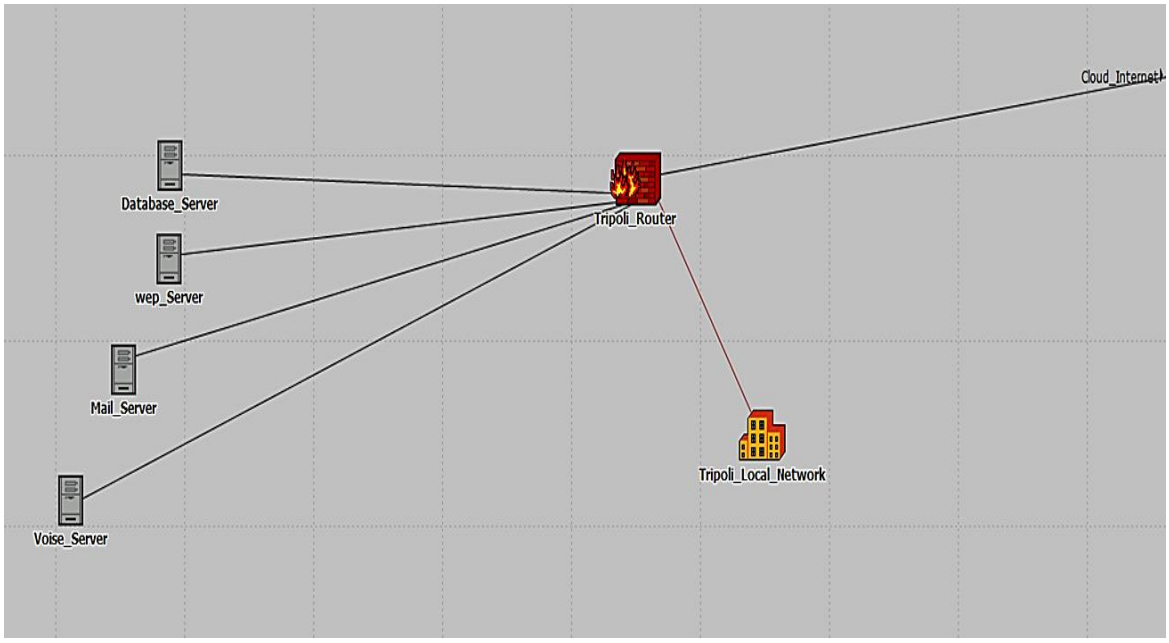


Figure (5.11) - VPN scenario For Internal Side of Libyan Academy – Tripoli Branch.

3. Defining applications, profiles and traffic demands:

Select Application Definitions: Default. This will create 8 new applications using heavy and light modes..

- Select Profiles from the Profile Configuration field. This will create 5 profiles. We want six, so Profile Configuration_rows = 6. Unfold the net row, row 6, and call it Profile Name: DB Access Profile and select the Database Access application (Heavy) .

- To create a Ping, open up the Object Palette and select the ip_ping_traffic Tool in palette internet_toolbox, and set the source and destination nodes of the ping for each one.

• Analyze the ping traces: Select all the ping demands (purple arrows), edit the Attributes using Ping Pattern: Record Route. Mark Apply Changes to Selected Objects to make changes on every selected component.

• Defining the services admitted by the servers**:** from Multiservice Server change the Application: Supported Services and select new dialog all the applications beside database access will be supported using Rows: 10 and inserting a different application for each row. to use all of them but Database Access (Heavy) and Database Access (Light).

• Do the same process for DB Server but with support the remaining applications: Database Access (Light) and Database Access (Heavy).

• Defining the profiles of the Stations.

Assign the following profiles to the Servers:

Table (5.2) - Servers Profiles

Nodes	Application: Supported Profiles
Station 2, Station 5 and Station 10	DB Access Profile
Remaining stations	Engineer

• Program the Firewall Proxy to deny the Database application traffic. Edit the Firewall Attributes, unfold the Proxy Server Information_row 1 (for this application) and indicate Proxy Server Deployed: No. The remaining applications can go across the device, so we will write Proxy Server Deployed: Yes to the remainder. The only one with default values to Proxy Server Deployed: No is Remote Login.

4. Assigning IP addresses to all the interfaces:

From the Project Editor, Protocols_IP_Addressing_Auto-Assign IP ddresses.

5. Assigning the default router to stations and DB Server:

Select Stations 7,8 and 9 and DB Server. change the parameter IP Hosts Parameters_Default Route by checking the IP address of the Firewall-to-Switch 1 interface. To find out the IP address of this interface, first click on the Switch 1 – Firewall link waiting for the yellow message to pop up. Once we have this

value we can find out the IP Address editing the Attributes of the Firewall and reading the value for IP Routing .

- **Creating the second and third scenarios**

1. Creating the VPN scenario using mode: Compulsory

Duplicate the scenario and define two VPNs creating the links Router 4 – Firewall and Router 2 – Network Server. The VPNs can be configured using Mode: Compulsory. This will make all the traffic generated by the stations will go past the VPN Server compulsory, even if it is not in the shortest path. The two VPNs will use encryption algorithms between the two VLANs, so the Encryption and decryption times will be different.

• Duplicate the scenario: from and rename new scenario Scenario Name: With VPN Compulsory.

• Edit the Attributes of the IP VPN Config control. Create two new rows into the VPN Configuration branch, once for each VPNS with these values:

2. Creating the scenario with Virtual Private Networks (VPNs) using mode: Voluntary

• Starting from the scenario VPN Compulsoryb we can duplicate it from the Project Editor doing Scenarios_Duplicate Scenario... with Scenario Name: VPN Voluntary.

• Edit the Attributes of the IP VPN control, and for each of the two rows that define the VPNs, change the field of Operation Mode to Voluntary.

Results of VPN Simulation.

Table (5.3)-Ping response times

Source	Destination: Google	Destination: Station 7
Station 1	No VPN: 0,02390 seconds Compulsory:: 0,06933 seconds Voluntary: 0,02390 seconds	No VPN: 0,03146 seconds Compulsory:: 0,04919 seconds Voluntary: 0,03146 seconds
Station 4	Sense VPN: 0,02301 seconds Compulsory: 0,03798 seconds Voluntary: 0,02301 seconds	Sense VPN: 0,03057 seconds Compulsory: 0,03099 seconds Voluntary: 0,03057 seconds
Station 10	Sense VPN: 0,01807 seconds Compulsory: 0,01807 seconds Voluntary: 0,01807 seconds	Sense VPN: 0,02562 seconds Compulsory: 0,02562 seconds Voluntary: 0,02562 seconds

1- High security, because just encryption packets will go across a Tunnel Destination and it need to decryption at Destination.

2- If we don’t care about security, the path with the less number of hops can never be VPN Compulsory because it needs to go across a Tunnel Destination and then take a longer way to come back. For this reason, the shortest and faster path will always be without VPNs.

3- When using VPNs, a short delay appears due to the encryption and decryption lags. This thing would never have happened without VPNs. As we can see, the Response Time is not affected by the VPN mode (Compulsory/Voluntary).

5.4. Dual-Homed Router and Host Simulation

Dual-Homed Router

The most simple security scheme a router filters the traffic between Internal Network private as (Tripoli Branch) and External Network as (Bengazi Branch) by Internet.

Filtering is performed at layer 3 with Access Control Lists (ACLs), frame filtering rules. We can permit/deny the pass of packets depending on these parameters:

- Protocol: TCP, IP, ICMP, RIP,...
- Source/Destination IP Address
- Source/Destination port

Dual-Homed Host

• Application Layer filtering (as a proxy)

• Router has now two functionalities: packet filtering and routing. Performance is reduced.

• Easier to use and to maintain log files.

Lab Scenarios

In this Lab we will simulate a scenario with Dual-Homed router and a scenario with Dual-Homed Host. In order to test all the possibilities of these technologies we will create an internal and an external network, with two servers each (FTP and HTTP).

The FTP Server of the internal network is supposed to be confidential: we don't want any illegal Access to it (either internal (Tripoli) or external(Bengazi)).

- **Creating the scenario**

1- Open a new OPNET IT Guru Academic Edition Project.

• Project Name: The Libyan Academy _Dual Hommed Router i Host

• Scenario Name: No Filters

• Network Scale: Office

Network Components: - as the table (5.4) and Figure (5.13) .

Table (5.4) - Network components

QTY	Component	Pallette
7	m_Int_wkstn	Sm_Int_Model_List
4	Sm_Int_Server	Sm_Int_Model_List
4	ethernet4_slip8_gtwy	internet_toolbox
1	ip32_cloud	internet_toolbox
2	ethernet16_switch	internet_toolbox
1	Sm_Application_Config	Sm_Int_Model_List
1	Profile Config	internet_toolbox
	PPP_DS1	internet_toolbox
	100BaseT	internet_toolbox

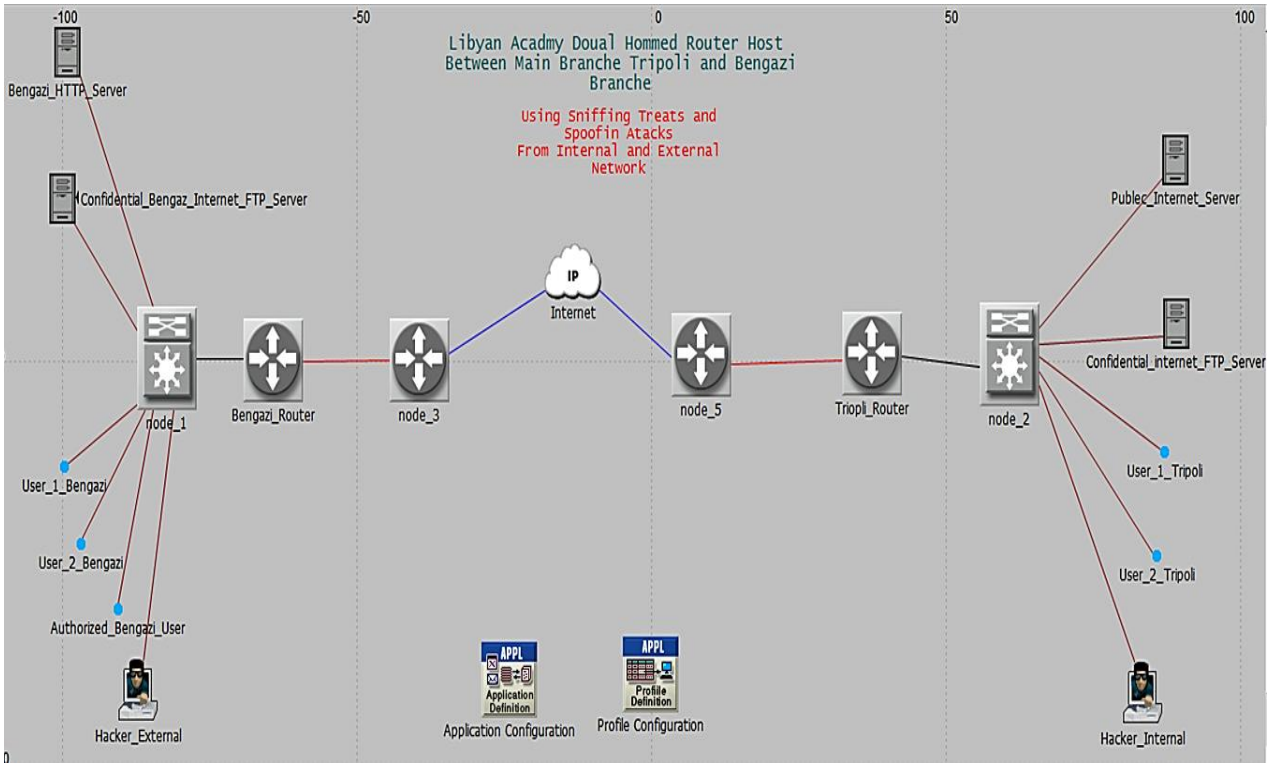


Figure (5.12) - Dual-Homed Router and Host Scenario.

4. Configuring the profiles

Create two profiles (FTP Profile and Web Profile) to accept all the FTP/Web Browsing applications (Heavy and Light).

5. Associate the profiles to the workstations:

• Assign FTP Profile to External Hacker, Internal Hacker, Authorized External User and Internal User #2 , and Assign Web Profile to Internal User #1, External User #1 and External User #2.

4. Change the Server Address parameter at the Attributes.

5. Set the preferential station destinations.

6. Assigning services to servers.

7. Assigning addresses.

8. Programming the routing tables.

9. Defining the simulation length.

Set Duration 15 minutes at Configure/Run Simulation.

Results of Dual-Homed Router and Host Simulation.

Ping's success of Dual-Homed Router and Host are:-

Table (5.5) -Ping's success

	Internal User (Tripoli)#1 TO External HTTP Server (Bengazi)	**External User (Bengazi)#1 TO Public Internal HTTP Server (Tripoli)**	**Internal User (Tripoli)#2 TO Confidential Internal FTP Server (Tripoli)**	**External User (Bengazi)#1 TO Confidential Internal FTP Server (Tripoli)**
No Filters	YES	YES	YES	NO
Dual Hommed Router	YES	YES	YES	NO
Dual Hommed Host	YES	YES	YES	NO

5.5. Screened Host / Screened (DMZ) Simulation

- **Screened Host**

• Filtering at Layer-3 (packets) and Layer-5 (application)

• Packet filtering is performed by routers

• A Firewall (aka bastion host) at the internal network acts as a proxy and establishes external and internal connections

• Parametrical security (incoming/outgoing messages)

• The router is used to limit the quantity of traffic to the bastion host, rejecting certain packets specified at the router's security policy

- **Screened Subnet (DMZ)**

•Parametrical and internal security.

• The same router of Screened Host (external firewall) protects the server against external attacks.

• An additional router (internal firewall) protects the server against internal attacks.

• As a result we have a Demilitarized Zone (DMZ). All the traffic accessing this area has crossed a router (the external network traffic as well as the internal network traffic).

• Connections controlled by the proxy depend on the security level we want to obtain.

Lab Scenarios

To create a scenario using Screened Host, We will create an internal network (Tripoli) with an FTP, HTTP and DB Server, and an internal network with a DB and FTP Server, and a HTTP Server. We want to protect the internal DB and FTP Server against two kinds of attacks: internal and external. Additionally we want to permit the traffic to the HTTP internal server.

- **Creating the Scenario**

1. Open a new Project in OPNET IT Guru Academic Edition (File_ New Project)

Using the following parameters:

• Project Name: Libyan Academy_Screened

• Scenario Name: ScreenedHost

• Network Scale: Office

2. Deploy the following components on the scenario:

Table (5.6) -Components of Screened network.

Qty	Component	Pallette
1	ip_32_cloud	internet_toolbox
1	Application Config	internet_toolbox
1	Profile Config	internet_toolbox
1	IP Attribute Config	internet_toolbox
2	ethernet4_slip8_gtwy	internet_toolbox
1	ethernet2_slip8_firewall	internet_toolbox
2	ethernet16_switch	internet_toolbox
4	Sm_Int_wkstn	Sm_Int_Model_List
3	Sm_Int_Server	Sm_Int_Model_List
	PPP_DS1	internet_toolbox
	100BaseT	internet_toolbox

3. Place the components on the scenario as the figure (5.13)

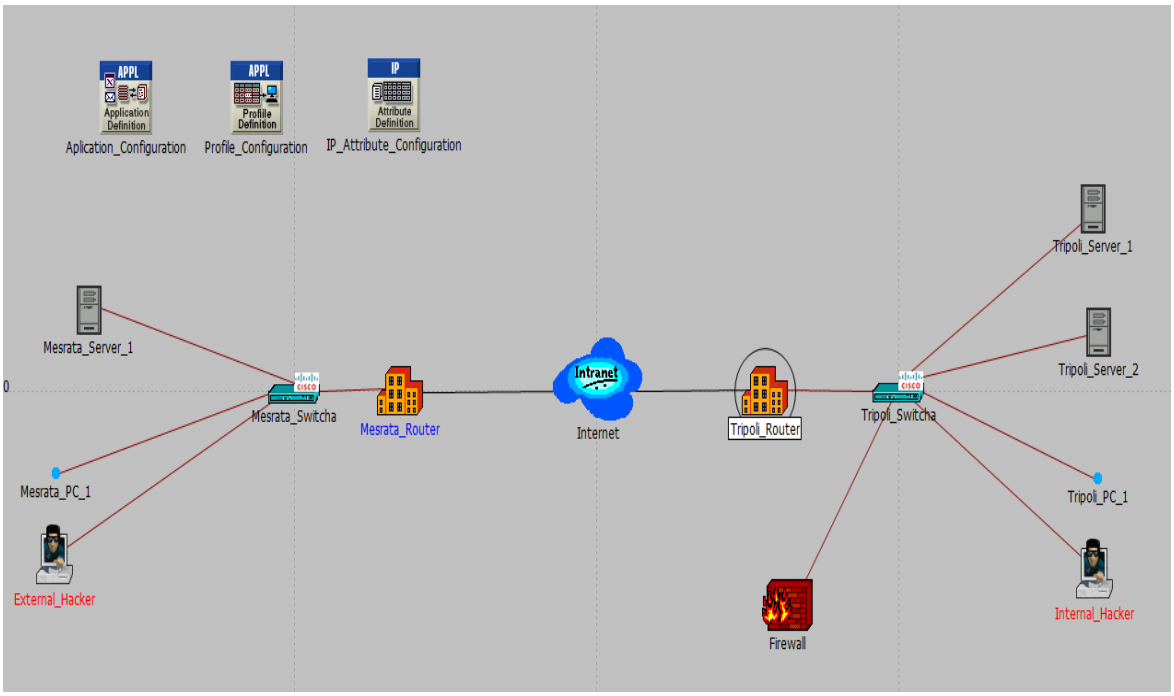


Figure (5.13) -Screened Host Scenario.

Rename the nodes as seen in the picture, because we will refer to them by their name hereinafter. The Internal Station #1 will be a hacker in the internal

network (Tripoli). External Station #2 will be a hacker in the external network (Mesrata) as well.

4. Assigning IP addresses to all stations, interfaces and sub interfaces:

5. Assigning a default gateway to stations and servers:

6. Configuring the Application Config control:

7. Configuring the Profile Config control:

8. Assigning applications and services.

9. Assigning profiles to the workstations.

10. Assigning the Attribute Server Address on all servers.

11. Assigning application demands.

12. Editing the static routing table and filtering rules of the Proxy.

13. Editing the static routing table of Tripoli Router.

- ## Creating the second scenario

1. Duplicate the scenario:

From the Project Editor Duplicate Scenario with Name: Screened Subnet With DMZ.

The new scenario is the same as we have so far, but this time the internal Stations of Tripoli will be connected to Switch 2 through an ethernet_4_slip8_gtwy router(at internet_toolbox pallette), which will link them to the Proxy. The internal users will be at a switched LAN with ethernet16_switch (at internet_toolbox palette). The new link's wires will use 100BaseT (at Links palette). The server's layout will be the same as we have (DMZ).

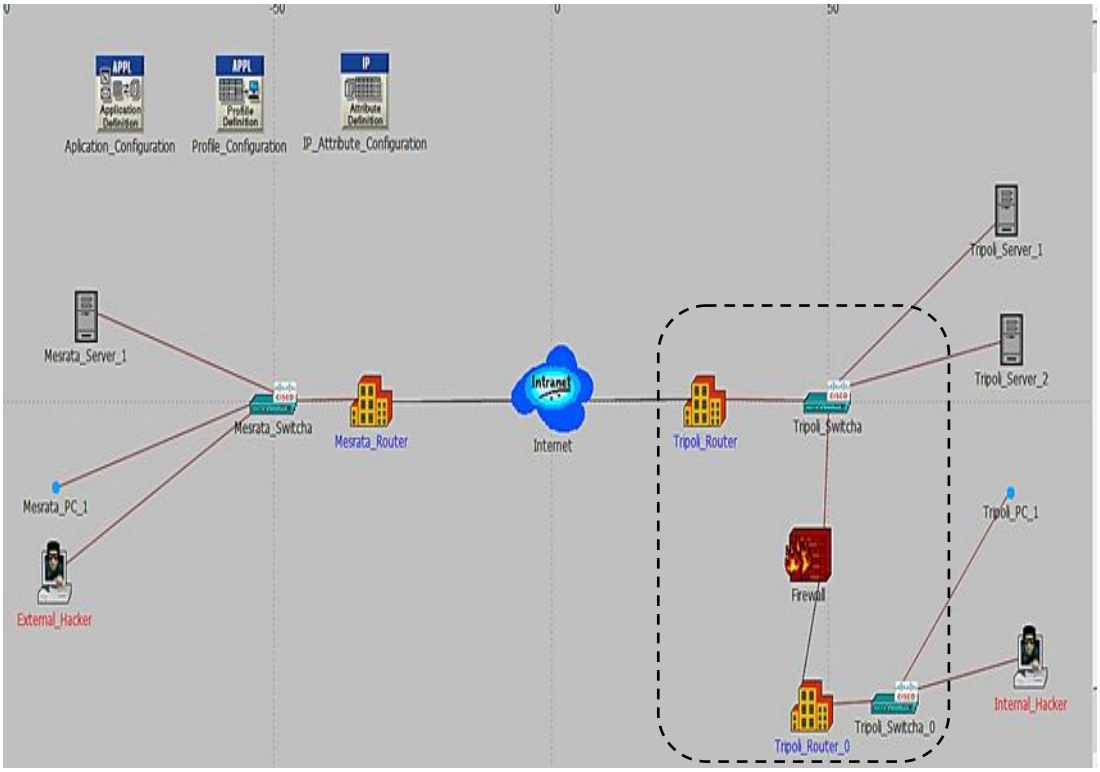


Figure (5.14) - The scenario Screened DMZ.

2. Assigning IP addresses again:

Create the network 213.190.1.0/25, separated of 213.180.1.0 (only servers will be at here now). Now this network is called Demilitarized Zone (DMZ) because is isolated from external and internal attacks. Another network is created: 190.20.20.0/24, between Tripoli Internal Router #2 and Proxy.

3. Assigning an ACL to Tripoli Internal Router #2:

The security policy of our network still being the same: we have to avoid access to Tripoli Internal Server #1 (FTP and DB server). We will create an ACL at Internal Router #1, where:

• The Incoming Traffic At DMZ list denies all traffic sent to Tripoli Internal Server #1(213.180.1.4) and permits all the remaining traffic.

• The Outgoing Traffic From DMZ denies outgoing traffic from Tripoli Internal Server#1, but permits the remaining outgoing traffic.

4. Assigning ACLs to interfaces at Tripoli Internal Router #2.
5. Creation of the routing table of Internal Router #2, and modification of the routing tables of Internal Router #1 and Proxy.
6. Reprogramming the ACL of the Internal Router.

Results of Screened Host/Subnet DMZ) Simulation

1- All interested traffic between the internal network and the external network go necessarily across the router and firewall.

IP Address	Hop Delay	Node Name
194.179.95.4	0,00000	Office Network.External Station #1
190.50.50.1	0,00005	Office Network.External Router
192.0.0.1	0,00070	Office Network.Internet
190.30.30.1	0,00068	Office Network.Internal Router
213.180.1.6	0,00005	Office Network.Proxy
213.180.1.5	0,00005	Office Network.Internal Server #2
213.180.1.5	0,00001	Office Network.Internal Server #2
190.30.30.2	0,00004	Office Network.Proxy
192.0.0.2	0,00005	Office Network.Internal Router
190.50.50.2	0,00070	Office Network.Internet
194.179.95.1	0,00068	Office Network.External Router
194.179.95.4	0,00005	Office Network.External Station #1

Figure (5.15) - ping from External Station #1 to Internal Server #2

2- It is impossible for an Internal Station to avoid the bastion host changing the default gateway

IP Address	Hop Delay	Node Name
194.179.95.4	0,00000	Office Network.Estació Externa 1
190.50.50.1	0,00006	Office Network.Router Extern
192.0.0.1	0,00137	Office Network.Internet
190.30.30.1	0,00068	Office Network.Router Intern
213.180.1.6	0,00005	Office Network.Proxy
213.180.1.2	0,00005	Office Network.Estació Interna 1
213.180.1.2	0,00001	Office Network.Estació Interna 1
190.30.30.2	0,00004	Office Network.Proxy
192.0.0.2	0,00005	Office Network.Router Intern
190.50.50.2	0,00070	Office Network.Internet
194.179.95.1	0,00068	Office Network.Router Extern
194.179.95.4	0,00005	Office Network.Estació Externa 1

Figure (5.16)- change the default route of Internal Station #1 pointing to 190.30.30.1

3- The traffic load rejected by the proxy increases if the ACLs of the router are disabled because this traffic use to be rejected by the router, i.e., connections to the Internal Server #1.

5.6. VLAN'S Simulation

VLANs (Virtual Bridged Local Area Network or Virtual LANs) are defined in the IEEE 802.1Q standard. They're used to divide a network in different logical virtual LANs .Each user belongs to a virtual LAN independent from his placement. Logical groups of users bring together network components spread all over the network into a common broadcast domain. Efficiency is increased, and collision domains are decreased. Each VLAN is identified by a VID (VLAN ID), an integer from 1 to 4094.

VLAN can be implemented mainly by bridges and switches (VLAN-aware).
The bridges and switches ports are divided in two types, regarding to their usage in VLANs:

• Access Ports: They're default ports. An access port can belong only to one VLAN, and the messages that go across the port will be untagged. They connect VLAN-aware devices with VLAN-unaware devices.

• Trunk Ports: Can interconnect VLANs. This way, frames from many switches can be exchanged, regardless of the VLAN they belong to. Frames across these ports are tagged.

The information about the LAN the frames belong to is transmitted only when frames are transmitted by the Trunk Port through the Trunk Link to the destination switch. In this case, the information about the destination LAN is inside the tag (header).
Frames going out of Access Ports do not have any tag, because there's only one VLAN per every Access Port. The tag identifying the VLAN membership is inside level 2 frames, between the MAC header and the payload.

Lab Scenarios

There are 2 scenarios, The first scenario studies the switch performance in a wired switched Ethernet network. The second scenario improves the switch Security performance by configuring VLANs.

- **Generate Scenario**

1. generate first scenario with name " No VLAN" same as Figure (5.17)
2. Duplicate the scenario and Rename it to "With _VLAN".

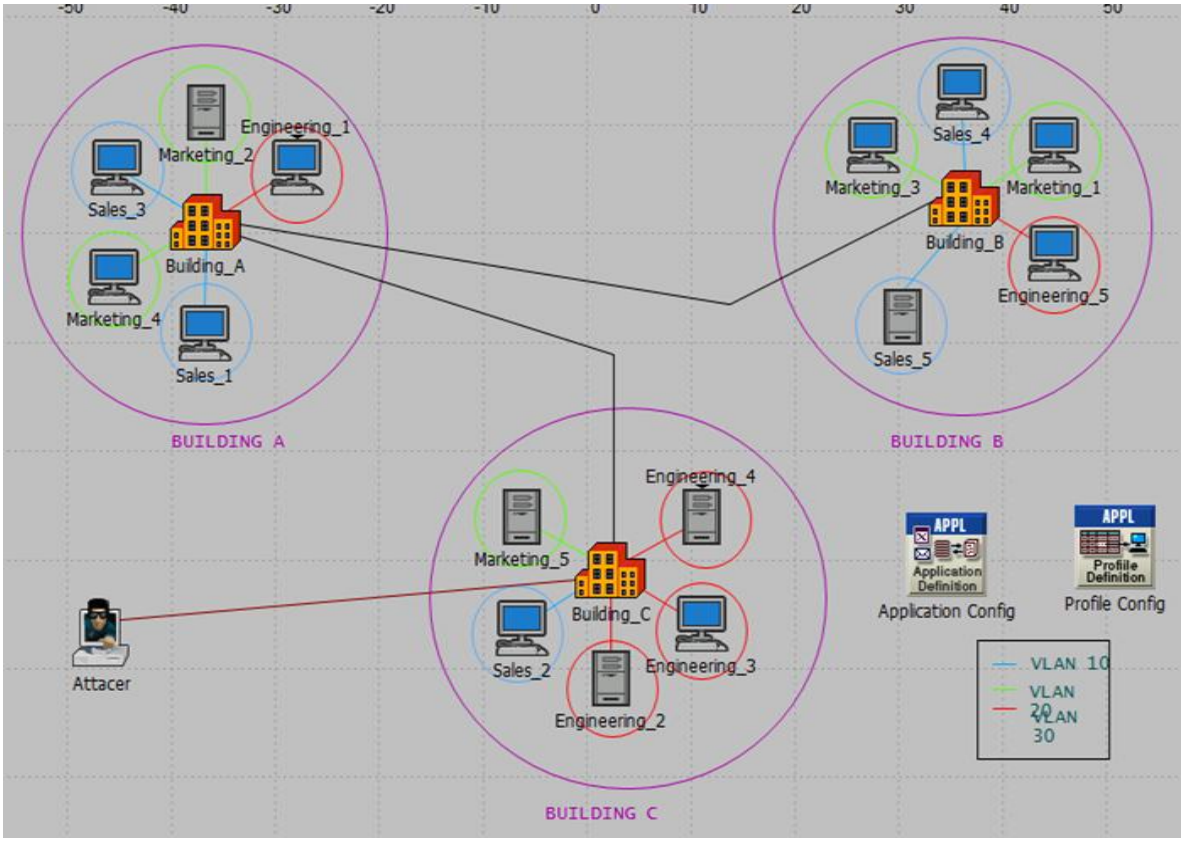


Figure (5.17) - VLAN scenario.

In this scenario, groups of users belonging to different divisions(Departments) – engineering, marketing, and sales – are connected to Ethernet LAN switches. These users hit a variety of servers running FTP, Database, HTTP, and email services. The users running these various applications between their workstations and servers.

Explore the attribute values of the Application Config and Profile Config to understand how the application traffic has been configured in this topology.

Expand **Switch Port Configuration**, and then, expand **P0** (or any row) to see other details and expand **VLAN Parameters** – verify the Scheme field is set to **Default**. This indicates no VLANs have been configured in the network.

Note the data rate of the links between Building_A&Building_C, and Building_A&Building_B with the units bits/sec.

VLAN Results

View output results: Application Response Times for Email and FTP applications as observed by end-user, and Switch throughput statistics.



Figure (5.18) –Email Downloaded / Upload and average Ftp Download /Upload

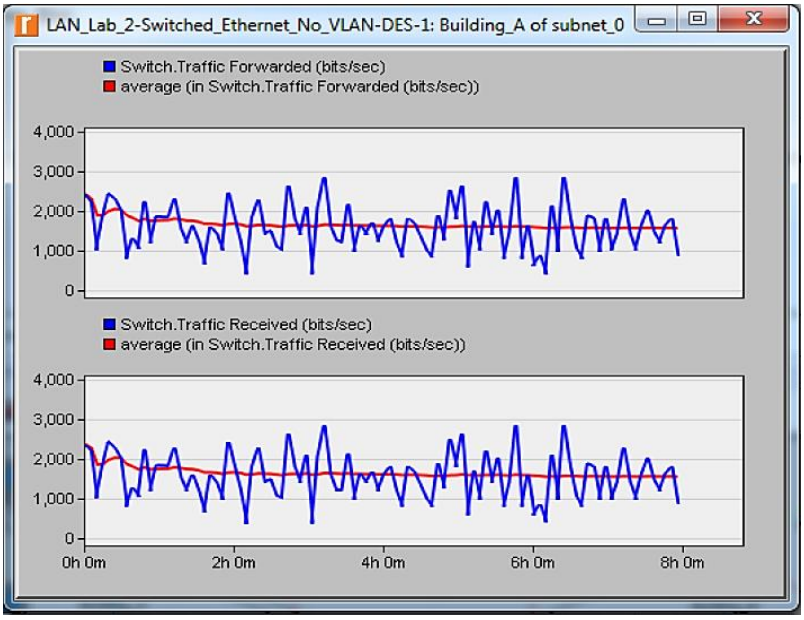


Figure (5.19) –Switch A Traffic forwarded / Received and average in Switch A Traffic forwarded / Received

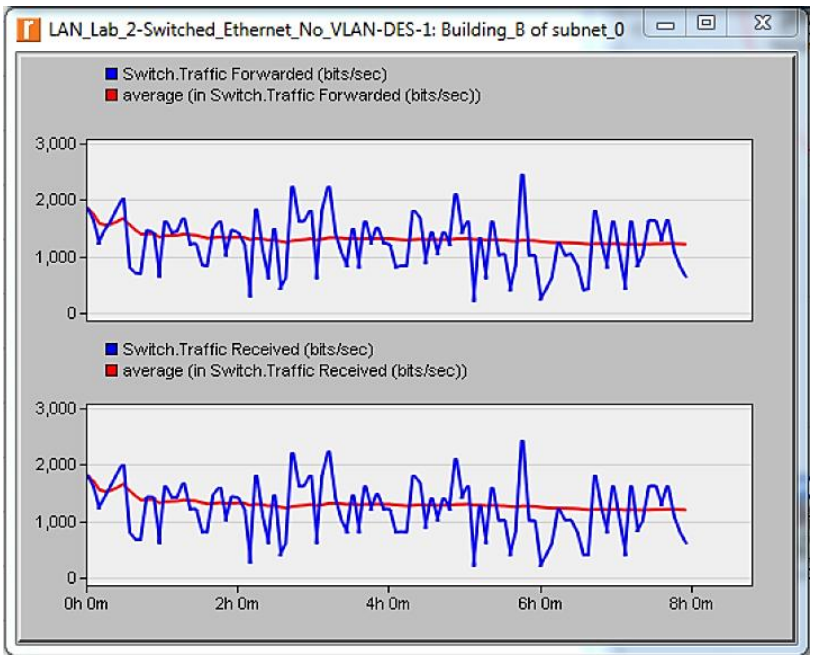


Figure (5.20) –Switch B Traffic forwarded / Received and average in Switch B Traffic forwarded / Received

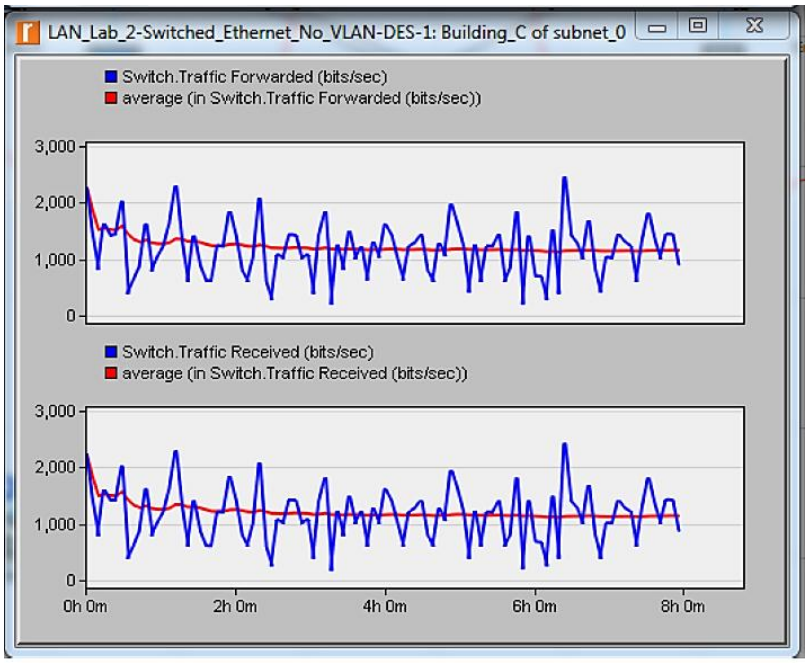


Figure (5. 21) –Switch C Traffic forwarded / Received and average in Switch C Traffic forwarded / Received

5.7. The Libyan Academy scenario

The network model for The Libyan Academy simulation consists from three Branches of The Libyan Academy that are located in three different cities at Libya country. The local area network (LAN) structure for all Branches is the same ,as shown in Figures (5. 22) , (5. 23) , (5. 24) , (5. 25) and (5.26).

In each LAN (three Buildings and in each Building are 5 workstations, one main switch called (Bay Networks Centilion100 Switch) and one router called (Cisco C4000 Router) connecting to IP cloud by bi-directional PPP_DS1 link. The workstations are connected to the switches by bi-directional 10Base_T links. The proposed network carries applications Data Base.

There are some important objects in OPNET that are used to simplify and facilitate the work with it. In this scenario, some of these objects that are used are Application Configuration and Profile Configuration as show in Figures

(5. 22) , (5. 23) , (5. 24) , (5. 25) and (5.26).

1. Application Configuration Object: is an object used to define and configure all Applications in the network according to the user requirements. OPNET has most common applications like: HTTP, E-mail, video, File transfer, Voice, database. In this scenario, there is one application in the network model is a Data Base.

2. Profile Configuration Object: is an object that can be used to create users profiles, profile can contains one or more applications and each application can be configured by the starting time and ending time. In this scenario, there is only one profile to all users called DB_ profile.



Figure (5. 22) - The Libyan Academy scenario Architecture.

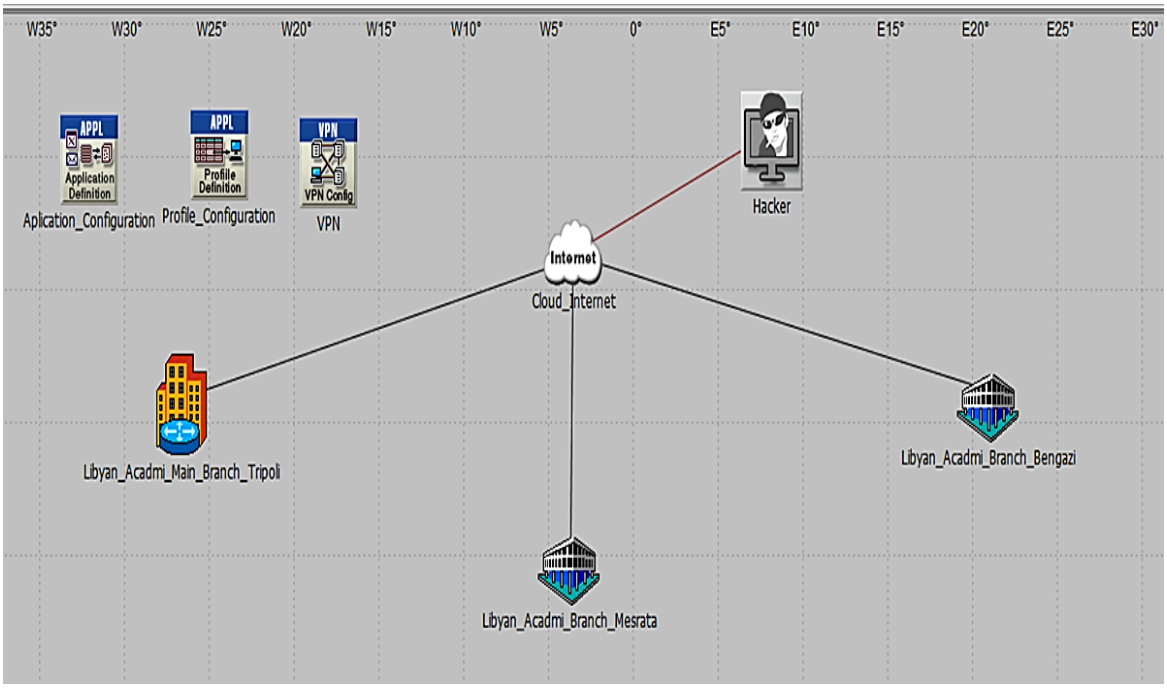


Figure (5. 23) - The Libyan Academy scenario Simulation.

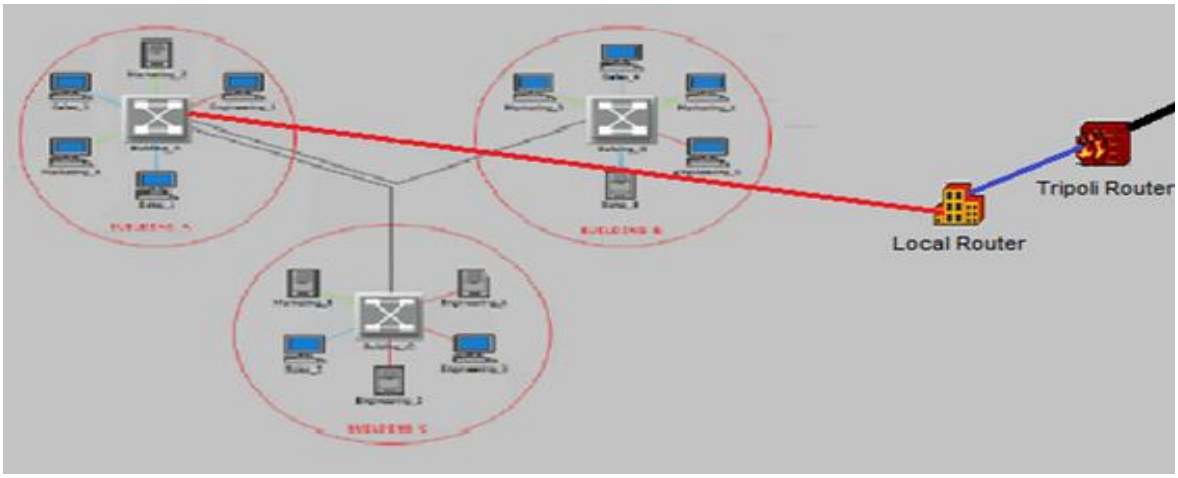


Figure (5. 24) – Main Branch **(**Tripoli) Simulation.

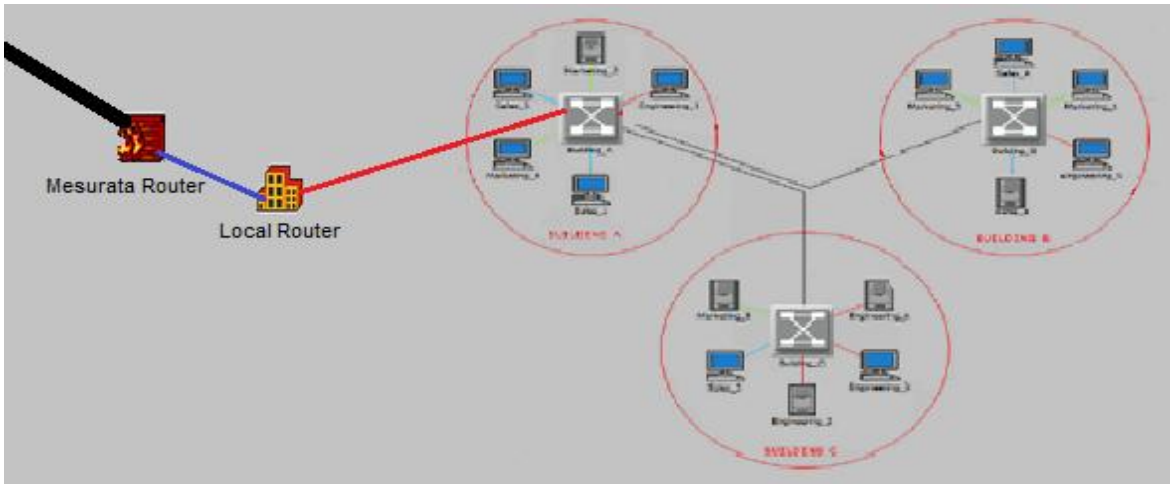


Figure (5. 25) – Mesurata Branch Simulation.

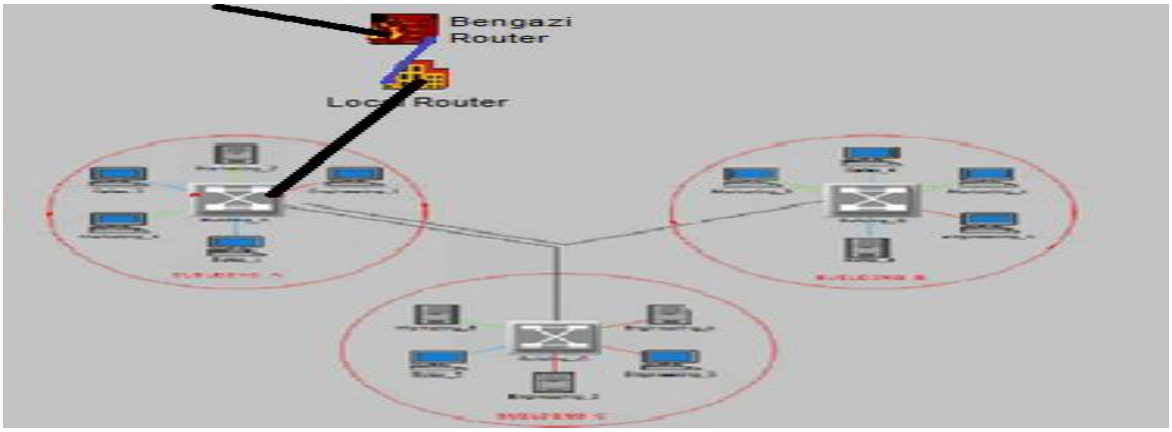


Figure (5. 26) - Bengazi Branch Simulation.

Network Simulation Results and Discussions :

In this scenario, a Comparison between the effect of some Security Mechanisms like Packet Filter Firewall and VPN on the DB Qos. To measure the QoS of the DB application and availability of attacks prevent during collected major factors those affect the DB QoS such as: delay (sec), jitter (sec), traffic sends (packet/sec) and traffic received (packet/sec). The duration of simulation is 8 minutes and the results are obtained as shown in figures (5.27) **,** (5.28) **,** (5.29) and (5.30) . those represented the Comparison between Firewall

and VPN in DB Network, The blue line represent using Firewall; whereas the red line represent using VPN.

Figure (5.27) shows the Jitter using Firewall and VPN did not exceed the time constraint (0.075 sec), Figure (5.28) shows the end to end delay using Firewall did exceed the time constraint (0.15 sec) but using VPN did not exceed the time constraint (0.15 sec) , Figure (5.29) shows the DB traffic received using Firewall = 200 Packets/sec) and the DB traffic received using VPN = 200 (Packets/sec), Figure (5.30)shows the DB traffic sent using Firewall = 200 Packets/sec and the DB traffic sent using VPN = 200 (Packets/sec).

Figure (5.28) shows using the packet filter firewall degrade QoS where introduce end to end delay exceed the time constraint (0.15 sec) because the firewall will inspect each packet that passes through it. But using the VPN is end to end delay does not exceed the time constraint (0.15 sec) because the firewall will not filter the traffic because the IP packets in the tunnel will be encapsulated inside an IP datagram. In both cases (firewall and VPN) no packet loss and jitter has acceptable ratios. VPN introduces better QoS from the traditional firewall; therefore NPN is more suitable to DB network.

Different parameters captured to security mechanisms (traditional firewall and VPN) are summarized in Table (5.8).

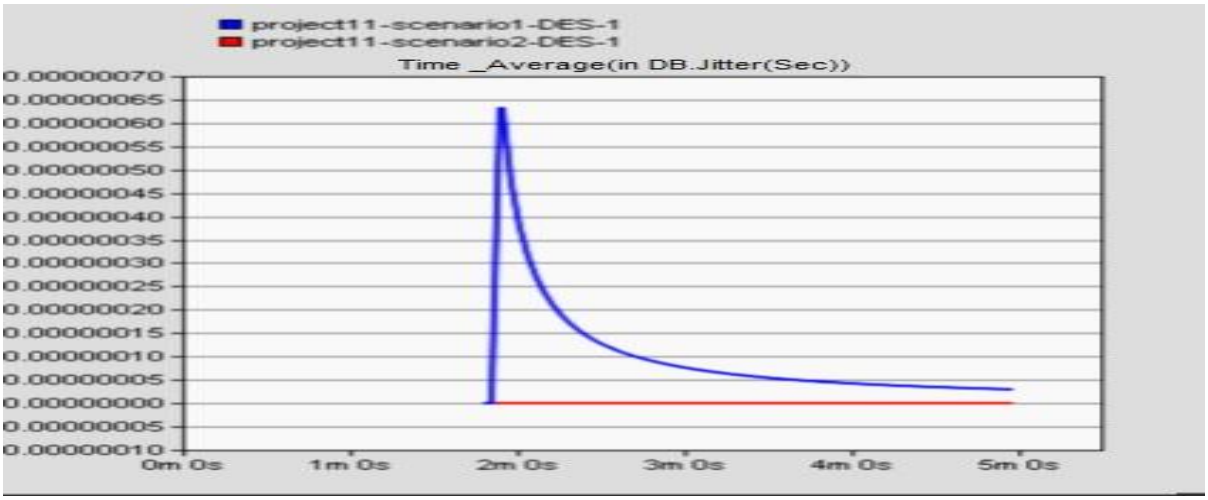


Figure (5.27) - DB Jitter.



Figure (5.28) -DB Packet end to end delay.

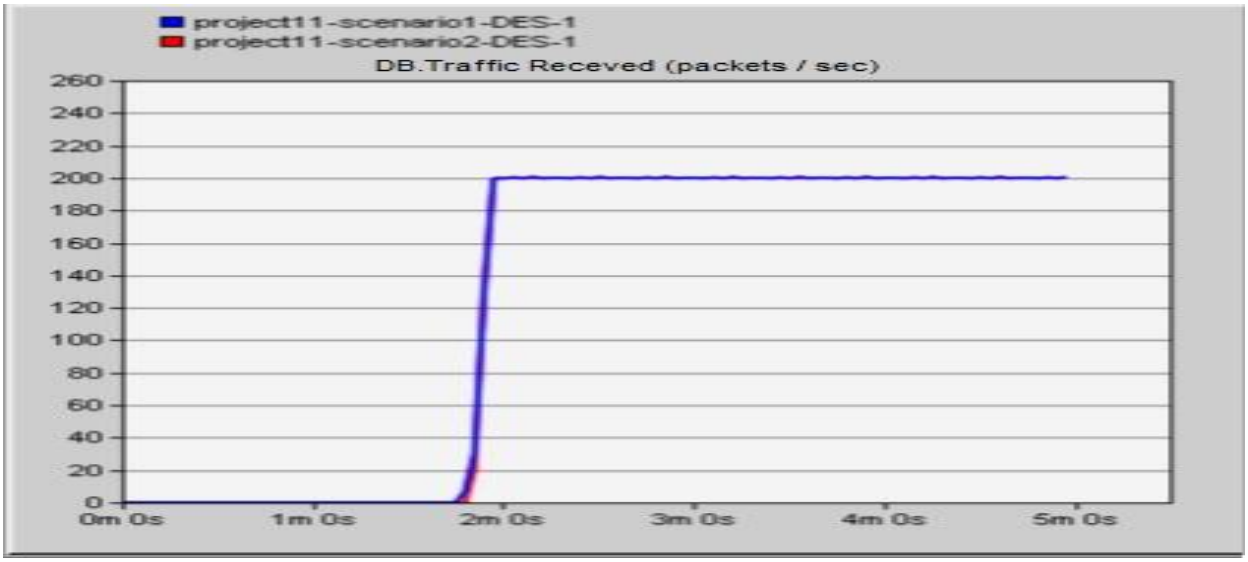


Figure (5.29) - DB Traffic Received (packet/sec)

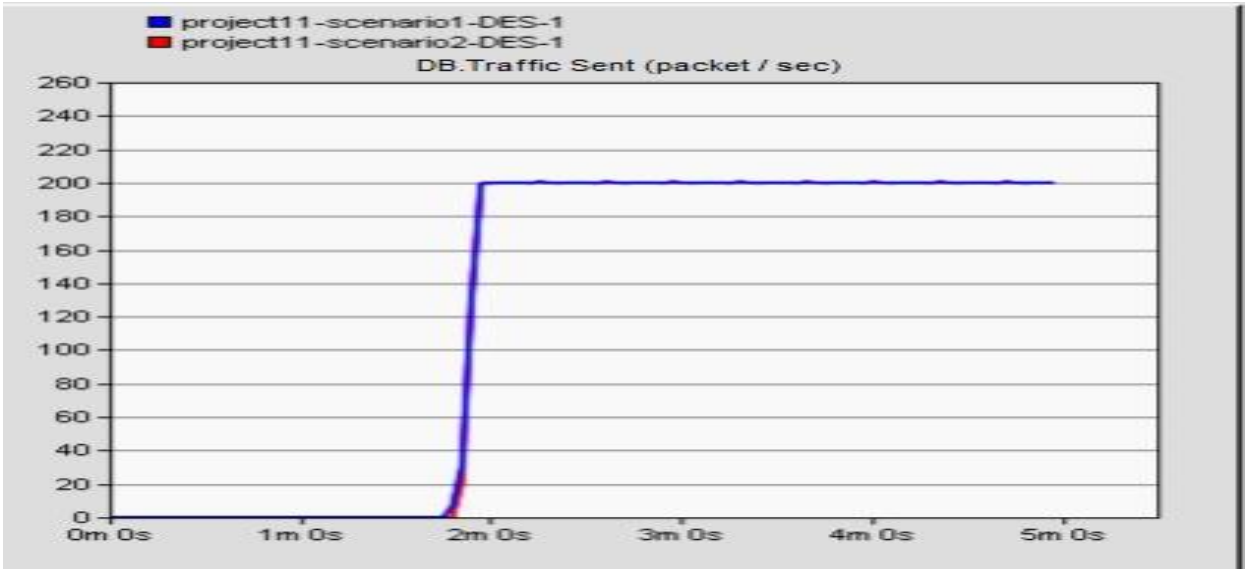


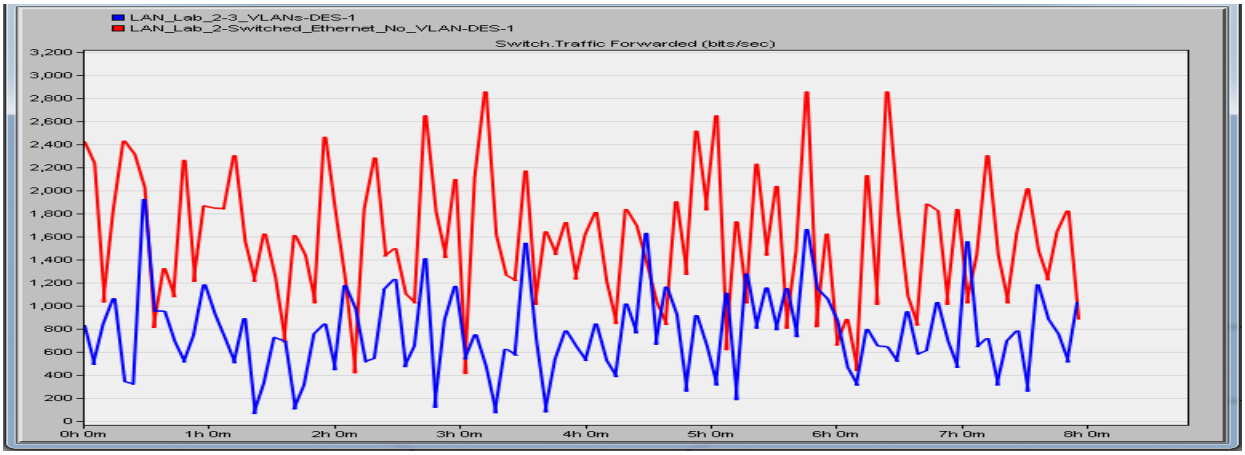
Figure (5.30) - DB Traffic Send (packet/sec**)**

Table (5.7)- Comparison between Effect Firewall and VPN on DB QoS.

Parameters	**Firewall**	**VPN**
DB Jitter (sec)	0.00000060	0.0
DB packet End-To-End Delay(sec)	0.186	0.106
DB Traffic Received (packet /sec)	200	200
DB Traffic Sent (packet /sec)	200	200
Packet loss by Sniff or spoof	0.0	0.0

From the result summarized in Table (5.8), Traditional Firewall will cause degrade QoS by introduce delay with unacceptable ratio. While the VPN best QoS from Firewall in DB networks where introduce delay with acceptable ratio not exceed constraint (0.15 sec). Consequently, running DB over a VPN can ensure security and high QoS.

Figure (5.31) shows Comparison between Effect of Traffic Forwarded (bits/ sec) with VLAN and without VLAN on execute time (8:00 H).



(5.31) - Traffic Forwarded (bits/ sec) with VLAN and without VLAN.

Figure (5.32) shows Comparison between Effect of average point- to – point delay (sec) with VLAN and without VLAN on execute time (8:00 H).

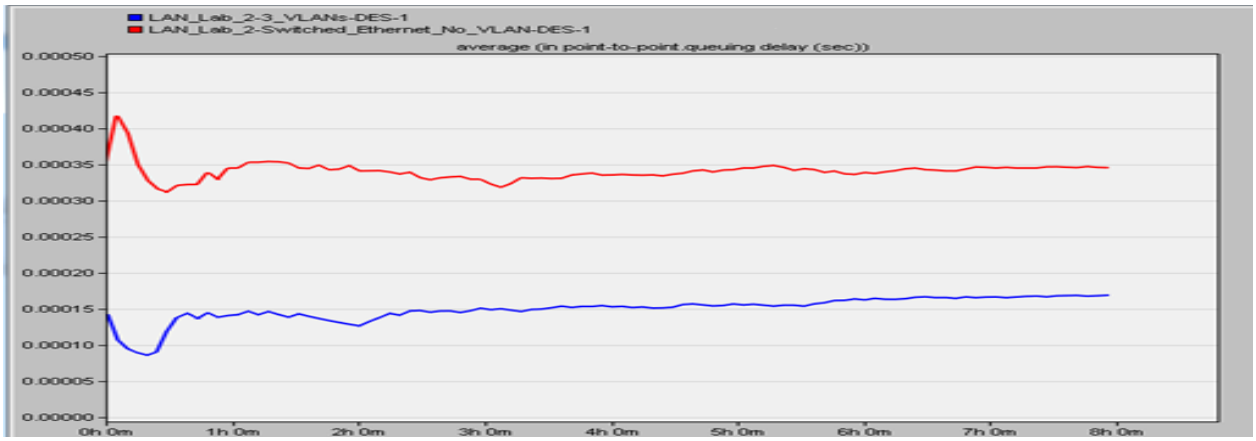


Figure (5.32) - average point- to – point delay (sec) .

This chapter presents the conclusions drawn from the obtained results. It also discusses briefly the potential for future research work.

7.1. Conclusion

- **Firewalls** must be maintained regularly to assure critical measures of success are kept within acceptable levels of performance and Successful firewall management requires adherence to principles that have been put forth by reputable organizations to ensure that firewalls and network security configurations are maintained correctly.

- **VPN** is High security, because just encryption packets will go across a Tunnel Destination and it need to decryption at Destination. If we don't care about security, the path with the less number of hops can never be VPN Compulsory because it needs to go across a Tunnel Destination and then take a longer way to come back. For this reason, the shortest and faster path will always be without VPNs and When using VPNs, a short delay appears due to the encryption and decryption lags. This thing would never have happened without VPNs.

- The parametric security offered by **(Dual-Homed and Dual-Homed Host)**

Table (6.1) - The parametric security of (Dual-Homed and Dual-Homed Host)

	NoFilters	DualHommed Host	DualHommed Router
Can Authorized External User Have access to Confidential FTP Server?	YES	YES	YES
Can External Hacker attack Confidential FTP Server?	YES	NO	NO
Can Internal Hacker attack Confidential FTP Server?	YES	YES	YES

.

- The parametric security offered by **Screened Host** with the parametric security and internal security as well offered by **DMZ**, **I**nternal attacks can be avoided only with DMZ.

Table (6.2) - The parametric security of (Screened Host and Screened DMZ).

Scenario	Internal Station #1	External Station #2
ScreenedHost	Yes	No
ScreenedSubnetAmbDMZ	No	No

- Screened Subnet (DMZ) is much protected from Spoofing Attacks and Sniffing Threats, because we have a Demilitarized Zone (DMZ). All the traffic accessing this area has crossed a router (the external network traffic as well as the internal network traffic).

- With **VLAN** Efficiency is increased, and collision domains are decreased Because , Each VLAN is identified by a VID (VLAN ID), an integer from 1 to 4094.

- **The Conclusions** of the affects some of the Security Mechanisms such as Packet Filter Firewall , Virtual Private Network (VPN) and Virtual Local Area Network (VLAN) on the QoS of DB application using OPNET and analyzed simulations of the results allow to be made conclusions as follows: VPN gives best QoS from Firewall because the values of the parameters that effect on QoS such as: delay, jitter, packet loss to be within the acceptable range and with VLAN gives best QoS from NO VLAN .

7.2. Future Works

During the development of this study, several other aspects had been identified as potential points of further analysis.

1- Investigate and study on how to improve many software for sniffing an spoofing detection and prevention that work under operating systems.

2- Investigate and study on how to improve detection tools for sniffing and spoofing.

3- Write the functions and modules to implement the suggested proposal.

References

[1] Obunadike Georgina and Tyokyaa K. Richard ," Optimization of Computer Network for Efficient Performance ” Federal University Dutsinma , Nigeria, Department of Mathematical Sciences and IT, in 2015.

[2] Rajni Ranjan Singh and Deepak Singh Tomar , " Network Forensics: Detection and Analysis of Stealth Port Scanning Attack " Maulana Azad National Institute of Technology, Bhopal, India,in 2014.

[3] Dr. Abdul-Bary R. Sulaiman and Omar Kh. Salih Alhafidh ," Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering , College of Electronic Engineering, Computer and Information Dep. University of Mosul , Iraq, in 2014 .

[4] Hussein A. Mohammed and Adnan Hussein Ali " Effect of some Security Mechanisms on the QOS VoIP Application using OPNET " Electrical & Electronics Engineering Techniques College – Baghdad, in 2013.

[5] Mohammad Z. Ahmad, Mustafa I. Akbas, Damla " Design and development of a simulation environment in OPNET using High Performance Computing " University of Central Florida Baghdad, in 2013.

[6] An Engineer Sparsh Mittal, , " OPNET: An Integrated Design Paradigm for Simulations " ,Department of Electronics and Communications From Indian Institute of Technology ,in SEPTEMBER 2012,

[7] Some of Engineers of ," Sniffing Attacks Prevention and Detection Techniques in Wired and Wireless Local Area Networks (LAN) ", Computer department of BUID University, UAE, Dubai , in 2011.

[8] Sharmin Rashid, Subhra Prosun Paul,”Proposed Methods of IP Spoofing Detection &Prevention “,World University of Bangladesh, Dhanmondi, Dhaka, Bangladesh,2012.

[9] Elham Abu-ElShwashi," DATA SECURTY INSIDE THE Internet /Networks; Spoofing Issues ",Department Of Electrical and Computer Engineering, The Libyan Academy, Jul 2008.

[10] Daemon. IP Spoofing Demystified. Phrack Magazine Review, June 1996.

[11] Computer Incident Advisory Committee (CIAC). Advisory Notice F-08 Internet Spoofing and Hijacked Session Attacks, 1995.

[12] Richard Chow. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. International Journal of Network Security & Its Applications ,2009.

[13] Kevin Hamlen. Security Issues for cloud computing. International Journal of Information Security and Privacy, 2010.

[14] Cisco IOS XR Routing Configuration Guide for the Cisco XR 12000 Series Router, Release 4.1, Retrieved 13:55, NOV, 2015. from http://www.cisco.com.

[15] MUHAMMAD NAEEM ASLAM YASSAR AZIZ , " Traffic Engineering with Multi-Protocol Label Switching", 2008.

[16] D. O. Awduche, "MPLS and Traffic Engineering in IP Networks," University of Minnesota, IEEE communication magazine, December 1999.

[17] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford "Traffic Engineering for IP Networks", Network, IEEE, March-April 2000.

[18] Yiannis Karalis." Technological Educational Institute of Crete , Simulation secure internet Architectural using OPNET", 2009.

[19] Mohd Nazri Ismail and Abdullah Mohd Zin. "Development of Simulation Model in Heterogeneous Network Environment : Comparing the Accuracy of Simulation Model for Data Transfers Measurement over Wide Area Network". Asian Network for Scientific Information. Information Technology Journal, 2008.

[20] D. M. Divakaran, H. A. Murthy and T. A. Gonsalves, ``Detection of SYN Flooding Attacks Using Linear Prediction Analysis," 14th IEEE International Conference on Networks, Sep 2006.

[21] K. Jannu and R. Deekonda, “OPNET simulation of voice over MPLS with considering Traffic Engineering,” Blekinge Institue of Technology, 2010.

[22] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, May 2000.

[23] Mohd Nazri Ismail, Abdullah Mohd Zin, "Development of Simulation Model: An Ethernet Case Study in Heterogeneous Environment," IEEE, The 3rd International Symposium on Information Technology , 2008.

[24] Mohd Nazri Ismail, Abdullah Mohd Zin, "Comparing the Accuracy of End-to-End Network Performance Measurement Testbed and Simulation Model for Data Transfers in Heterogeneous Environment," ams, IEEE, Second Asia International Conference on Modelling & Simulation (AMS), 2008.

[25] Guiomar Corral, Agustin Zaballos , Cesc Canet ,University Of Ramon Llull, Spain, “Proposal of new challenge labs for the OPNET IT Guru Academic Edition”, 2013.