# **LITERATURE REVIEW**

**Literature review concerning networking in banking sector and its security coupled with firewalls.**

Table of Contents

[**LITERATURE REVIEW** 1](#_Toc62340210)

[**Literature review concerning networking in banking sector and its security coupled with firewalls** 1](#_Toc62340211)

[INTRODUCTION 1](#_Toc62340212)

[NETWORK 5](#_Toc62340213)

[TYPES OF NETWORK 5](#_Toc62340214)

[BANKING and NETWORKING 5](#_Toc62340215)

[BANK MANAGEMENT SYSTEM 7](#_Toc62340216)

[NETWORK ADVANTAGES 8](#_Toc62340217)

[NETWORK DISADVANTAGES 9](#_Toc62340218)

[SECURITY CONCEPT 9](#_Toc62340219)

[NETWORK SECURITY 12](#_Toc62340220)

[NETWORK FORENSICS 12](#_Toc62340221)

[TYPES OF NETWORK SECURITY 13](#_Toc62340222)

[THREATS TO NETWORK SECURITY 15](#_Toc62340223)

[DATA TRANSMISSION MODE 15](#_Toc62340224)

[DATA TRANSMISSION EQUIPMENTS 17](#_Toc62340225)

[FIREWALL 18](#_Toc62340226)

[TYPES OF FIREWALL 21](#_Toc62340227)

[COMPONENT OF A FIREWALL 21](#_Toc62340228)

[TECHNIQUIES USED IN FIREWALLS 22](#_Toc62340229)

[REFERENCES 22](#_Toc62340230)

# INTRODUCTION

This part talks about literature review in computer network security in banking system. When we talk about computer networking is made possible by linking different computers to each other, and there are information that is been carried out during the usage of this system which can be protected by firewalls, that’s why we say there is no fundamental difference between network and that of firewall, it is always suggested that there should be no network without a firewall.

Long time ago, brick walls were built between buildings in apartment complexes, so that if fire broke out it will not be possible for the fire to spread from one building to the other. In a natural term these walls are known as firewalls.

A computer is an electronic device that manipulate data, it has the ability to store retrieve and process data (GCFGlobal, 1998-2020). The devices that are connected may be

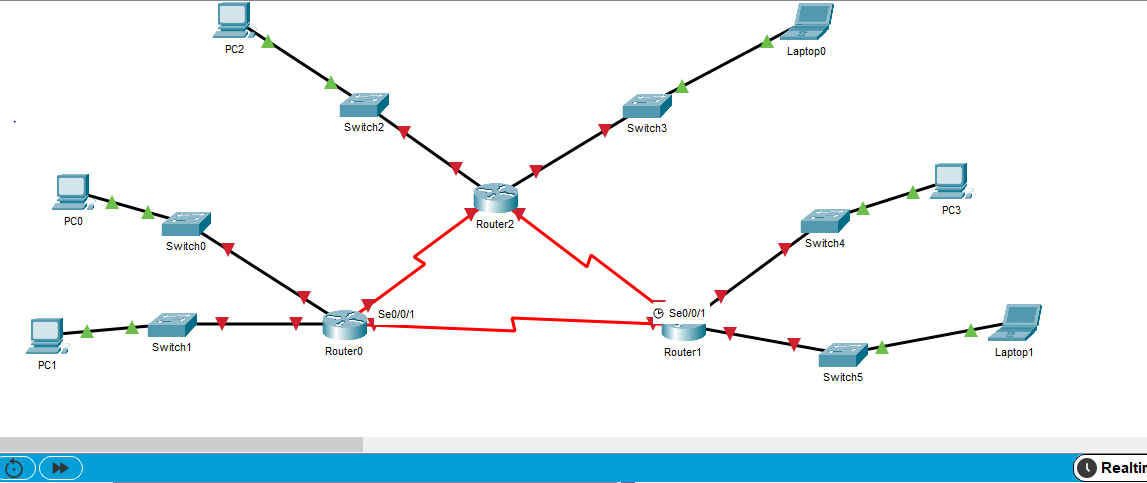
* Main Frame Computers: This is the central data repository, which are also called hub in a corporate data processed center, which are users link using less power devices, e.g. terminals or workstation. The presentation of mainframe often implies a centralized form of computing. Modern mainframe can run several operating systems at the same time using visual machine mainframe. Mainframe runs different operating system as if they are running on different computers. These visual machines capability is available on personal computers but run much more easily on powerful mainframe which can change system capabilities without harming any functionality. Mainframes are made to handle high volume of data. Examples of mainframe computer are IBM Zseries, System Z9 and system Z10 servers. (VIRENDRA18, n.d.)
* Input Terminals: When a device enter data into a computer is known as one-way handheld data terminal which are normally used for the collection of data. When input terminal is mentioned is also known as input-output terminal whereby the screen readout and the data provide feedback from the computer.

(britannica, 2021) define computer network as two or more computers connected together for the purpose of communicating data electronically, apart from the connection of devices, a network system is the backbone of every communication of a computer system which allows data and information’s to be transferred. Let us take for example, during this Covid-19 pandemic where workers are made to work from home, some workers can do this job at their convenient time with potable computers over phone lines. Workers can even do multiple jobs while still working.

Computer also act as a mailbox where members for instance of a company or specialist relates in there various office concerning any issues which they need to discuss and they can transmit their messages through the means of a computer. An equipment such as multiplexers, communication card acts as one of the means of communication within computers with high speed on a single share medium. Although there are other devices which can also communicate with computers.

(RECEPTION SYSTEM FOR AN INTERACTIVE COMPUTER NETWORK AND METHOD OF OPERATION, 1994) states that an interactive computer system network enables a user to display information, such as news, financial and cultural information, and perform desire transaction services such as banking and shopping through any plurality of types of personal computers. It is also stating that network is interconnection of computers communication lines, peripherals etc. further more the book also talk about transactional feature of interactive network which serves user time and money and frustration, by reducing the time spending travelling standing in line and communicating with sales personnel.

(COMPUTER NETWORK SECURITY MANAGEMENT SYSTEM, 2000) describe computer network as the network in which data link layer addresses, e.g. MAC address of the network card of a client node. It was further illustrated how nodes on the internet are identified by IP address. The actual purpose of using network is sharing of resources. Present inventions relate to computer networks which uses IP protocol, and which also include data linking layers of addresses such as network incorporating ethernet and WAN/LAN technologies, as well as token ring.



Topology Example of how network operates where an IP address is assigned for the LAN and WAN network which are linked together by nodes where they can be able to communicate with each other.

(BARONE, 2020) define bank as a financial institution licensed to receive deposit and make loans, bank do provide financial services such currency exchange, wealth management etc. they also exhibit the capacity of money creation. The connections of computer are link together in networking and are at risk to computer crimes. This is where firewall comes in, to protect the information of the network which act as intermediary between the network computers and the network itself,

(Internet Firewalls and Network Security, 1996) This book states that the major objectives of a firewall is to protect one network from another. Usually, the network that is been protected belongs to you or is your responsibility and the network you are protecting against is an external network that cannot be trusted and from which security intrusion can originate. Which means that your sensitive data are been protected from an unauthorized user and allowing bonafide users to have access to the network resources.

These firewalls act as a choke-point that monitors and rejects applications-level network traffic which also operate in the network and transport layers, such that they examine the IP and TCP headers of incoming and outgoing packets and reject or pass packet based on the programmed packet filter rules.

DATA LINK

NETWORK

SESSION

PRESENTATION

TRANSPORT

APPLICATION

FIREWALL

INTERNAL NETWORK

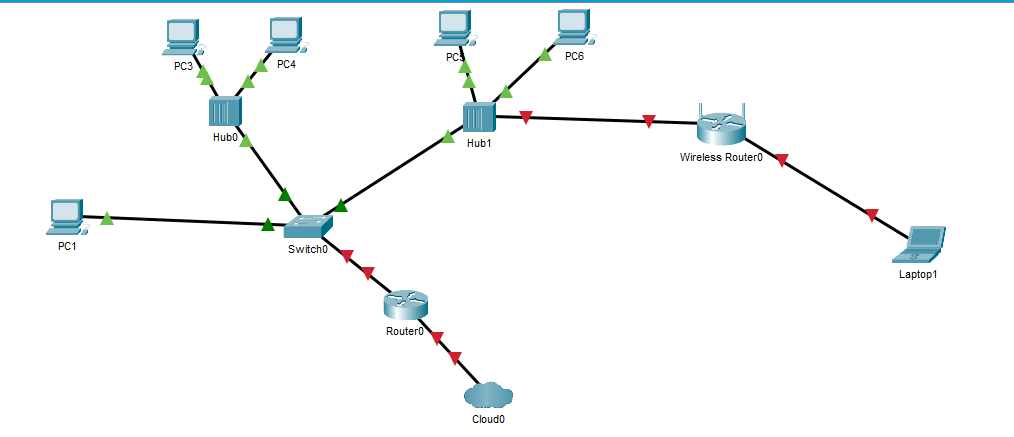
FIREWALL

OPERATION

In an organization like the banking system firewall is the backbone instrument which use to implement security work policy. In the enhancement of this policies, authenticity privacy and security techniques are well needed. In addition, firewall itself act as a resistant to infiltration

# NETWORK

In computer networking distant computer are link to each other or interconnected together through the means of a communication channel. In this case several computers can be connected to one computer and vice-versa. This connection is possible with the aid of internal cables or nodes which purpose is to help in the communication of a distant computer in a geographical region to aid in communication. Data are been shared and transmitted through this mode.



HOME NETWORK TOPOLOGY

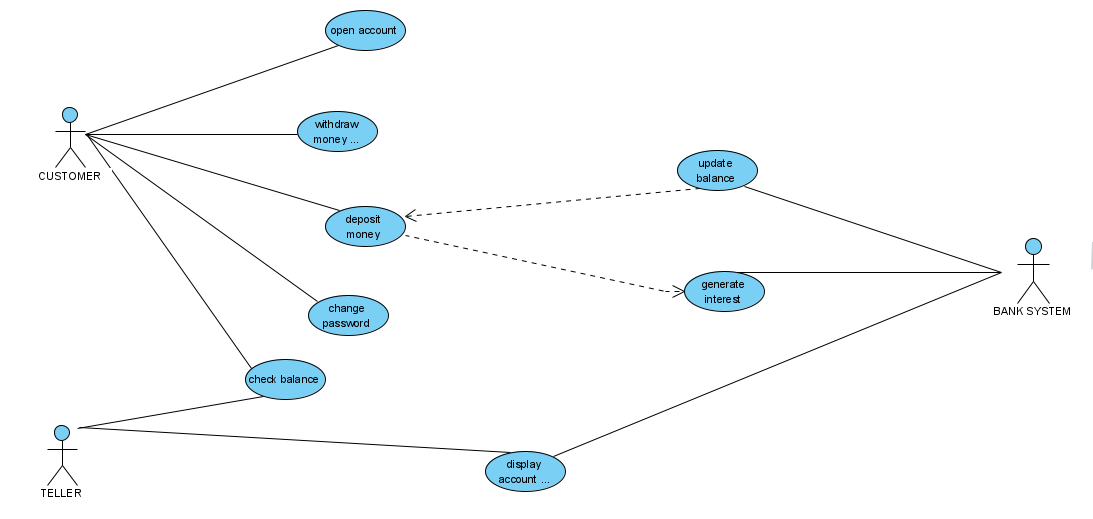
## TYPES OF NETWORK

* Wide Area Network (WAN): A wide geographical scale network are known as WAN. This connect computer to each other in a longer physical distance. WAN connects low voltage devices remotely which allow communication between them even though they are miles away from each other. WAN are normally use for large computer as a file server. Telecommunication link, satellite link or radio wave are part of link that WAN send data to using modern. Somethings, network configuration can be more censorious when the flow of data within the network are heavy. When the internet is mentioned the first thing that comes to mind is the WAN which connect all computers to each other around the world today.
* Metropolitan Area Network: This type of network can be owned and maintained by a single person or a company, is a type of network that act as a bridge between wide Area Network and the Local Area Network. As stated above microcomputers and other devices are connected within a metropolitan area.
* Local Area Network: This is one of the most discussed networks, most popular network and simplest network type. LAN is used to connect computers and low voltage devices to each other in a small distance, it is basically use in office buildings, it allows users to share information within their local area. LAN is connected to using routers to transfer data.
* Wireless Local Area Network WLAN: Its functionality are likely that of LAN, Wireless Local Area Network makes use of wireless network technology e.g. WI-FI, this can also be seen in LAN this network does not require physical cable for the connection of the network.

# BANKING and NETWORKING

Various equipment is satisfied by the broad range of network. Resources sharing and permission of information is one of the goals. In banking system information are run and are carried out effectively.

(BANKING: A Very Short Introduction, 2016) this book explains bank as an institution that accept deposits from savers, extend loans to borrowers and provide a range of financial services to its customers. Banks are central part of a financial system which place a major role in organizing of funds between the savers and the borrowers, including companies’ household and even the government. In recent decade, the use of advance technology has changed the way banks operates. And have also help banks to generate more funds. Electronic distribution channel is wildly using this day by customers in different part of the world, this include telephones, Automated Teller Machines (ATM), Mobile banking and internet banking which help customers in gaining access to the banking services. Innovations in payment have led to a shift from cheques and cash to more fast and electronic payment system. Such as credit card and debit cards, also contactless payment technology, the recent history of banking has witness relentless growth of large banking organization. Much of the growth of the largest banks has been fueled by the acquisition of competitors.



Used Case Diagram of a Banking System

#### Office automation system

Banks shoulders Office Automation System. This office automation system are information systems that store, create, display, modify and communicate in business correlations, it can be in writing, video and verbal form.

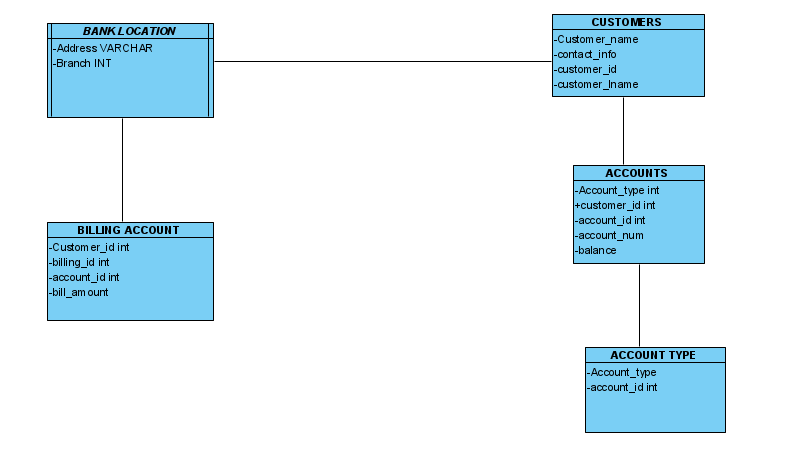
##### Examples of office automation system

* Meetings: This is one of the office automated system, meetings are very difficult to organize somethings, whereby you think about how to the meeting will be schedule and locating a perfect place for such meeting also ensuring the right people show up, finding time that work with everyone by sending group emails can be difficult that is why some tools e.g. doodle helps in this aspect regardless the time zone of each participants. Also the streamline of face to face meetings tools such as team allows member group to engage in a conference. This allow participant to exchange ideas and information, discussions, proposal on different issues.
* Electronic Mailing: This is another way of sending data and information electronically through a central computer or telephone network and several data network unlike the old time were letters are being sent. This has really help in speed quality at which data or messages is been transmitted. It also helps in the reduction of cost whereby the stamping of papers is been voided.
* Electronic Fund Transfer: This has to with the transfer of funds electronically from one bank account to another which comprises of multiple enterprises or single enterprises through a computer system whereby no staff of the bank has any intervention in such transaction. it can also be used to sort out salaries social and public payment etc.
* Facsimile Transmission: This is none as fax sometimes called telecopying or telefax. It is a system of communication that transmit a writing or printed document by scan and convert such information into signal wave which are transferred by wire to a fax receiver remotely.

## BANK MANAGEMENT SYSTEM

Banks uses this application by allowing customers to perform basic transactions from automatic machine from the bank through a computer, telephone smartphone through the internet. In this system customers can create their account also withdraw and deposit money for their account and still have the capacity to view report from the account. The viewing of customers account details is still visible in this platform which they can perform various transaction of their choice in accordance with their requirements. There are well secured connections that guild this transaction.

Bank uses database to create user accounts (schema) and create other account for department such as marketing and HR, it then provides an analyst to access the account of the department schema.



BANK DATABASE SCHEMA

## NETWORK ADVANTAGES

* Information and resource sharing: Terminals and microcomputer in the network are eligible to share files which act as an assistance in improving the processing of data and making of decisions.
* The sharing of single internet connection: when you secure the network properly there is a tendency that you spend less which helps in the protection of your system.
* Workload sharing flexibility: Several works can be done by each of the terminals present in the network. Workers can as well do multiple jobs during busy hours without leaving their sits.
* Increment of storage capacity: Multimedia and files can be accessed without storing them remotely on other machines e.g. music.

Sharing of peripheral equipment: a single online can be share be several micro-computers and this can occur in the Wild Area Network

## NETWORK DISADVANTAGES

* The transmission of data through a computer network the data can be corrupted due to invaders. These hackers can intrude into the network system by sending TROJANS which can corrupt the data.

CASE EXAMPLE

In August 2005, a Moroccan named Farid Essebar and a Turk named Attilla Ekici were arrested creating and distributing of Zotob, Rbot, and Mytob worms. It was believed that Essebar wrote the worm code and Ekici offered him financial assistants. The Mytob worm affected a wild range of windows systems, Zotob worm affected the system of some corporations such as New York Times, ABC News, CNN and so on. (Computer Forensics Investigating Network Intrusions & Cyber Crime, 2010)

* The procurement and securement of the communication gadgets are costly to maintain and run. For a network to function at optimal state it most be maintained and secure properly.
* Inaccessibility can occur in a file server that is when the file server breaks down.
* To maintain and manage a large network can be complicated, it requires a professional and you will then need to employ a network manager for such job.

## SECURITY CONCEPT

* DEMILITARIZED ZONE DMZ: This is a perimeter network that protects an organization internal Local Area Network from untrusted traffic (DMZ, 2021). This technology is use in the aspect of providing a third-party network access without the compromise of the security network. Between a private and public network DMZ act as a subnet. This DMZ brings out all external facing services from an untrusted network and it aid the addition of an extra layer of security by protecting the important data which are store in the internal network., e.g. the usage of firewalls in filtering traffics. Organizations like banks uses DMZ to access untrusted network.

##### HOW BANKS USES DMZ

Banks this day, now make their web server more accessible from the internet. By this the entire network of that bank is put at a risky position. No bank wants its network to be hacked so they pay an external firm to host their website on the firewall. In doing this it might affect their performance. So, what they do is that they allow the public server which is hosted on the network to be separated and secluded. This DMZ is secluded by a security gateway. E.g. firewalls which help in filtering the traffics as stated earlier between the Demilitarized Zone and the Local Area Network. There is also another security gateway that helps in filtering traffics which are estranging the DMZ from an external network.

If there is possibility for an intruder to pass through the external firewall which may compromise a part of the DMZ system, the intruder will then have the internal firewall to contend with before they can access any important data. Most banks used a well secured DMZ in which no matter how skilled the intruder is the DMZ tends to raise an alarm when the security is breached.

* VIRTUAL PRIVATE NETWORK (VPN): This protect your network when using public network. It encrypts the internet traffic and changes everything that has to do with your identity online. Which act as a security for any attacker to track or steal your data on the internet. This encryption usually occurs in real time. A VPN host runs a configured remote server which allows the network to redirect the hidden IP address by a VPN. This means that when you use the internet everything that you do the VPN server act as the source of your data and not even the internet service provider ISP can vie or access the data you receive or send through the internet.

One of the most amazing things above the VPN is that it turns all your data into balderdash if for instance your data is been accessed it will make no sense to the intruder.

* INTRUDER DETECTION SYSTEM IDS: this is a system that monitor and record a network for access violation and other malicious activities. This helps in keeping track and collection if malicious activities using an event management system and security information. Most intruder detection system do respond to detect some intrusion during discovery. Which are known as Intrusion Prevention System (IPS).

##### TYPES OF IDS DETECTION

* NETWORK INTRUSION DETECTION SYSTEM (NIDS): This is where incoming network traffic are been analyzed.
* HOST BASED INTRUSION DETECTION SYSTEM (HIDS): All important operating systems files are been monitored by this system.

##### HOW BANKS USES IDS IN NETWORKS

The monitoring of traffics to and from of all the devices in the network is done when IDS is placed at a strategic point of that network. IDS then analyze all passing traffic and matches them on a subnet to a library of known attack. The attack is then identified which might lead to abnormality behavior, alert it then sent to the administrator.

##### TECHNIQUES USE IN IDS IN NETWORKS.

There are different techniques that are use in IDS to track any cyber criminal who are trying to breach the security network of a bank. Such techniques are fragmentation, avoiding default, address spoofing and proxying, pattern change evasion etc.

Let us discuss few of the techniques listed above.

* Fragmentation: This system helps in detection of any attack signature, when fragment packet is sent it put the attacker under a radar and eventually the attacker will be detected.
* Pattern change evasion: this is system that IDS rely on for detecting attacks.

# NETWORK SECURITY

When a computer is protected from an authorized use is known as network security. Banks and other organizations have put in place different techniques in protecting their network against malicious attack which include destruction of hardware system and software systems of the computer. The invasion of unauthorize users can corrupt the database of the network and even lead to loss of data, that is why network security is very important and can be applied to prevent such an unauthorized usage.

Network security can be applied in different ways example of such is the information services and we also have electronic bulletin which is also considered as one of the interaction sections, customer services and electronic fund transfer. As far as network is concern, it is vulnerable to intrusion and attack from hackers that is why there must be security system that is put in place to protect the computer system and network.

# NETWORK FORENSICS

(Computer Forensics Investigating Network Intrusions & Cyber Crime, 2010) This book defines network forensics as the recording, capturing and analyzing of event in network in other to discover where an attack is coming from. Network traffic capturing over a network is a simple theory but relatively complex in practice, because there is a large amount of data that flow through the network that is why an investigator needs to backup the recorded data so as to free up the recording media and keep the data for future analysis.

In network forensics there are some information’s that can be revealed

* The traces and evidence, how intruder enters the network, the path of intrusion etc., but one thing should be put into consideration that network forensics cannot do the following examples such as linking of a suspect to an attack and trying to solve the case alone using network forensic.

#### DIFFERENT WAYS IN WHICH INTRUSSION ARE PROCESSED

* Attackers gather information about a network that helps them to intrude in that network which is know as Enumeration. For Enumeration to occur there are certain information that are needed

Topology of the network

Types of traffic and the network architecture

Number of live hosts.

#### SCANNERS

Most hackers are very versatile, and they use different scanner to attack and find vulnerability in the network. examples of scanner hackers use are, Virus, Trojans, Email Infection, Router Attacks and Password Cracking.

##### HOW BANKS COMBACT THESE SCANNERS

There are different ways which the banking system combat these scanners.

* They combat scanners from the attacked computers and intermediate computers which are placed as a form of files, logs, tools and ambient data.
* The use of firewalls: this is where the investigator checks the firewall and if the firewall itself is the victim, then the firewall will be treated like any other devices when obtaining evidence.
* Checking the internetworking devices
* Checking the victim computer.

## TYPES OF NETWORK SECURITY

* Files Protection: This system involves the creation program in protection of personal files from each other. They are sensitive also act as protection of files. Example of this is the Word-Perfect S.I which permits the closing a file using a password.
* Password: These are private and unique different numbers and characters which gives permission to users before accessing the computer. A list of an authorized password is stored which is been compared to against the character in the system. When a user enter the code or character and the code is correct then the user now have the permission to access the computer and there are limited time in which the user can implement the code if the code are not correct or the password are wrong.
* Security Server: printing facility and database storage are one of the outside systems and network computer which special computers like security severs helps in securing the connection between them.

(What Is Server Security - and Why Should You Care?, 1988-2019) states that security servers cover the processes and tools to protect the valuable data and held on an organization’s servers, as well as to protect the server resources.

* Encryption: encryption is the process of whereby data are been encrypted or encoded and messages are transmitted from one end of computer line to another. This process has various tools with well standard and good techniques that ensure messages are not readable when there is a transition of data between nodes in the network. In encryption there are two different keys that are used in coding information which are the public key and private key. This private key is encoded by the sender.
* Data Availability: if there if a prevention in accessing the information the availability of that information is affected or when you convert the information to a lesser form for example hard disk and floppy disk which are easily corrupted or damaged. In most case there are several ways where this computer hardware is damage either by flood or fire hazard also the memory of the system can be erased completely. In other to prevent such hazard, the backup of all data in different location should be put into consideration as the first thing to do. That is why banks today have recovery plan for the restoration of their lost data should anything hazard occur taking for example, a bank in Nigeria Zenith Bank Nigeria PLC located in Benin City the capital of Edo State where the entire building was gush by fire, this did not call for any worries cause the bank has put on all the necessary tools for the recovery of all the data and information of that bank (ogbebo, 2021)

## THREATS TO NETWORK SECURITY

As far as security in networking is concern there are different threat in information of a computer system, and there are different losses that occur in this process.

Accuracy integrity loss

Confidentiality loss

Business asset loss by fraud

## DATA TRANSMISSION MODE

There are three types of data transmission mode.

SIMPLEX TRANSMISSION MODE: The transmission of data is permitted in one direction in this mode, it is normally used in a special situation where there is flow of data in one way only. For instance, when a customer receives money in the bank which is transmitted through a computer the customer has no means of replying back during the same process because is known to be one-way thing.

SENDER

RECEIVER

Simplex Transmission Mode

HALF DUPLEX TRANSMISSION MODE: In this mode there is a tendency of communication in both sides but at different times. This mode is costlier than the simplex mode line. Duplex is mostly use when there is conversation over a computer or a telephone line.

siSSIM

RECEIVER

SENDER

The Half Duplex Transmission

FULL DUPLEX TRANSMISSION MODE: This mode channel has the ability in transmission of data simultaneously it is a bi-directional network data and information are transmitted at one time.

The full duplex transmission uses a pair of twisted cables for receiving packets and is the most active and very versatile in transmission.

RECEIVER

SENDER

FULL DUPLEX TRANSMISSION

##### DIFFERENCES BETWEEN THE FULL DUPLEX AND HALF DUPLEX TRANSMISSION MODE

* In half duplex mode the characters are immediately display on the monitor
* In full duplex mode the data does not display on the monitor until it is received and return
* Half duplex is a time saver.
* Full duplex does not save time because the alleviation collision and the transmission of frames.
* Bandwidth conservation are use in half duplex mode.

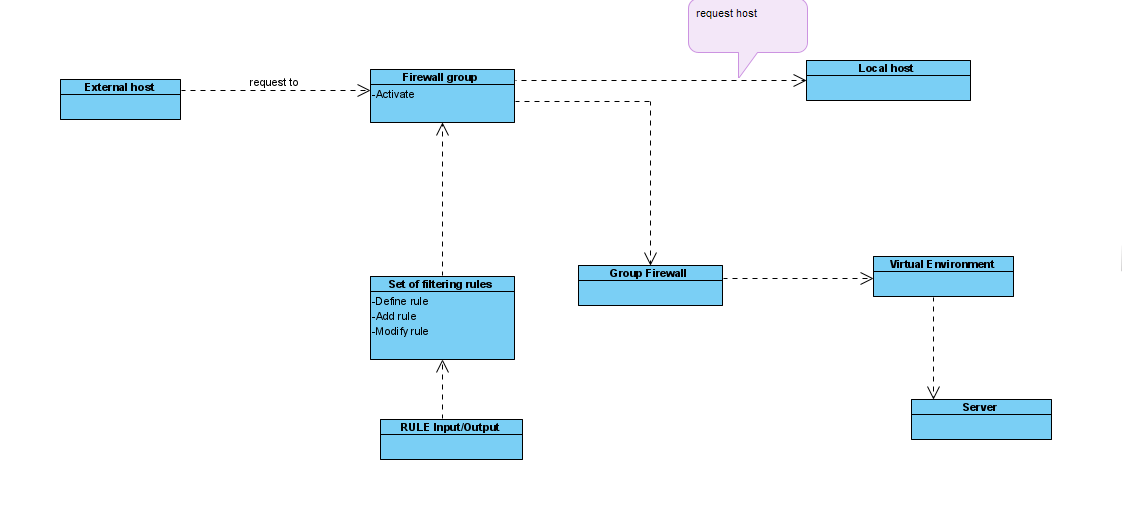
## DATA TRANSMISSION EQUIPMENTS

These are equipment’s facilities which are used in communication and the transmission of data over the network. Thus, the absent of such equipment can lead to failure in transmission and there will not be any possibility of operating on the network. Examples of such equipment’s.

* COMMUNICATION CARD: Some communication network that has multiple terminals are been controlled by this exceptional network interface devices. This device can receive, store and forward messages which is being assisted by its memory. It has the ability in providing temporary buffer storage and store data control program.
* ACOUSTIC COUPLERS AND MODEM: Back in the 1970s Acoustic Couplers was very popular then, it allows computers to connect using telephone handset. A transmission of 300 baud using a telephone handset was done by the first acoustic couplers. Acoustic couplers transmit information by converting the data into sound signal, and that signal is been sent through a telephone line then the receiving coupler will then interpret those signals. But in these recent days, modem is used instead, due to its speed and dependency to transmit data over the telephone lines. They are also easy to use. On a rare condition traveler still uses acoustic couplers if they do not have access to a network connection or modem. (Computer Hope, 2021)
* MULTIPLEXERS (MUX): This is the transmission of data from a multiple source over one line at a given time. Data are coded in a special way by this Multiplexers in order to sort out its destination. Multiplexers are sometimes called multiplexors which basically known for the selection of data, they are used in the selection of input lines and thereby sending them to the output, example of this device is the one-way rotary switch. A rotary switch are manual switches which can be used in the selection of signal lines or individual data by simply turning on or turning off its inputs.
* PBX DATA: This is known as the Private Branch Exchange. Companies or organization like Banks use this as a private telephone network within its organization. Banks uses this phone system in communicating within the bank internally and for external purpose.

# FIREWALL

This are system software and hardware that connect both the intranet to the external network which help the internet block all unauthorized access to the network. The major objectives of this firewalls are that it helps in the protection of one network to the other. It acts as a bridge between the internal network and the external network. It safeguarded all information that comes in from an external source to the internal source from computer virus and other malicious activities. Most organization like bank rely on this for the protection of their network. And they use several approach in building their firewalls such as the ‘ROLL YOUR OWN’ approach which involves the customization of firewall solutions in protecting their banks. It is also regarded as one of the most effective approach when is implemented.



CLASS DIAGRAM OF A FIREWALL

There are some gateway products that are available in the internet security corporation e.g. Firewall-1 Gateway. Before we explain what firewall-1 gateway is and does let us define the difference between gateway and firewall.

Gateway: this is a network node or networking hardware that helps in connection of two separate network to communicate with one another. While firewall is a system software and hardware application that sets rules to decide which data packets can have access in entering the networking system.

(Internet Firewalls and Network Security, 1996) this book explains firewall-1 gateway as a commercial gateway product, available from the internet corporation, which currently running on SUN SPARCstations.

There are various methods in which this product establishes its network security. Such methods are packet filtering and Application gateway.

Firewall-1 gateway configuration is done using a graphical interface like Open Look for SunOS operating systems.

FEATURES OF FIREWALL-1 GATEWAY

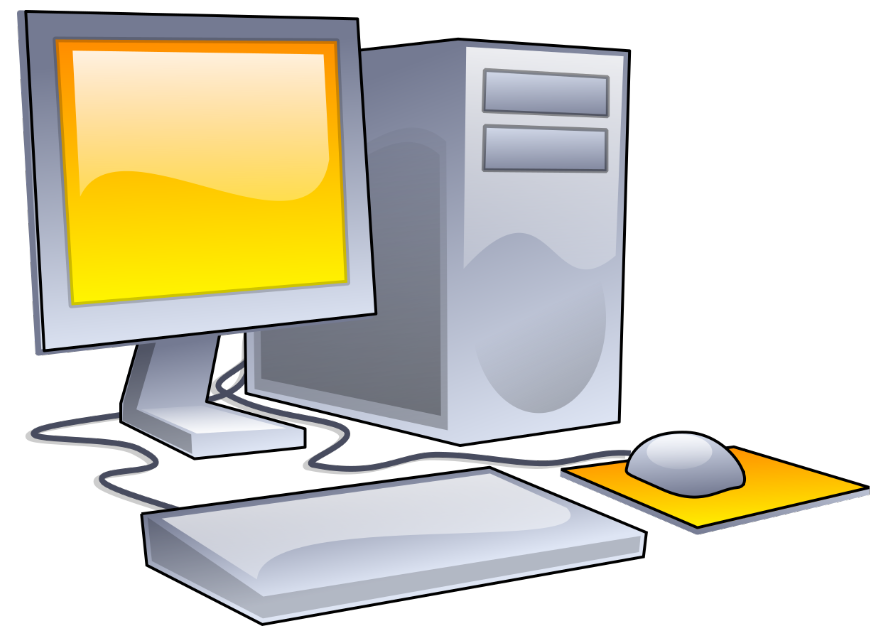
* Adding information to stateless connections.
* Secure packet filtering.
* Alerting and audition
* FTP sessions and authentication telnet.
* The creation of encrypted channels.

The basic uniqueness of this product is that it uses packet filtering as its basic mechanism, which is carried out in layer 7 and 2 of the Open System Interconnection Model.

Firewall-1 can run on different platform or operating system such as

* Hardware platform
* Operating system e.g. Network server platform.
* Graphical interfaces
* Network interfaces.

The firewall-1 gateway is a well secured router that act as a security router between an internal and external network of an organization. E.g. banks, any unauthorized network are sent through this firewall which can be verified by the internal security to see if it complies with its policies.



Firewall-1

External untrusted network Internal Trusted Network

DIAGRAM OF FIREWALL-I GATEWAY SECURITY

## TYPES OF FIREWALL

#### Cloud firewall.

#### Packet filtering firewall.

* Hardware firewall: these are firewalls that uses physical appliances which act in a similar manner to traffic routers in intercepting packet data and traffic request before connecting them to the network servers. This helps unauthorized traffic from outside the network to be intercepted before the network endpoint of the organization are uncovered. Although as this may concern it also has a weakness because is often easy for an attacker to detour this firewall.
* Circuit level firewall: these are firewall that can close any connection by the usage of configured rules, which means that both ends of the connection can be verified properly.
* Stateful inspection firewall.
* Application gateway firewall also known as proxy firewall.

## COMPONENT OF A FIREWALL

* Internet protocol packet filtering.
* Network address translation (NAT) service.
* SOCK server.
* Proxy server.
* Mail relay service.
* Logging etc.

## TECHNIQUIES USED IN FIREWALLS

* Service protocol: the accessing of inbound or outbound network can be determined by this process.
* Direction control: this dictate the direction on how a service request can flow and initiated through a firewall.
* Behavioral control: it determines how a network service is used.
* User control.

# REFERENCES

(BANKING: A Very Short Introduction, 2016)

(BARONE, 2020)

(COMPUTER NETWORK SECURITY MANAGEMENT SYSTEM, 2000)

(Computer Forensics Investigating Network Intrusions & Cyber Crime, 2010)

(Computer Hope, 2021)

(DMZ, 2021)

(GCFGlobal, 1998-2020)

(Internet Firewalls and Network Security, 1996)

(RECEPTION SYSTEM FOR AN INTERACTIVE COMPUTER NETWORK AND METHOD OF OPERATION, 1994)

(VIRENDRA18, n.d.)

(What Is Server Security - and Why Should You Care?, 1988-2019)

(britannica, 2021)

(ogbebo, 2021)

Goddard, J. and Wilson, J.O., 2016. *Banking: A very short introduction*. Oxford University Press.

EC-Council, 2009. *Computer Forensics: Investigating Network Intrusions and Cyber Crime*. Nelson Education.

Hare, C. and Siyan, K., 1996. Master the Complexities of Network Security: Internet Firewalls and Network Security 2nd Edition.

Orchier, J., Soriano, R., Salvaterra, L., Ardito, D. and Byreddy, A., JPMorgan Chase Bank NA, 2000. *Computer network security management system*. U.S. Patent 6,070,244.

Filepp, R., Gordon, M.L., Bidwell, A.W., Young, F.C., Wolf, A.M., Meo, S., Tiemann, D., Cohen, R.D., Bellar, M., Appleman, K.H. and Abrahams, L., 1994. *Reception system for an interactive computer network and method of operation*. U.S. Patent 5,347,632.