UNIVERSITY OF ZIMBABWE

FACULTY OF ENGINEERING

DEPARTMENT OF ELECTRICAL ENGINEERING

PROJECT TITLE: NETWORK FIREWALL TECHNOLOGIES

AUTHOR: **MANGENA HILLARY, R113658Y**

SUPERVISOR: **MR SAMUEL CHARI**

THIS PROJECT IS SUBMITTED IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE BSc Hons DEGREE IN ELECTRICAL ENGINEERING

JUNE 2014

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Mr. Samuel Chari, for his honest and valid advice. I also wish to extend my gratitude to the UZ Department of Electrical Engineering for giving me all the necessary support during the compilation of this document. Lastly, special thanks to my family, without their motivation and support, this project would not have been such a resounding success.

ABSTRACT

This project is mainly concerned with the functionality of network firewalls and data filtering at a transport level. When one wishes to set up a network (LAN, WAN, etc), such knowledge is relevant because the process of selecting a suitable security system (firewall) can be extremely difficult. In this document, firewall functionality, the 3 main technical standards currently in use, and their relative advantages and disadvantages are explained. The first section gives a concise illustration of how the ISO 7-layer OSI model operates and this knowledge is later used to explain firewall performance. The last chapter then describes in vivid detail, the filtering schemes currently in use. Collectively, this document can serve as a stepping stone for future research in a bid to better the systems that currently exist. Analysis and the inferences are presented in the conclusion, and the document is complete.

TABLE OF CONTENTS

TABLE OF CONTENTS continued

CHAPTER 1: RESEARCH OVERVIEW

1.1 INTRODUCTION

In the early 1980s, the internet was relatively new and its users valued openness since this made the sharing and collaboration of information a lot easier. However, as the years went by, the internet expanded and its use became much more diverse.

In 1988, one of the first ever malware was developed, and was named the Morris Worm, after the person who created it, Robert. T. Morris. The Morris Worm was initially designed to measure the size of the internet but, because of flaws in its design, it ended up being a dangerous development that had the ability to slow down a PC's response to the point that an infected computer would become unusable. The estimated cost of the damage inflicted by this worm was put at USD10M by the United States Accountability office. Although the Morris Worm was without a doubt the most dangerous malware present at that time, there were many other reported cases of attempted or successful network intrusions. In light of all these, it became clear that there was need to invest in network security technology.

Many network security systems have been developed over the years and listed below are some of those that are regarded as the most successful;

(i) *IDS (Intrusion Detection System)* – operate by making it difficult for an intruder to utilize or temper with network resources once access has been gained.

(ii) *NAT (Network Address Translation)* – these make it difficult for an outsider to map the network.

(iii) *Virus Scanner* – they search for malware or any potentially dangerous software within the network.

(iv) *Network Firewalls* – control the incoming and outgoing of traffic to and from the network.

Defense in depth, which refers to the use of many security mechanisms simultaneously, is the most effective way of protecting a network but, this can be expensive. The search of a perfect systems security solution is still on but for now, firewalls are the cornerstone of most security systems.

1.2 JUSTIFICATION

Everyday hackers remind us of the need to secure our networks. The list below contains some of the most damaging incidences that resulted from security breaches.

(i) In April 2014, Google made public that they had identified a bug that exploits an error in the cryptographic software library used by internet services to keep data transmissions private. This bug, known as 'Heartbleed,' could have had catastrophic financial ramifications particularly on internet bankers had it been expertly exploited and is thought to have been in existence since early 2012.

Heartbleed bug symbol

(ii) Edward Joseph Snowden is an American citizen who in 2013, was charged with espionage. He was accused of having disclosed classified information which he acquired while working as a contractor at the US NSA, information which he would not have acquired had there been effective security measures in place.

(iii) Julian Assange through his Wikileaks website has managed to publish information which many, including the government of Zimbabwe, can argue isn't supposed to be public knowledge. The documents that make up this website what it is today were not legitimately acquired, and the hacking could have been prevented if more money had been spent on network security improvements.

(iv) In 2013, it was alleged that the US NSA had bugged the German Chancellor, Angella Merkel's phone and they were able to listen to her private phone calls. This development strained the relationship between Europe's largest economy and the world's largest economy at the time it happened, and with better security, this could have been avoided.

The incidences just described prove that the existing security systems do not meet the minimum requirements and there is need to invest more in this sector. As is the case in item (iv), poor network security can have devastating effects on world stability and further research needs to be done to improve the current systems. However, such improvements can only be done if all existing knowledge on network firewalls has been mastered.

1.3 AIM

The main aim of this project is to gather in-depth knowledge on Network Firewall Technologies by relating the OSI reference model to the firewall technical standards currently in use.

1.4 OBJECTIVES

1. To acquire in depth knowledge of the 7-layer OSI reference model.
2. To explain data filtering and how it is used as a security measure.
3. To gather detailed knowledge on the existing firewall technical standards.
4. To compare the firewall standards and present their relative advantages and disadvantages.

1.5 METHODOLOGY

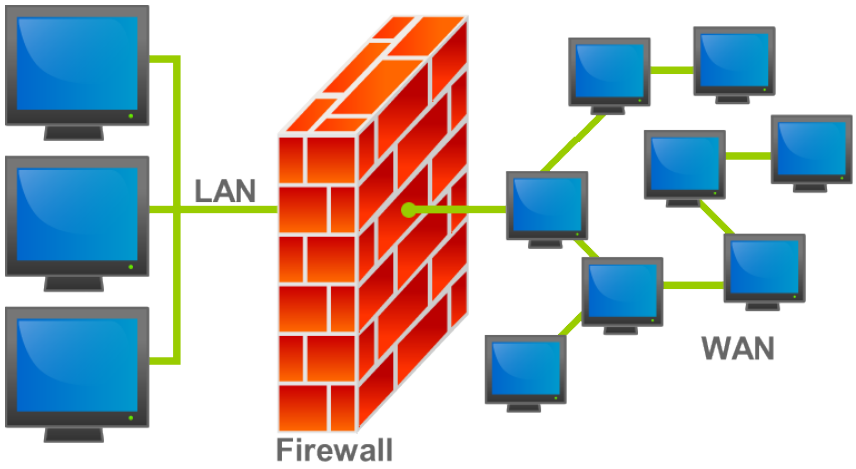
- Research on the internet
- Research using the UZ library resources
- Consultation

CHAPTER TWO: FIREWALL OVERVIEW AND THE OSI MODEL

2.1 WHAT IS A FIREWALL?

A firewall is software or a hardware based security system that controls the incoming and outgoing of information (network traffic) into and out of a network, or an individual computer, according to a specified set of rules.

Essentially, firewalls protect networks from the internet. However, they can also protect smaller networks from others of different trust levels, or sensitive parts of a particular network from being accessed by unauthorized personnel e.g. the information in the accounting department of a firm must be inaccessible to the rest of the company's network. Below is an illustration showing the typical location of a firewall separating two networks, in this case a LAN from a WAN;



[1] Fig 2.1

It is important to note that there is no other way to traverse from one network to the other, except through the firewall.

Firewalls can be divided into two basic types, hardware and software firewalls, and each is explained in turn on the following page.

1From en.m.wikipedia.org/wiki/Firewall_(computing)

2.2 HARDWARE FIREWALLS

This is the type of firewall that is placed at the network edge. By virtue of this location, it is able to shield an entire network (all the PCs in that network) from the internet or other external networks of different trust levels.

Hardware firewalls are mostly employed by small businesses even though they also find use in home networks where, the broadband router will usually act as the hardware firewall. Examples of hardware based network firewalls include;

1. Check Point firewall-1
2. The CISCO PIX and ASA

2.3 SOFTWARE FIREWALLS

Software firewalls are user driven. Each firewall is installed into every single system in a given network. Typically, a software based firewall is just software application usually built into an operating system. A typical example of software based firewall is the Windows 7 firewall.

An advantage that hardware firewalls have over software firewalls is that, in the event that any of the PCs in the network is attacked by a virus, the firewall will not be affected.

NB: To provide maximum security to a given network, both hardware and software based firewalls should be used together. This is because the two complement each other. For instance, since we're now living in BYOD world, a person might bring an infected PC into a network and the hardware firewall won't protect the other PCs in that network from being infected but, the software based firewall will.

2.4 THE OSI 7 LAYER REFERENCE MODEL

This section deals with the functionality of the OSI model and this knowledge will be imperative in describing firewall technical standards later on.

Definition*;*

OSI stands for Open Systems Interconnect, and the OSI reference model is a scientific abstraction designed to explain the complicated processes that take place during network communications, in a clear and understandable way. It was developed by the International Standardization Organization, ISO, in 1984.

Definitions of commonly used terms

-protocol: a predefined way of how a user's PC can communicate with a desired service

-datagram: a term that describes the form taken by data when it is being transferred within a network

-ruleset: this is a set of rules that describes the criteria used by a firewall to either allow or deny traffic

-firewall policy: these are the firewall settings, including the ruleset, that determine the overall behavior of a firewall

Figure 2.2 below shows the arrangement of the 7 layers that constitute the 7 layer OSI reference model;

APPLICATION LAYER
PRESENTATION LAYER
SESSION LAYER
TRANSPORT LAYER
NETWORK LAYER
DATA LINK LAYER
PHSYSICAL LAYER

Fig. 2.2

These layers are numbered from the bottom going up with the physical layer being layer 1.

Functions of each of the layers

Layer 7: Application Layer

This where network specific applications such as mail and file transfer are found. Applications such as MS Word or Outlook connect at this layer if there is need for network connection.

Layer 6: The Presentation Layer

This layer gives a context for, or it enables communication between the layers of the model. It prepares data from the lower layers for presentation to the upper layers. Decryption and encryption of data is done here.

Layer 5: Session

The session layer controls dialogue/handshaking between different computers. This is also where processes such as duplexing, restarts and terminations are controlled.

Layer 4: The Transport Layer

It provides a platform for the transparent transfer of data. Protocols such as TCP (for reliable connections) and UDP (for non-reliable connections) operate in the transport layer. This layer also provides the following,

(i) End to end connections
(ii) Reliability
(iii) Flow control

Layer 3: Network Layer

The routing of data packets takes place in the network layer. It also provides connections between hosts on different networks. Some of the protocols that operate here are IPv4 and IPv6.

Layer 2: Data Link

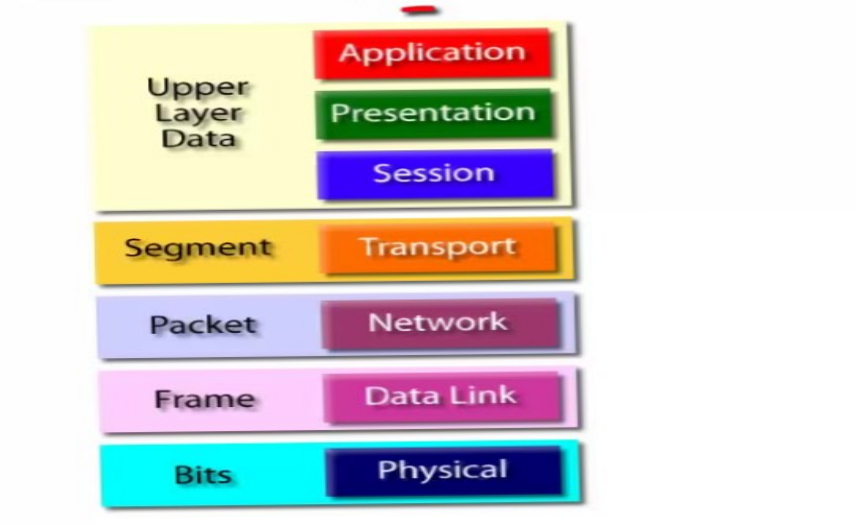
It facilitates connections between hosts on different networks. Protocols that operate at the data link layer include Ethernet and MAC (Media Access Control) addresses/Hardware addresses.

Layer 1: The Physical Layer

It describes the electrical and physical specifications of devices e.g. cables, connectors, hubs, repeaters etc. In the event of a fault in a network, troubleshooting begins at the Physical layer.

Datagrams

The datagrams that operate at each of the layers are shown on the left hand side in the figure below;



[2] Fig 2.3

The table shown in fig. 2.4 is a summary of the protocols that operate at each of the 7 layers of the OSI model. The MPLS protocol operates in between layers 2 and 3, and hence it appears on both layers.

2Extracted from a YouTube tutorial based on chapter 2 of the book, The Accidental Administrator: Cisco Router Step-by-Step Configuration Guide by Don R. Crowley/www.soundtraing.net

	Layer	Name	Protocols
Software	Layer 7	Application	Telnet, SMTP, HTTP, FTP, IMAP, POP3, SNMP
	Layer 6	Presentation	MPEG, ASCII, TLS, SSL
	Layer 5	Session	NetBIOS, SAP
	Layer 4	Transport	TCP, UDP
	Layer 3	Network	IPv4, IPv6, ICMP, IPSec, ARP, MPLS
Hardware	Layer 2	Data Link	MPLS, RARP, Ethernet, 802.11x, PPP, Frame Relay, ATM, FDDI, Fibre Channel
	Layer 1	Physical	RS232, DSL, 10BaseT, 100BaseTX, ISDN, T1

[3]Fig. 2.4

2.5 EXPLAINING INTER-NETWORK COMMUNICATION USING THE OSI MODEL

This explanation is best given by use of an example as done below:

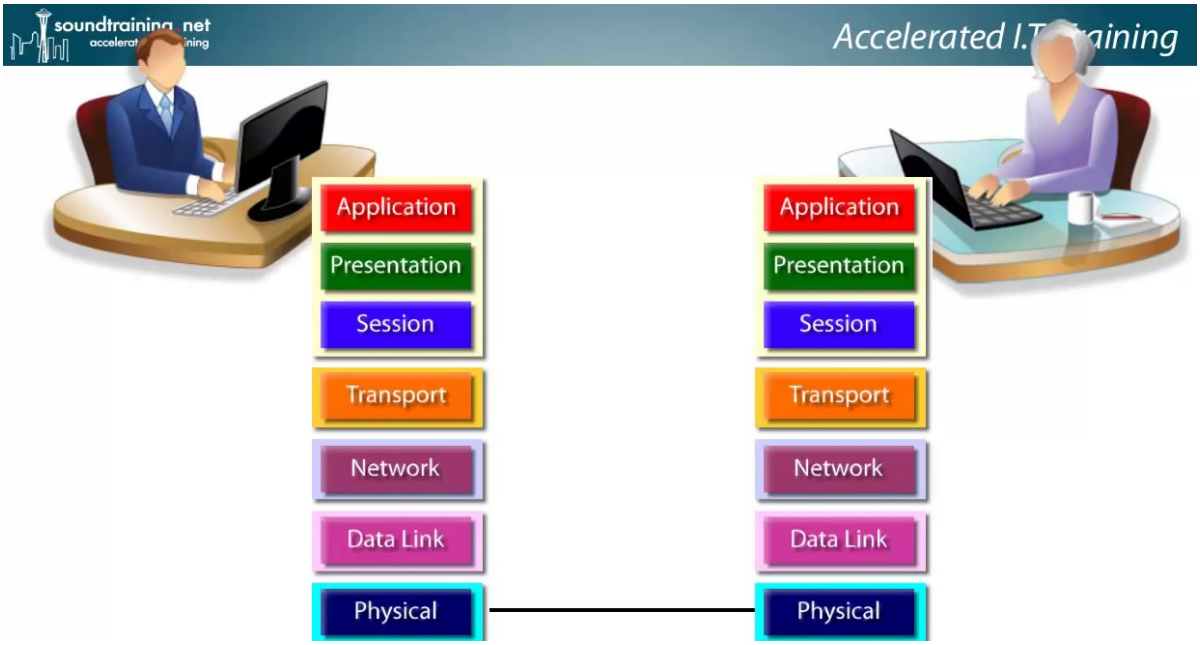
Referring to figure 2.5, assume that the man on the left wants to send a data file to the woman on the right.

For the man's objective to be achieved, once he clicks 'send' on his computer, the file he wishes to transfer to the woman is converted into upper layer data as it moves from his computer to the application layer. It remains in this form as it moves down the top three layers sequentially. This upper layer data is then encapsulated into segments when it reaches the transport layer, i.e. Segment headers are attached to the upper layer data at layer 4. At layer 3, each segment is encapsulated into a packet, which is then encapsulated into a frame at the data link layer. Finally,

3 Extracted from a YouTube tutorial based on chapter 2 of the book, The Accidental Administrator: Cisco Router Step-by-Step Configuration Guide by Don R. Crowley/www.soundtraing.net

the frames are converted into bits at the physical layer, and these bits are the ones that are sent to the physical layer on the other network.

When the information, which will now be in the form of bits, reaches the other network, it ascends the stack. As this happens, headers and encapsulations are removed at the appropriate layers until only the desired data file is delivered to the woman. To summarise, the processes that the data packets go through while descending the OSI stack are reversed or undone when those packets ascend the stack.



[4]Fig 2.5

As seen in the figure above, the only time when there is a physical connection between the 2 networks is on the physical layer.

CHAPTER THREE: FIREWALL TECHNICAL STANDARDS

4 Extracted from a YouTube tutorial on Cisco Router Training 101 which is based on chapter 2 of the book, The Accidental Administrator: Cisco Router Step-by-Step Configuration Guide by Don R. Crowley/www.soundtraing.net

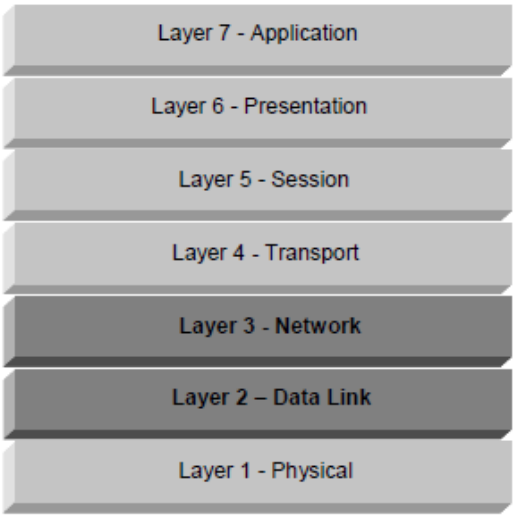
3.1 INTRODUCTION

Since its inception, firewall technology has improved substantially over the years. From simple packet filtering firewalls, today firewalls have the ability inspect data packets at higher layers of the OSI model. This chapter explains in detail, the three main firewall standards:

1. Packet filters
2. Application layer gateways
3. Stateful inspection

3.2 PACKET FILTERS

Packet Filters are the most basic type of firewall. They screen all traffic at the network and data link layers of the OSI model, and do not operate at any other layer of the OSI model,



[5]Fig. 3.1 Data inspection is only done as far as the network layer

Packet filters operate by observing the source and destination IP addresses and protocol numbers. In the cases of TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) the port numbers are observed instead. Some texts refer to Packet filters as being essentially routing devices and this is because they are sometimes built into routers or UNIX

5 Extracted from, Guidelines on Firewalls and Firewall Policy (pdf online) by John Wack, Ken Cutler and Jamie Pole, special publication 800-41, page 6, fig 2.

kernels. The rule set configured into the firewall determines the traffic which is rejected and the traffic which is allowed through. Below is a partial sample of a simple packet filter rule set:

Source address	Source Port	Destination Address	Destination Port	Action	Description
Any	Any	223.114.1.0	> 1023	Deny	Rule to prevent return TCP connections to internal subnetwork.
223.114.1.1	Any	Any	Any	Deny	Prevent firewall from connecting to anything.
Any	Any	223.114.1.1	Any	Allow	Allow external users from directly accessing the firewall system.
223.114.1.0	Any	Any	Any	Allow	Internal users have access to external servers.
Any	Any	223.114.1.2	SMTP	Deny	External users can to send email in.

[6]Fig 3.2

Note that this sample is far too simplistic and rule sets for practical firewalls are much more detailed. In reference to fig. 3.2, the firewall is protecting a network whose address range is 223.114.1.0 ≤ address ≤ 223.114.1.254. Firstly, the packet filter will accept any incoming data packet. It then examines its source and destination addresses as well as its ports. This enables the firewall to determine the protocol in use. Lastly the firewall will work through the rules from top to bottom and will take one of the following actions as appropriate,

(i) Discard: the packet is dropped and no error message is returned to the source. In this action the outsider is not made aware of the firewall's presence, and this is known as the black hole methodology.

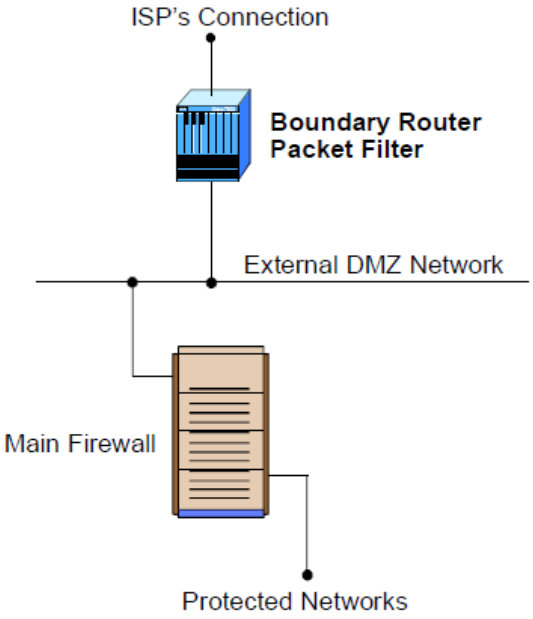
6Extracted from, Guidelines on Firewalls and Firewall Policy (pdf online) by John Wack, Ken Cutler and Jamie Pole, special publication 800-41.

(ii) Deny: the data packet is not allowed to pass through the firewall but an error message is returned to the source.

(iii) Accept: The packet is allowed to pass through the packet filter.

Packet Filter as a Boundary Router

A boundary router is a router that connects an intranet to an external untrusted network, usually the internet. It incorporates a packet filter which is placed at the internet service provider's, ISP's, side and is linked to the main firewall and via a demilitarized zone, DMZ.



[7]Fig 3.3 Packet filter functioning as a boundary router

Packet filters are suitable for this functionality because they are capable of accommodating many different protocols since they do not screen data at higher layers. They are generally flexible and can act as the first line of defense.

Advantages and disadvantages of packet filters

The advantages and disadvantages of all firewalls are largely determined by the layers on the OSI 7 layer model on which the firewalls examine the incoming or outgoing data packets.

7 Extracted from, Guidelines on Firewalls and Firewall Policy (pdf online) by John Wack, Ken Cutler and Jamie Pole, special publication 800-41, page 7, fig 2.4

Generally, the more the layers on which packet examination is done, the more reliable the firewall is.

Advantages

(i) Relatively cheap: Routers being developed today can perform packet filtering and this eliminates any additional costs incurred when buying the firewall.
(ii) Speed: Because they do not screen data above the network layer, packet filters are fast as compared to other technologies.
(iii) Range: They have a wider range and can be used in most networks. This is because most protocols are covered in layers 2 and 3 of the OSI model.
(iv) Packet filters require less processing memory and processing power compared to other firewall technologies.
(v) Because of their flexibility, they can be used in boundary routers as explain earlier.

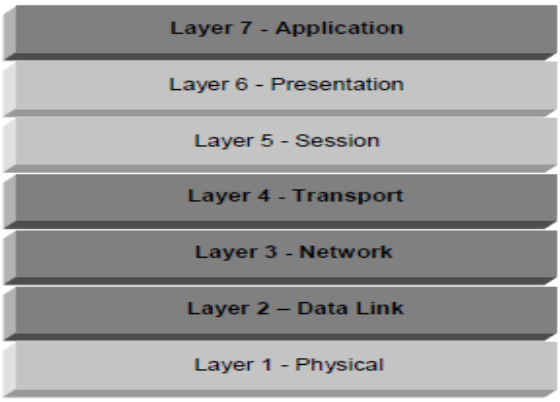
Disadvantages

(i) Packet filters cannot verify or authenticate services/users and as a result unauthorized people can gain access to restricted services or areas of a network.
(ii) They do not provide content security e.g. scanning for viruses.
(iii) Packet Filters cannot automatically open and close specific ports as and when required. Unwanted or harmful software can therefore enter a network through the ports when they are open but not in use.
(iv) They do not provide protection against malware intrusions that exploit application specific limitations. This means that, for instance, if an application is accepted by a firewall, all of its accompanying files and functions are also accepted. And if any of these are malicious, the network the network can easily be compromised.
(v) Also, packet filters are difficult to maintain and, although this is subject to debate, what isn't in doubt is that experts can have difficulties when configuring a fairly complex set of rules.

As a conclusion, it can be said that packet filtering is not very reliable. However, Packet Filters are better suited for systems were speed is of paramount importance and user authentication is less significant.

3.3 APPLICATION-PROXIES (APPLICATION LAYER GATEWAYS)

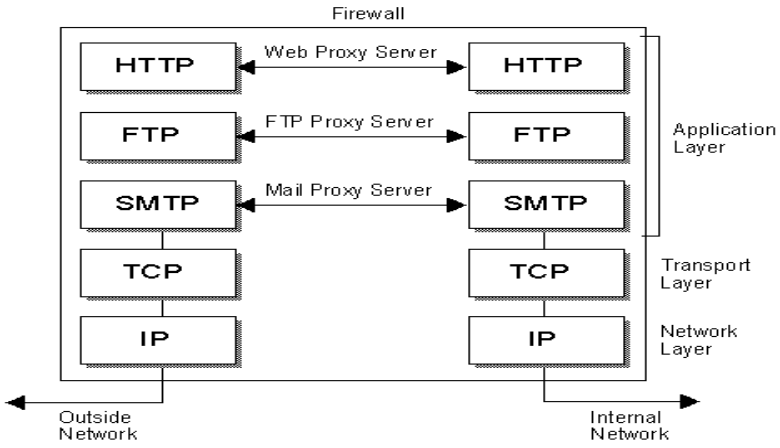
Sometimes referred to as Application Layer Gateways because they operate at the Application Layer, Application Proxies examine data at both lower and higher level layers of the OSI model. As their name suggests, they act as intermediaries between users and servers. User connections are terminated at the proxy and a whole new connection from the proxy to destination host is initiated. Because connections are screened across more layers, application proxies provide significantly greater security compared to packet filters, although this feature also has its downside.



[8] Fig. 3.4

Layers on which data packet inspection is done in Application Proxies are shown in the darker grey shed.

8 Extracted from, Guidelines on Firewalls and Firewall Policy (pdf online) by John Wack, Ken Cutler and Jamie Pole, special publication 800-41, page 13, fig 2.6



[9]Fig. 3.5 illustrates some of the protocols handled by application proxies

As can be seen in fig. 3.5, the Simple Mail Transfer Protocol for emailing, and the HTTP for web services, are inspected at the application layer. TCP data packets are inspected at the transport layer and those for IP, at the Network Layer. A firewall proxy operates by converting a two-party session essentially into a four-party session. This means that, for example, if an internal user wishes to access a website on the internet, the packets encapsulated in the request are first inspected at the HTTP server before being forwarded to the website. Also, the packets returned by the website will be checked at the HTTP server and then sent to the user host machine. There is no direct communication between user host and website. This implies that a process that was supposed to comprise of 2 virtual connections i.e. user host to website, now comprises of 4 connections i.e. user host to HTTP server and then HTTP server to website.

Because of their ability to examine connections across most the layers, and also because they turn two-party session into four-party, they have the following advantages and disadvantages;

Advantages

(i) They provide content security e.g. screening of malware based on specific sites and accessed web pages.

(ii) Improved security because they allow for user authentication which can be in any one of the following forms,

a) Asking for user ID and password

9 Extracted from www.akadia.com/services/firewall_proxy_server.html

b) Requiring source address
c) Biometric verification

(iii) They ensure that only the service that will have been required is accessed or utilized.

(iv) Caching is possible, (temporary storage of data).

Disadvantages

(i) Due to maximum examination of data, more memory and processing power is necessary and this is expensive.

(ii) They are slow since data packets are examined at lower and higher level layers and this takes a considerable amount of time. This makes them unsuitable for real time applications.

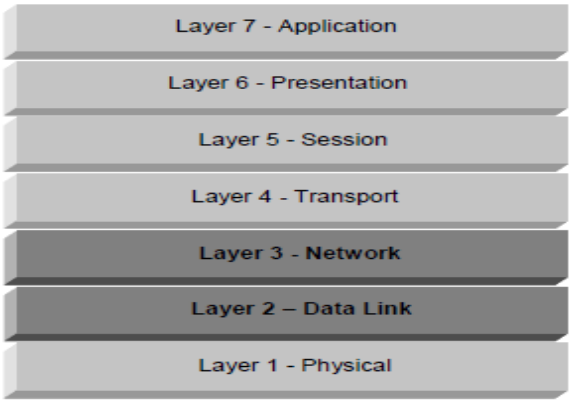
(iii) In large environments i.e. where many different applications are integrated into a single system, application proxies cannot be used because many new technologies cannot be proxied. In other words, as new application protocols come into place, there is need to develop new corresponding proxies that can handle them.

Examples of application layer gateway firewalls are,

1. Enterprise Firewall/Symantec Raptor
2. Gauntlet, from secure computing

3.4 STATEFUL INSPECTION FIREWALLS

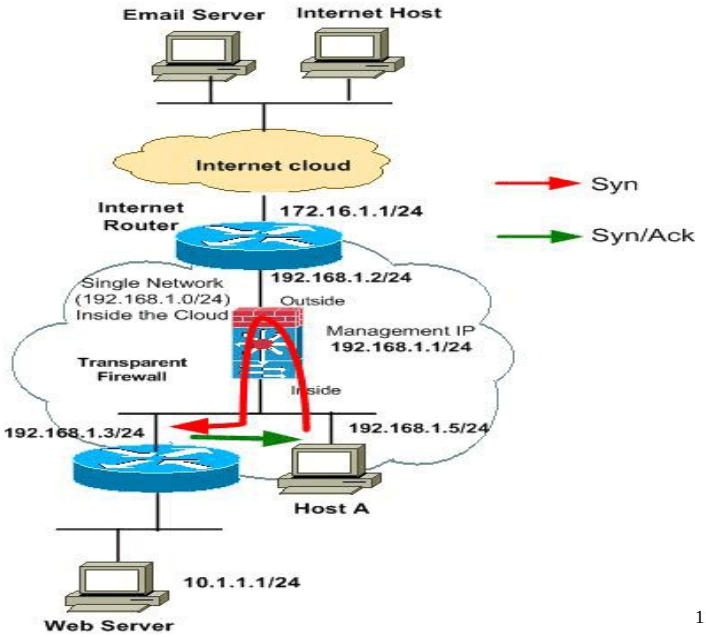
In Stateful Inspection, data is examined at the network and transport layers as shown in the darker grey shed in fig 3.6.



[10]Fig 3.6

This firewall technology was developed with the idea of bettering security provided by packet filters while retaining the speed feature of packet filtering. It allows for specific ports to be opened such that traffic can pass through if the configured requirements are met. The name Stateful Inspection is derived from the firewall's ability to keep a record of network connection states in a state table.

OPERATION OF STATEFUL INSPECTION FIREWALLS



[11] Fig 3.7

10 Extracted from, Guidelines on Firewalls and Firewall Policy (pdf online) by John Wack, Ken Cutler and Jamie Pole, special publication 800-41, page 11, fig 2.5

11 (From previous page) Extracted from www.cisco.com/c/dam/en/us/support/docs/interfaces-modules/catalyst-6500series-f.w-abrv

Firstly, a TCP connection is initiated and this is done as follows, the client (Host A) sends a SYNC (synchronize) packet to the destination host which is usually the server (Router 192.168.1.3/24 in fig 3.7) which in turn sends an SYNC-ACK packet back to the client host. The client will then send acknowledgment (ACK packet) of receiving the SYNC-ACK packet and the TCP connection is initiated. This process is repeated for many connections and the information related to each connection is stored in a state table.

Then, whenever a packet wants to pass through the firewall, the firewall will check in the state table if there is any active connection between the source and destination of that packet. If so, packet is accepted, if not, it is rejected. Below is an example of a state table:

Source address	Source Port	Destination Address	Destination Port	Connection State
192.148.1.100	1121	210.9.88.29	74	Established
192.162.1.132	1131	216.32.42.123	74	Established
192.162.1.141	1222	173.66.32.122	20	Established
192.168.1.146	1223	177.231.32.12	66	Established

[12]Fig 3.8

Examples of Stateful firewalls include;

a) Check Point FireWall-1
b) Cisco PIX

Advantages

(i) Flexible: They were originally designed for TCP/IP protocol suits, but can be used with most new protocols.
(ii) They have a good balance between speed and security and in this regard can be considered as being better than packet filters.
(iii) Stateful firewalls use less memory and CPU cycles.

12 Extracted from, Guidelines on Firewalls and Firewall Policy (pdf online) by John Wack, Ken Cutler and Jamie Pole, special publication 800-41

(iv) They protect the network against denial of service and spoofing (spoofing is whereby the source address of a packet is modified to match that of a trusted site so that it is accepted by the firewall)

Disadvantages

(i) Because stateful inspection occurs at lower layers, services such as user authentication are not possible.

(ii) UDP and FTP Stateful inspection cannot handle all protocols e.g. applications using dynamic ports, hence they have limited range.

3.5 CHOICE OF A FIREWALL TECHNOLOGY

The choice of which type of firewall to use for a given system is not solely dictated by the relative advantages and disadvantages of the various types explained above. No firewall can be said to be better than another with absolute certainty. First, one must analyse the system to be protected then choose the most suitable firewall technology according to the needs of that network. A firewall that is perfectly suited for 1 network may fail on another. Below is an example to further illustrate this point;

Example

In this example, the objective is to determine which type of firewall is most suited to handle the passive FTP connection described below.

Passive FTP is used by some browsers when they initiate an FTP connection. In such a connection the client host must have a TCP connection to port 21 of the FTP server, and another TCP connection to a port higher than 21 for data communication. Ports used in this interaction are made known to the client when the passive mode requests are sent by use of the PASV command.

Assume that the FTP server is located behind the firewall and that people on the internet can FTP to this machine.

Packet Filters: Packet filtering handles standard FTP connections relatively well simply because fixed TCP ports 20 & 21 are used. However, for passive FTP, in order to facilitate interaction between client and the FTP server, all ports above 1024 need to be opened. This creates an unwanted hole that can be used to breach the firewall by malicious software.

Application Proxies: Any UDP or TCP connection passing through an application proxy requires twice the usual number of connection points. For example, a client host needs two open connections when dealing with a normal passive FTP but in the case of application level gateways, four connections are required. However, operating systems are designed in such a way that they have a limit to the number of open connection they can handle at any given time. Therefore, it can be seen that since application proxies work by increasing the number of ports, they are virtually incapable of handling passive FTP connections in high performance, high speed networks.

Stateful Inspection: These firewalls have an ability to understand connection context. When a client sends a PASV command to the server, Stateful Inspection reads the server's response and opens only the ports that are required for the passive FTP connection thereby significantly reducing security risk. Also, the stateful inspection allows the operating to perform all the routing function hence no permanent connections are established on the firewall and, once FTP connection is terminated, all open ports are closed.

Hence, on the analysis of how each the three standards handle the connections, it can be seen that Stateful Inspection firewalls are the most suitable to handle passive FTP connections.

CHAPTER FOUR: FILTERING

4.1 FILTERING OVERVIEW

INTRODUCTION

Because of its diversity, some of the information found on the internet may be viewed by some, as being offensive or unacceptable. For example, most parents do not want their children to have access to pornographic material. Also, there are governments who view some websites e.g. Wikkileaks in China, as being undesirable to the well being of their countries.
Access to all such information can be controlled by the process of content filtering. The issue of content filtering, sometimes referred to as information filtering or content screening will always be subject to debate and listed below are some of the reasons for filtering;

- Cultural: societies differ when it comes to matters concerning dress code and what is viewed as okay in some countries may be viewed as totally unacceptable in others.
- Political: other governments may wish to protect national interests by denying citizens access to sites that they deem inappropriate.
- Educational: some parents or institutions may see the need to only restrict internet access to websites that are scholastic.

This chapter deals with filtering at a transport level and explains the filtering schemes and protocols that are currently in use.

Definition

When applied to internet security, information filtering refers to the process whereby data packets that fail to meet configured requirements are blocked from entering a network. Filtering usually occurs at the network interface and is done by packet filtering software such as packet filters.

4.2 TYPES OF FILTERING

There are two main methods employed in network data filtering, the dynamic method and the database method.

In dynamic filtering, the filter analyses the web page to be opened and then uses a built in subroutine to classify the page as either enabled or disabled. The filter's appropriate subroutine analyses the web pages' keywords before classification is done. Although this method results in lower wait times for a page to be displayed, pages that meet desired criteria are sometimes blocked.

The database method operates by classifying website addresses and putting them all in a single database. Once a request to open a certain page is sent, the filter will search for the relevant address in the database and if it is listed as blocked, access will be denied, if not, access is granted. Major downsides of this method are:

(i) Database does not contain all web addresses.
(ii) Web addresses change frequently and therefore there is need for frequent updates and this is difficult to do.

Below are some of the different types of filtering;

Email Filtering

Email filtering can be done at both, the client or the server side. It is achieved by inspection of information contained in the mail headers, usually the sender's details or a file attachment.

Spam

Also called UBE (unsolicited bulk mail) or 'junk mail,' spam refers to the large numbers of unwanted mail that make their way to our mailboxes when we receive an email. Spammers utilize messaging software systems to send bulk mail, mostly to advertise discretely while evading any charges.

To mitigate this, software has been developed to examine transport level characteristics and differentiate spam from legitimate mail. However, spammers have also evolved and it is now extremely difficult to differentiate spam from legitimate mail by transport level analysis.

Browser-based Filtering

This is achieved by using a browser extension to enable or disable sites according to desired requirements. A browser extension is a computer software program that enables one to have control over their browsing experience, and is created by use of web technologies such as HTML and Java.

Content limited Filtering

This is achieved by liaising with ISPs so that only those sites that are permissible will be offered to the general populace.

Search Engine Filtering

Most search engines have a safety filter that can be turned either on or off whenever the authorities feel there is need to do so. As such, all material that is deemed inappropriate will not appear on search results although access can be gained by use of that site's URL address. This is handy because, to some extent, it does not allow kids to view adult sites.

4.3 FILTERING SCHEMES

In general, the higher the OSI model layers on which a filtering scheme operates, the better the filtering capabilities of that scheme. Each of the protocols shown in fig.2.4 supports some form of filtering. However, table fig.2.4 is not exhaustive and only the most prominent protocols are listed. This section describes filtering schemes, one for each layer, starting at the application layer.

SMTP Filtering

The simple mail transfer protocol is found on layer 7 (Application layer) of the OSI model. It is responsible for all the emailing in a network. The processes that occur during a single SMTP filtering session are described below:

First, the email sender's host, through the local server, will make itself known to the receiving host. The SMTP filter will respond to this by sending a message that contains what it is enabled to do, to both sender and receiver. This action is followed by the sender sending a message that contains its email address. Another message is sent to the receiving host, and this time it contains the recipient's email address. If there are any anomalies, the session is terminated. If all requirements are met, the sender will give a BDAT command, whose purpose in this case will be to inform all concerned parties that all is well, and the email is sent. When the mail is received, an acknowledgement message will be sent back to the sender. Lastly, a QUIT command is sent to the local server by the receiver's server and the session will be closed.

ASCII Filtering

The ASCII protocol appears on layer 6 (Presentation) of the OSI model. ASCII filtering is a 'capture in hardware' feature and it adds a new functionality to data filtering. Basically, ASCII filtering works by filtering off non-ASCII characters which are in turn converted into ASCII before being allowed through. This implies that ASCII filtering can be viewed as a method of data processing and not filtering in the traditional sense.

Network Basic Input Output System (NetBIOS)

This protocol is on layer 5 (Session) of the OSI model. It makes it possible for modern computer applications to communicate with computers that employ the TCP/IP protocol suit. This is achieved by the filtering off of old applications to enable compatibility between 2 computers that wish to communicate. Other functions of NetBIOS include,

(i) Establishing communication sessions
(ii) Distribution of datagrams to their intended destinations
(iii) Application Registration

TCP Filtering

This protocol is found on layer 4 of the OSI model. Rarely is TCP filtering explained independently and the reason for this that it is closely related to IP filtering. Usually, it is called TCP/IP filtering even though the two have very distinct roles. TCP enhances reliability of IP connections by assigning ports to IP addresses. TCP plays a major role in stateful inspection firewalls and this is explained in detail in section 3.4 of this document.

IP Filtering

Protocol is found on the Network layer, layer 3 of the OSI model. By definition, IP filtering is whereby data is filtered in accordance to source IP addresses. User/ administration reserves the right to block any IP addresses as per their requirements and these IP addresses may be singular or in a certain range. IP filtering does not rely in any way on the application utilizing a given network but only on the network connections. IP filters can be divided into several classes;

(a) Custom IP filters: these enable the network administrator to create a list of IP addresses and categorize them into 2, one that contains addresses to be blocked and another that contains those which are permissible.
(b) Country IP filtering: Every country has a unique set of IP addresses. This means that one can configure their filter to deny IP addresses from certain countries for different reasons e.g. one may block a country that is known for being a large source of spam.
(c) Advanced IP Checking: This feature gives the user an ability to choose how to deal with different proxy servers. This is achieved by the sustained monitoring of any device's ports and checking the appropriate FTP, HTTP and RDP resources.

Advantages of IP Filtering

1. Enhance profits in international businesses by enabling the maximization of profits where demand is high.
2. Non-potential customers are not allowed access to the site and this ensures that server resources and bandwidth is only reserved for potential buyers.

Protocols at layers 1 and 2

The Data Link and the Transport layers are hardware oriented and therefore any filtering that occurs there is not software related. The filtering here is usually done in transmission channels by high pass filters, band pass filters or low pass filters, and is mainly aimed at controlling bandwidth.

CHAPTER 5: CONCLUSION & REFERENCES

5.1 CONCLUSION

This research has helped to give a clear illustration on the importance of firewall technology in all network security. The literature review explains the basic idea behind firewalls i.e. never allow unwanted material (malware) from accessing a network, and shows why this is a superior approach compared to other security mechanisms e.g. anti viruses, which allow malware to enter a network and then attempts to destroy it. The document also shows the important role played by the OSI model in network communications and how it helps to describe the different firewall standards currently in use. However, it is imperative to note that this OSI model has many shortcomings and some of these are described below:

(i) The OSI model cannot be employed in systems that use higher level programming languages.

(ii) Because some protocols appear on more than 1 layer, it is difficult to implement and hence it has been widely criticized by some experts.

(iii) The many layers of this model result in slow communication and this is viewed as a major drawback particularly in LAN applications.

(iv) The engineers who came up with the OSI 7-Layer model deliberately excluded some technical aspects involved in data transmission to preserve simplicity and hence it can be inferred that it is not exhaustive.

Thus, it is clear that more research needs to be done to improve how internetwork communication is explained and therefore enhance network firewall technologies. There is need to reduce to the number of layers in the OSI model because as it stands, the 7 layers are just too much and the desired simplicity is to some extent, not realized.

The relative advantages and disadvantages of the 3 firewall standards described in this document are presented in chapter 3. However, the choice of which firewall to use for a particular network does not solely depend on them. The type of network to be protected, the budget and the information that needs to be preserved are all factors that need to be considered when choosing a firewall.

Most people who extensively use their emails know how annoying spam can be. Currently, spam is being countered by filtration at a transport level through analysis of IP addresses.

But, with the amount of illegitimate mail that makes its way to people's mailboxes, it can be concluded that this has not been very effective. Alternatively, more spam can be avoided by TCP analysis hence there is need for further research.

This document is relevant to anyone who wishes to set up any kind of network where information security is a priority.

Lastly, the process of gathering and selecting the appropriate information for this document was extremely strenuous. This was mainly because 'reputable texts' sometimes contradict and careful analysis had to be done to determine what information to discard. However, working through this project and compiling this document was a thoroughly satisfying exercise!

5.2 REFERENCES

1. Web Security by Amrit Tiwana, digital press (UZ main library)

2. Essential Check-Point, Firewall-1, by Dameon D. Welch-Abernathy (UZ library) / http: // www.aw.com/cseng/

3. Guidelines on Firewalls and Firewall Policy by John Wack, Ken Cutler and Jamie Pole, online pdf special publication 800-41

4. The Accidental Administrator: Cisco Router Step-by-Step Configuration Guide by Don. Crowley

5. Networking with Microsoft TCP/IP, Certified Administrator's Resource Edition, by Drew Heywood and ROB Scrimger

6. Cisco Security Specialists, Guide to PIX Firewalls by Vitaly Osipov, Mike Sweeny, Woody Weaver, Charles E. Rile, Umer Khan

7. BBC news (www.bbc.com) and CNN news (www.cnn.com)