COMPARATIVE STUDY OF WEB APPLICATION AND NETWORK FIREWALLS

A PROJECT REPORT

Submitted by

Raghu :RA1811003010303
Jugal Prasad :RA1811003010306
Nilaabh Keshav:RA1811003010295
Jadhav Sudhir :RA1811003010300

Under the guidance of
Mrs S.Poornima
Assistant professor
(Department of computer science and engineering)

Bachelor of technology in Computer Science and Engineering

S.R.M. Nagar, Kattankulathur, Kancheepuram District

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this project report titled **Comparative study of web application and network layer firewalls** is the bonafide work of

Jadhav Sudhir [RA1811003010300]
Nilaabh Keshav [RA1811003010295]
Jugal Prasad [RA1811003010306]
Raghu [RA1811003010303]

who carried out the project work under my supervision. Certified further,

that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candi-

date.

SIGNATURE

Mrs.S.Poornima

GUIDE
Associate Professor
Dept. of Computer Science & Engineering

TABLE OF CONTENTS

7- Benefits and limitation of network layer firewalls

8- Benefits and limitations of web application firewalls

9- Firewall attack mitigation technique

9.1-Conserve Resources in Use, While Maximizing Available Ones

9.2-Ramp up the defences

9.3-If Being infected -Become a Bot

10- Security requirement with Firewall analysis

11- Firewall deployment with LAN access control

12- Firewall deployment with application level control

12.1-A definition of Application control

12.2-Feature and benefit of application control

12.3-Deploy web Application Firewall

13- Firewall deployment with Comprehensive server security

13.1-Virtualized server environment -A technology overview

13.2-Virtualized server hardware function

13.3-Protection for virtual network configurations

14- Benefits of combination

ABSTRACT

Cyber attacks have been bothering many organisations including well established as well as newly established startup firms. Firewalls are looked up as saviours from these attacks which can cause the severe problems to organisations and humans. Network layer firewalls can stop the attacks to some extent but the problem persists.Web application firewall can prevent these attacks to some more extent. In a technical sense, the difference between application-level firewalls and network-level firewalls is the layers of security they operate on. While web application firewalls operate on layer 7 (applications), network firewalls operate on layers 3 and 4 (data transfer and network).This project is going to focus on differences between the two in detail with their functionality,performance and power with providing information about common cyber attacks.

1 INTRODUCTION

1.1 FIREWALL

Firewall is a protective barrier which stands and protects network from any traffic or packets that seem to be a threat to the trusted network (SearchNetworking, 2015), it provides protection for user data and services against risks associated with Internet connectivity (Dominguez, 2000-2002). There are different type of firewalls that protect the layers of TCP/IP models.

2 TCP/IP COMMUNICATION FOR FIREWALL

TCP/IP is a basic communication protocol of the internet, TCP/IP are two separate protocol, which does something individual on their own. The Transmission Control Protocol (TCP) ensures the reliability of data transmission across Internet connected networks. TCP examines packets for errors and resubmits packets if any errors are found, whiles Internet Protocol directs how packets of information are sent out over networks, (Hope, 2015) .TCP/IP are used together to defines a set of rules allowing computers to communicate over network. TCP/IP ensures data are packaged, addressed, routed and successful delivered to the right destination. (Safaa Zaman; Fakhri Karray , 2009).

In the TCP/IP model, there are four layer of TCP/IP and each layer has their own role and function. Furthermore each layer has vulnerabilities and different types of attacks depending on the layer the attack occurred. Firewall has been implemented and firewall operates and functions differently depending on the layer the firewall are deployed. (Safaa Zaman; Fakhri Karray , 2009). The four layer of TCP/IP Model are:

- Application Layer
- Transport Layer
- Internet Layer (also referred as Network Layer)
- Network access layer (also referred as Data Link Layer)

Application Layer is the upper and fourth layer of TCP/IP Model, the Application layer is responsible for providing network service to application. Application layer ensures the host programs interface with Transport layer service to use network (Thomas, 2008-2015). The Application protocols that functions on the application layer are HTTP, FTP, SNMP and Telnet etc.

Transport Layer is the third of fourth layer of TCP/IP Model, the Transport layer is responsible for transmitting data. Transport layer uses TCP or UDP protocol to functions on this layer. TCP is considerably reliable because it ensures that the data transfer takes place and guaranteed delivery to the destination host whiles UDP does

not guarantee data delivery. TCP carries out checks to ensure the data has safely arrived but if any error was found, it will retransmit the packet which UDP does not do that. (Authority, 2010)

Internet Layer is the second of fourth layer of TCP/IP Model, internet layer is responsible for data that contains source and destination IP address. Internet layer turns the data to IP Datagram then ensure the datagram is forwarded to the appropriate destination IP Address. The protocols that functions on the internet layer are Internet Protocol, Internet Control Message Protocol (Thomas, 2008-2015).

Network Access layer is the first and lowest of fourth layer of TCP/IP Model, Network Access layer is responsible for ensuring the data is physically sent across network, Network access layer does this by sending bits signals through wire or wireless. The protocols that functions on Network access layer are Ethernet, Frame delay (Thomas, 2008-2015).

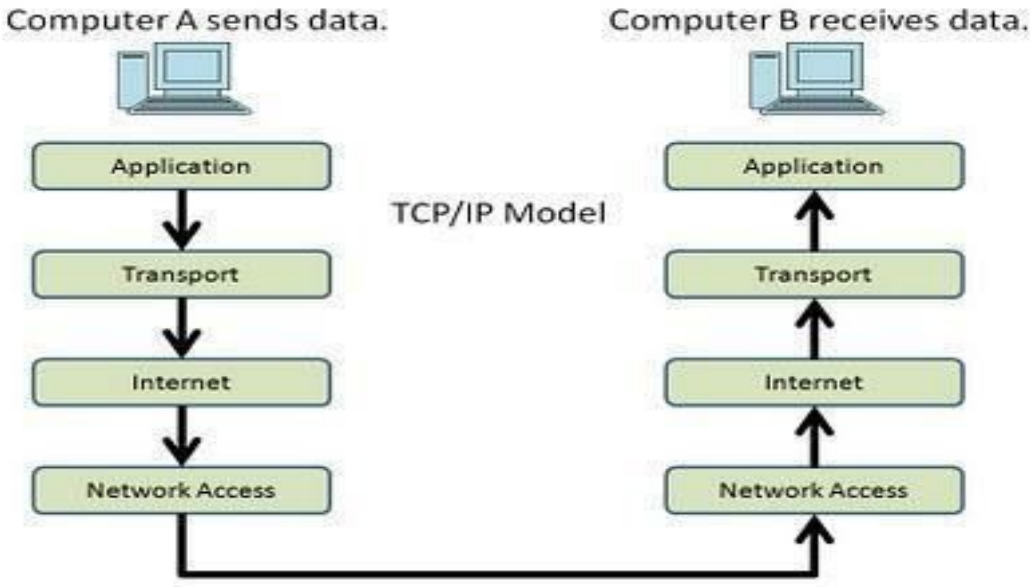


Fig. 2:1: Data Flow through TCP/IP (TCP/IP MODEL, 2014)

Communication takes place within the TCP/IP Model when the application sends a data in **Fig.2:1.** As soon as Computer A send the data, the data moves down to Transport Layer, where UDP or TCP adds the source and destination port numbers on the data and then passes it on to Internet Layer. The Internet layer adds the source and destination IP addresses and passes it on to the network access layer. The network interface layer adds the source and destination Ethernet addresses. Computer B receives the data on the network access layer then uses the same procedure to move the data up from network access to Application Layer. (Routing First-Step: TCP/IP layered protocol model, 2015)

TCP/IP MODELS	FIREWALLS
Application Layer (HTTP)	APPLICATION LAYER FIREWALL
Transport Layer (PORT)	NETWORK LAYER FIREWALL
Internet Layer (IP)	NETWORK LAYER FIREWALL
Network Access Layer (MAC)	NETWORK LAYER FIREWALL

Table. 2.1 – Implementation of Firewalls (FIREWALLS, 2015)

2.1 APPLICATION LAYER FIREWALL

Application layer firewall works on application layer of TCP/IP Model, application layer firewall stands between an internal client and any externally held server. Application layer firewalls are used to allow or disallow connections and these firewall never allows a direct connection between an internal client to the external server due to this the external server never has access to the internal network. Application layer firewall prevents execution of files which has been affected, it disallows any malicous code to executed due to its harmfulness. (Dominguez, 2000-2002)

Since application layer firewall deals with web traffic protocols such as HTTP. Web application firewall has been implemented to take responsbile for web traffic such as HTTP, HTTPS traffic and HTML and prevent any web based attacks to the network.

2.2 WEB APPLICATION FIREWALL

There are many Web applications of all kinds, some are in form of online shops or partner portals, attackers try any possible means to gain access or steal information for financial gain. The attackers use different methods which are mainly aimed at exploiting potential weak spots in the web application. Network layer firewall are not

capable of detecting web based attacks on web application (Maximilian Dermann, 2008).

Implementing web application firewall enhance extra layer of security since Web Application Firewalls protects web applications from web-based attacks, Web application firewalls examines HTTP traffic which comes in and out of web applications. The most significant problem of web application is SQL Injection. However the solution to this problem is to implement web application firewall. (Maximilian Dermann, 2008)

2.3.1 Web Application Firewall Architecture

There are different type of web application deployment and operating mode depending on the security of policies. This project will elaborate on the most significant deployment and operating mode of Web Application Firewall Architecture.

2.3.1.1 Appliance-based Web Application Firewall

Appliance-based Web application deployments stand behind the firewall and in front of organizational web servers (Beechey, 2009). Application-based Web Application are normally installed closest to the application and sometimes joined into the application code itself.

One of the example of Appliance based Web Application firewall used in this project to protect from web based attacks is ModSecurity, which normally installed as a module in Apache. An application can benefit of the features permitting the overhead to be held by the local server. The cost of deploying an application-based Web application firewall is usually low. (TechTarget, Introduction to Web application firewalls in the enterprise, 2000-2016)

Operating Mode in Web Application Firewall Architecture

The Important operating modes Web Application Firewall are:

- Reverse Proxy
- Layer 2 Bridge
- Network Monitor/Out of Band
- Host/Server Based
- Internet Hosted/Cloud (**New**)

2.3.1.2 Reverse Proxy

In this mode, the Web application firewall has an IP address and stands inline. Any incoming connection to the application is forwarded to the web application firewall which makes a distinct request to the web server. Encrypted connections are ended at Application Layer allowing the web application firewall decrypt and examine the web

traffic. **Fig 2:2** illustrates the architecture of the Web Application firewall and the position of the Reverse Proxy Server. It is the device with the shield and standing between the firewall and web server. (Pubal, 2015)

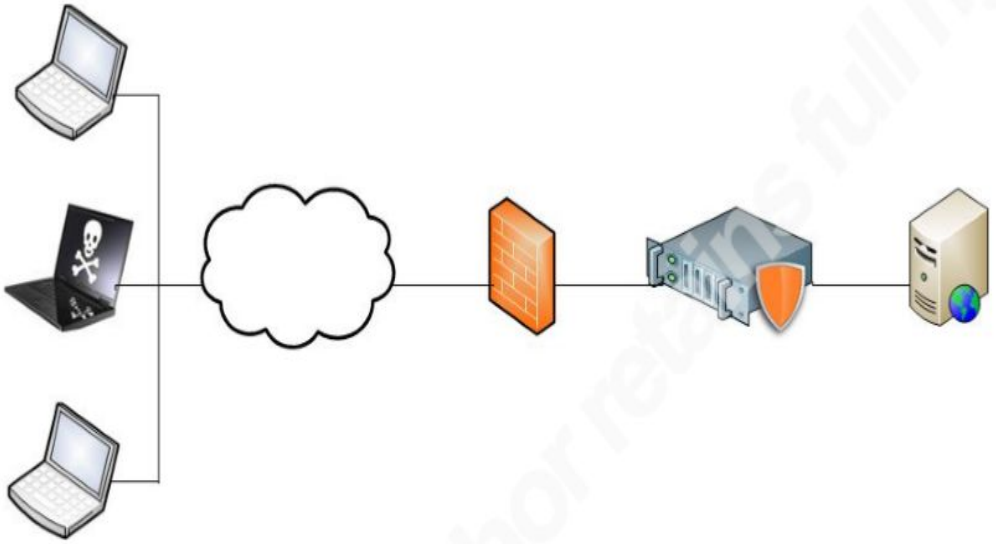


Fig. 2:2: Reverse Proxy Mode (Pubal, 2015)

2.3.1.3 Layer 2 Bridge

In this mode, the Web application firewall stands inline and performs as a Switch (Layer 2). The Web application firewall does passive SSL decryption, and is capable of blocking traffic by simply dropping the harmful packets. This permits for higher performance than reverse proxy with much less network changes (Pubal, 2015) but it does not offer an advanced services like other Web application firewall modes may offer.

2.3.1.4 Network Monitor/Out of Band

In this mode, the Web application firewall is not inline. It receives a copy of the traffic through the identifying port. It can inactively decrypt SSL traffic. The Web application firewall's ability to block traffic is quite limited, it only sends TCP-reset packets to interfere traffic. This mode has the minimum amount of effect on the network and application. It allows the Web application firewall to be configured to only alert on malicious traffic removing the danger of blocking false-positive detection and causing application (Pubal, 2015).

The architecture shown in **Fig. 2:3** demonstrate how the web application firewall standing as a switch and examines the traffic by receiving a copy of traffic passing to the web server. (Pubal, 2015)

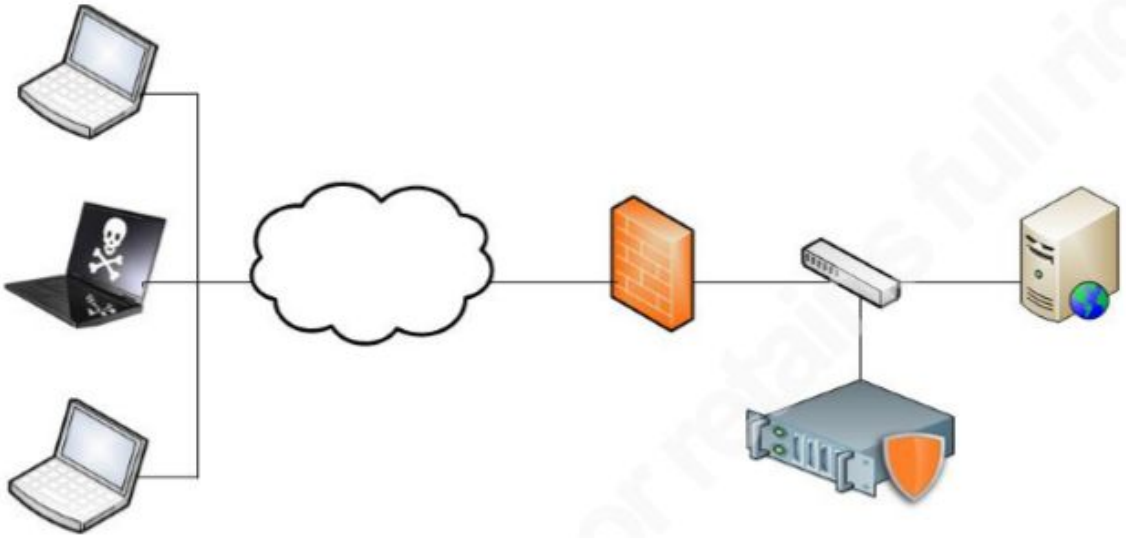


Fig. 2:3 - Out of Band Mode (Pubal, 2015).

2.3.1.5 Host/Server Based

A server based web application firewall is a software application implemented and installed on the web server. It is usually installed as an independent application or a web server plug-in. It puts additional load on the server.

The architecture shown in **Fig.2:4** demonstrates how the web application firewall functions as a software on the web server which represented as shield. (Pubal, 2015)

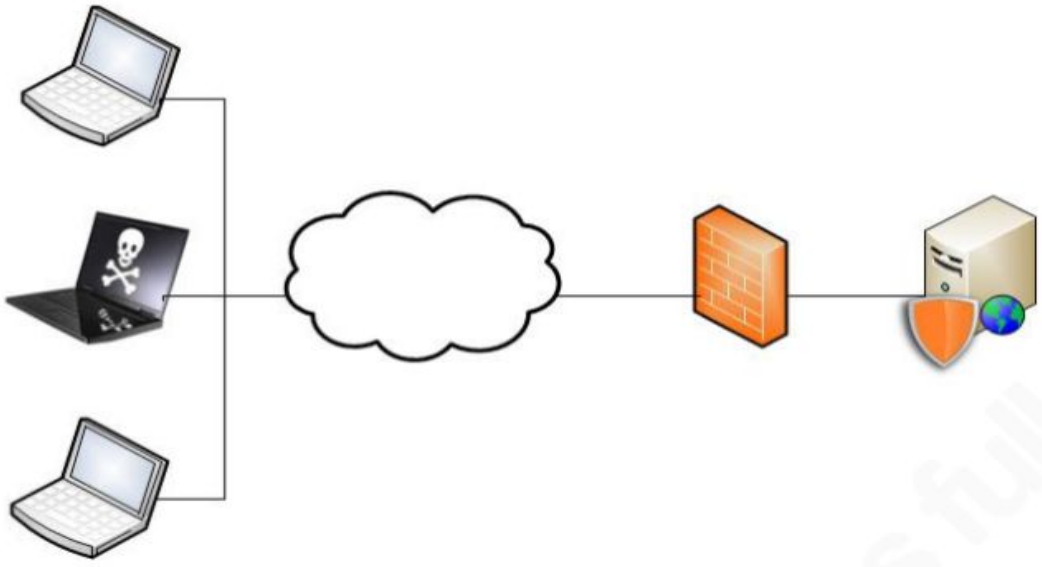


Fig. 2:4 – Host/Server Based Mode (Pubal, 2015)

2.3.1.6 Internet Hosted/Cloud (New)

This is a new Web Application firewall mode which the cloud provider implement web application firewall solutions. It is not widely used today but Gartner one of the world leading information technology and advisory company has predicted that more than 50% of public web application will be protected by Internet Hosted/Cloud web application firewall in 2020. It has been proved that less than 10% of public use internet hosted/cloud web application firewall today. This newly mode works more like reverse proxy, public DNS will be configured to point the cloud service, this will then establish another connection to the web application property (Pubal, 2015).

The architecture shown in **Fig. 2.5** demonstrates how the web application firewall represented as a shield in the cloud functions as a software as a service.

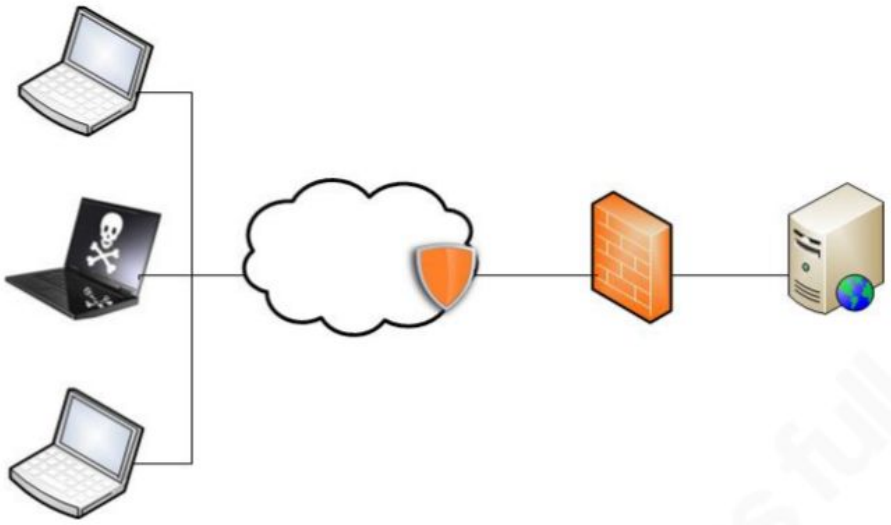


Fig. 2:5 – Cloud Mode (Pubal, 2015).

2.3 NETWORK LAYER FIREWALL

Network layer firewalls operates at Network Layer and Transport Layer (Layer 4) of the TCP/IP Model and Network layer firewall has the capability of making decisions on both Network and Transport layers. One of the signficant thing is that, it makes an important distinction about many network level firewalls when they route traffic directly through them. Which in that sense means, it can scan for source and destination information and accept or deny packets based on this information (Maxon, 2000).

Network firewalls are normally used when speed is needed. Packets are not passed to the application layer due to this the packets of its content is not examined, packets can be processed more rapidly. This is an advantage for firewalls that scan for connections to web and email servers, particularly the one that have high amounts of traffic. This is

due to the risk of delays when it comes to people accessing a website. This provides a layer of protection to the network and does not slow down the connectivity. Network firewalls are generally a cheaper option. Network layer firewalls functions under one of the following categories: packet filters and circuit layer gateways (Maxon, 2000).

2.3.1 Packet filter

Packet filter is a basic firewall which just examine packet then accept or deny based on the criteria given. It accepts or denies packet based on the source and destination IP address or source and destination port numbers based on the rule implemented (Maxon, 2000).

The two main functions of packet filter are Stateless Packet filter firewall and Stateful Packet filer firewall.

2.3.1.1 Stateless Packet Filter

Stateless Packet filter firewall just examines the packets based on source and destination, after the packet has been examined it accepts or denies packet. It does not understand the concept of TCP, it does not keep track of the packet that has already passed by. (Sharma, 2010) It is easy for an attacker to go through by indictating "reply" on the packer header (TechTarget, 2000-2015).

2.3.1.2 Stateful Packet Filter

Stateful Packet filter firewall on the other hand examines packets down to the application layer. Stateful packetful record every session information such as IP addresses and port numbers since stateful packet filtering understanding the TCP concept (TechTarget, 2000-2015).

2.3.2 Circuit Layer Gateways

Circuit layer gateways operate mainly in Transport Layer (layer 4). They make basic authorization decisions based on source and destination IP address as well as protocol type and port. This delivers a higher level of flexibility in that Circuit layer gateways decides whether inbound requests to ports are valid. Devices in VLSI Device like routers and switches have the capability of functioning like Network firewall (Maxon, 2000).

2.4 Network Firewall Architecture

Network Firewall architecture demonstrate how network firewall components are organized to deliver effective protection against users who are not authorised to access a network, network firewall is normally defined after the network security policy has been defined because it is supposed to be a model that enforces the security policy (Wiley, 2004).

The network security policy is imposed at secure boundaries within the network called perimeter networks (Wiley, 2004).

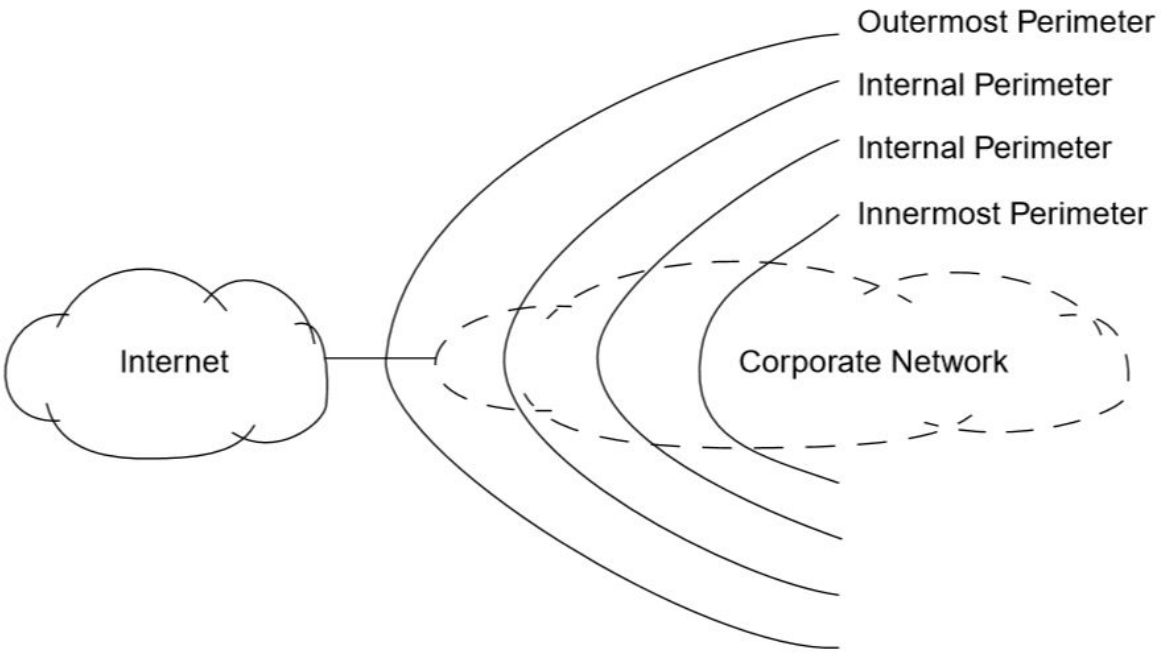


Fig.2:10 – Perimeter Network (Wiley, 2004)

In **Fig 2.10,** it demonstrates the possible firewall configuration, it shows that not all networks have three levels of perimeter networks. It is a neccesity to configure network firewalls to set network security policy or rules (Wiley, 2004). The architecture used in this Network firewall are:

- Screening Router
- Dual Home Gateway
- Screened Host Firewall
- Screened Subnet Firewall

2.4.3.1 SCREENING ROUTER

A screening router is a basic element of firewall architectures and regularly consists of a commercial router. There are some cases routing can be host-based, normally on hosts using the UNIX operating system. Screening routers filter the datagrams passing between the network connections in accordance with a previously defined routing table. Filtering is normally performed on IP datagrams based on these following fields(Harris, 1998).

- Source IP address
- Dual-Homed Host Firewall
- Destination IP address
- TCP/UDP Source port
- TCP/UDP Destination port

Furthermore, some routers have the capability to differentiate which network interface a datagram arrives on and use this information to make decision how the router should be filtered. It is very useful when traffic needs to be segmented from the exact networks and in removing IP address spoofing. Datagram arriving at the external

interface are known as inbound packets and datagrams arriving at the internal interface are known as outbound packets (Harris, 1998).

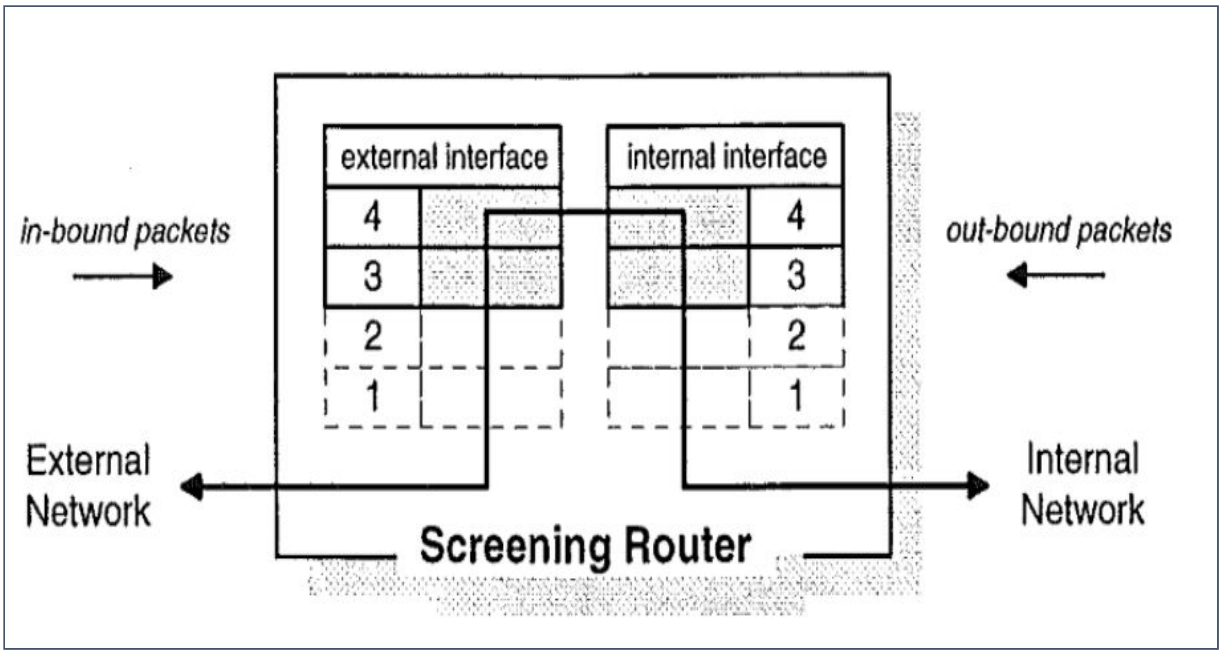


Fig.2:11 – Screening Router functioning at the TCP/IP Model (Harris, 1998).

In **Fig.2:11**, it demonstrates how the Screening Router operates in the TCP/IP model which is Network layer (Layer 3) and Transport (Layer 4). The grey color in boxes of the TCP/IP protocol stacks shows the layers on which the filtering rules largely operate. The flow of traffic is demonstrated by the double headed arrow as the flow of traffic passes between the internal and external interfaces (Harris, 1998).

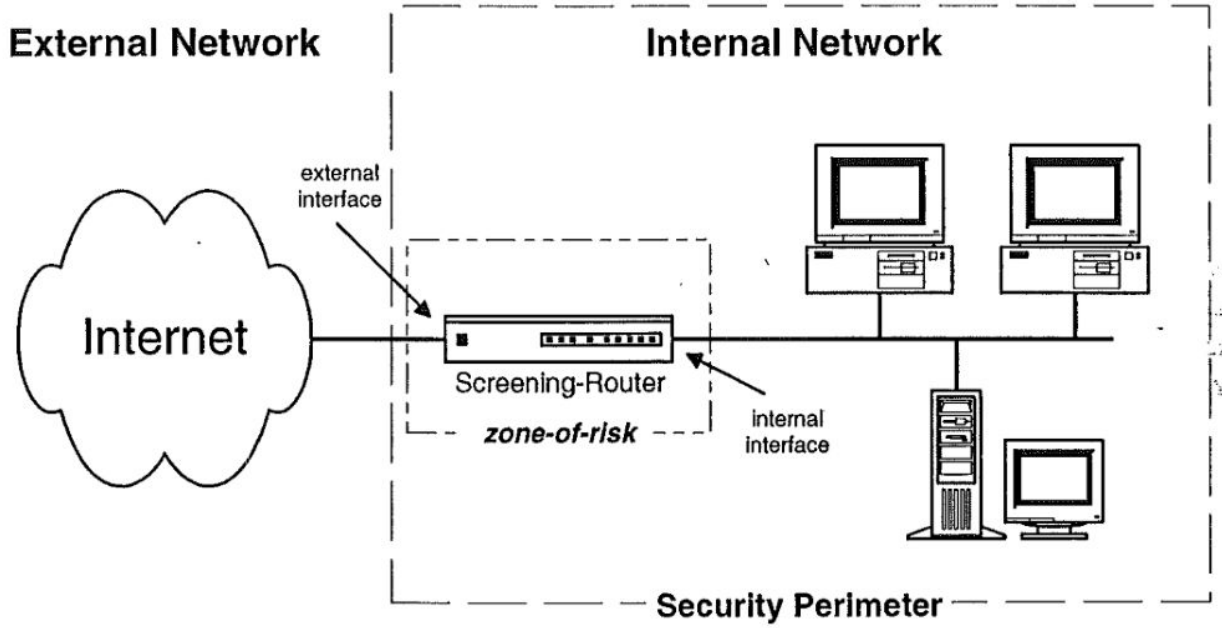


Fig.2:12 – Screening Router in firewall architecture (Harris, 1998).

In **Fig 2:12**, demonstrates the screen router based firewall architecture and distinguishing between the external and internal networks (Harris, 1998).

There is a straight communication paths between several hosts on the internal and external networks like the Internet. In a usual operation, the Zone of risk is visible and exposed to the number of hosts on the internal network and the number of peer-to-peer connections to the external network. The increase of hosts and connections make it very difficult to locate all the potential threat should be the Screen Router compromised (Harris, 1998).

The Screen router simply denies connections from to hosts or networks and also denies connections to exact ports. The capability of filtering on both UDP and TCP add an extra flexibility setting security policies (Harris, 1998).

Filter rules are usually implemented using a table of conditions and actions which are applied to each datagram until a deciding where to route or drop is reached. When the datagram has met all criteria stated in the row of the table, the action stated in that row of the table performs its duty, some systems apply the rules in a systematic manner from first to last. The rest impose an order based on the criteria in the rules, such as source and destination address (Harris, 1998).

A simple example of the screening-router, assume that University of Bedfordshire is breo.beds.ac.uk signified by the internal network shown in **Fig 2:12**, needs a mail connection to the University of Bedfordshire study.beds.ac.uk. A mail connection is regarded by a destination port number of 25, and a source port 2 $\geq$ 1024. The breo.beds.ac.uk mail connection is acknowledged by the 2 tuple "<IP number= 223.21.21.12, port 2 $\geq$ 1024>", however the study.beds.ac.uk mail gateway is acknowledged by the 2-tuple "<IP number= 192.15.18.5, port= 25>" (Harris, 1998).

The routing table requires to allow the type of connection as shown in **Table 2:4** (Harris, 1998).

ACTION	SOURCE IP ADDRESS	PORT NUMBER	DESTINATION IP ADDRESS	PORT NUMBERS	COMMENTS
Allow	223.21.21.12	$\geq$1024	192.15.18.5	25	Connection from breo.beds.ac.uk to study.beds.ac.uk mail gateway
Allow	192.15.18.5	25	223.21.21.12	$\geq$1024	Allow replies from the mail gateway at study.beds.ac.uk to breo.beds.ac.uk
Deny	-	-	-	-	If none of the above rules matches deny access to all other datagrams.

Table 2:4 – Routing Table (Harris, 1998).

2.4.3.2 Dual-Homed Host Firewall

In the dual homed host firewall, the host usually have two interfaces, one of them is connected to the private network (Internal Network) and the other one is connected to the Internet where it can get untrusted network (External Network). It is a must that all IP traffics passes through the firewall before arriving at a host in the private network (Internal Network).

The same way an internal host communicates with external hosts in the internet through the dual homed host. Straight communication that bypass or avoid the dual homed host is denied. This is done to ensure that IP packets from one network will not be directly routed to the other network. The dual homed host do not function as a router.

However, restricting IP packet forwarding makes sure the Internet and the private network are reasonably disconnected so even when system problems occur the firewall cannot fail exposed. IP packet can only be allowed through the firewall is through its application proxies itself not through the operating system layer (Wiley, 2004).

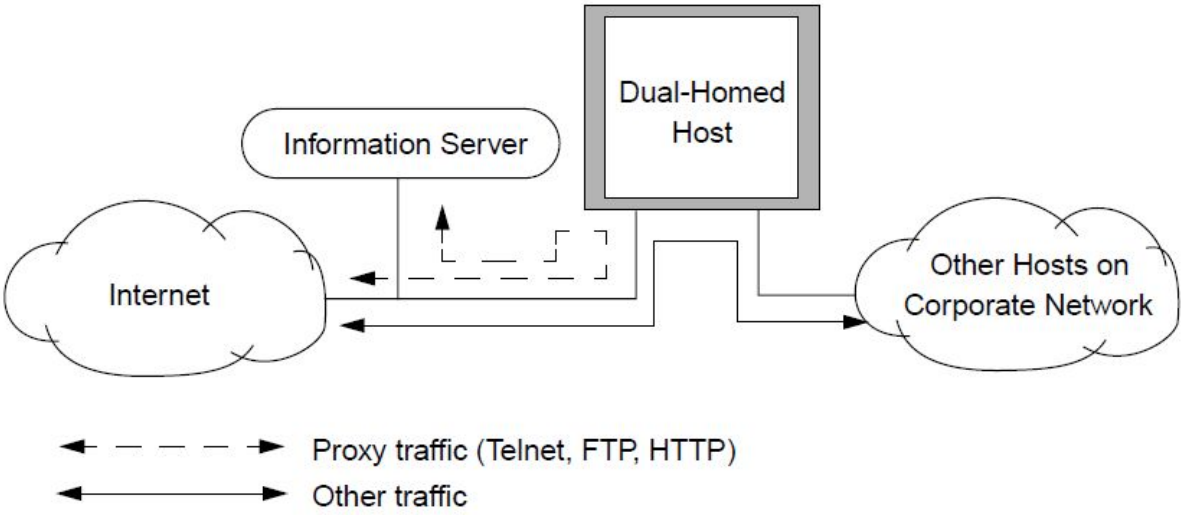


Fig. 2.13 – Dual Home Gateway Architecture (Wiley, 2004)**.**

The dual homed host blocks entries to the private network(Internal network) when it delivers proxy services like HTTP, FTP, the server offering the main service is placed between a packet filtering router and the dual-homed host which is present. This arrangement stops intruders from getting into the systems which securely protected by the dual-homed host (Wiley, 2004).

2.4.3.3 Screened Host Firewall

Screened Host firewall somehow differs from the dual-homed host firewall architecture, the dual home gateway permits the host firewall to be connected to two networks however the screened host firewall architecture rather permits the host providing the firewall to connect to the private network (Internal Network) only. A distinct screening router is located between the Internet and the host. The screened host firewall is a combined functionality of a packet filtering router and an application gateway (Wiley, 2004).

The screening router implements a packet filtering functionality and it configures which make the bastion host the only host in the private network (Internal Host) that can be examined from the Internet (External Network). Additional security can be implemented in the screening router by configuring it to decline traffic to exact ports on the bastion host as it shown in **Fig 2.14** the screening router is configured to accept or block connections between internal hosts and the Internet. The simplest 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.

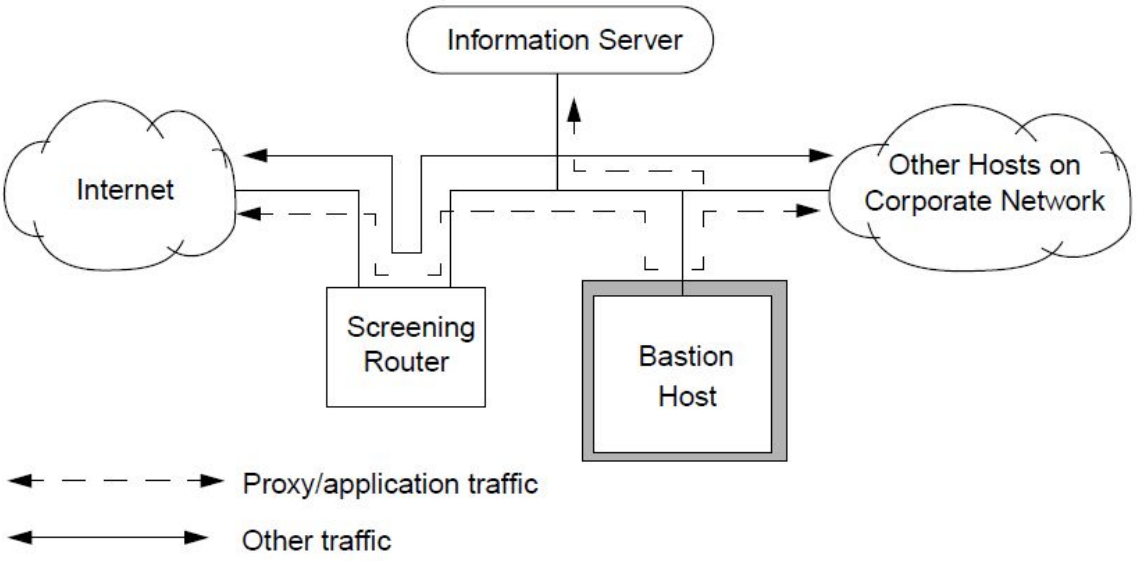


Fig. 2.14 – Screen Host firewall Architecture (Wiley, 2004)**.**

2.4.3.4 Screened Subnet Firewall

The screened subnet firewall is described as an extension of the screened host firewall. Similarly like screened host firewall, it normally uses both a bastion host and screening router but this firewall which could also be referred as the Demilitarized Zone. This gives an additional layer of security by including a perimeter network that further separate the private network (Internal Network) from the Internet (External Network). The firewall determines a Demilitarized Zone demarcated by the outer router and an internal router (Wiley, 2004).

The internal router and the outer router has Demilitarized Zone which is an inner screened subnet bounded. The information server and bastion host are placed within the Demilitarized Zone, as shown in **Fig 2.15**. The Demilitarized Zone is considered a separated network between the private network (Internal Network) and the Internet (External Network). The outer router prevents the network from external attacks by blocking entry to systems in the Demilitarized Zone (Wiley, 2004).

It also declines traffic to the external network from unauthorized sources in the internal network. The internal router controls Demilitarized Zone access to the internal network by passing traffic from the bastion host to the hosts in the internal network that are not in the Demilitarized Zone. Enable for an attack to get to any internal host placed outside the Demilitarized Zone, it must break through both routers (Wiley, 2004).

This architecture discloses only the Demilitarized Zone network to the outside world and retains the private network hidden (Wiley, 2004).

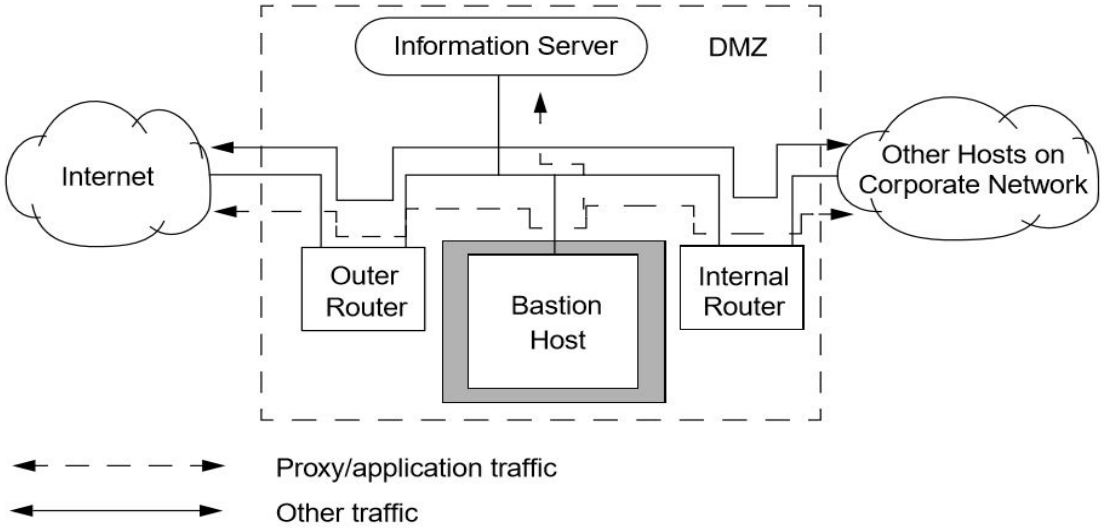


Fig 2.15 – Screened Subnet Firewall (Wiley, 2004)**.**

3 Network Layer Attack

3.1 *IP Spoofing Attack*

IP Spoofing attack is an attack occurs network/transport layer where the attacks transmits packets from the outside with a source address field containing an address of an internal host. The attacker expect that the use of a spoofed address will permit penetration of systems that employ simple source address security, in which packets from specific trusted internal hosts are accepted (Stallings, 2011).

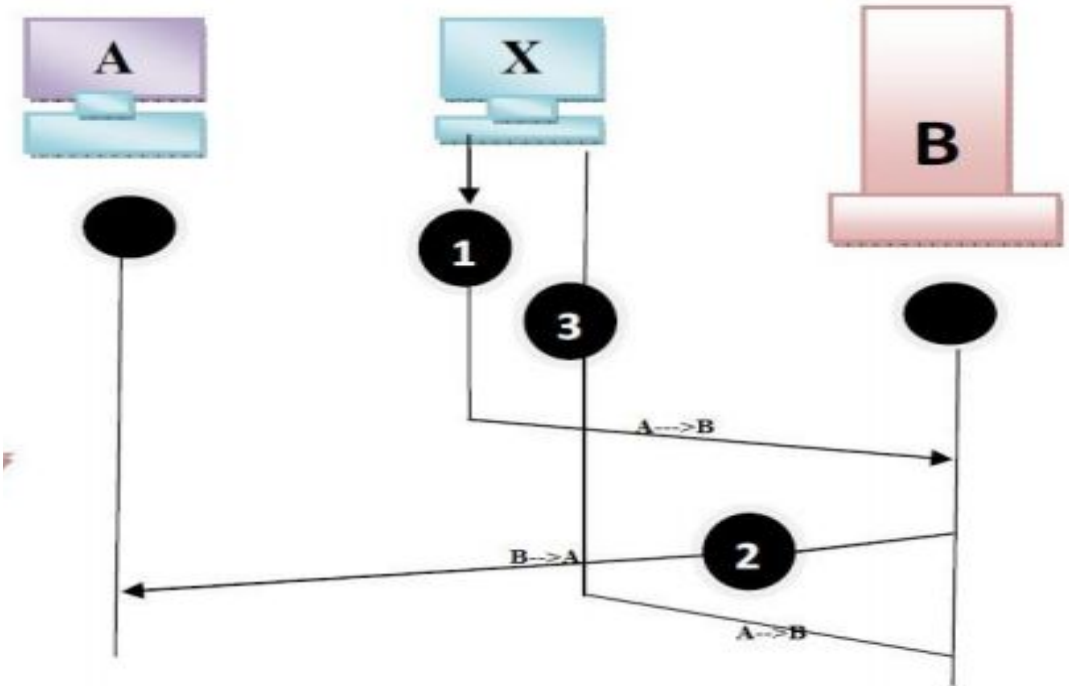


Fig 2:16 - Example of IP Spoofing (Ajit Kotkar, 2013)

In **Fig 2:16,** the IP spoofing attacker represent the "X" machine. The attacker managed to convince Machine "B" that he is the machine "A", The Machine "B" then sends packet to acknowledge Machine A, The attacker takes another packets that acknowledge the session number (Ajit Kotkar, 2013).

3.2 *DOS ATTACK - DENIAL OF SERVICE ATTACK*

Denial of service attack where the attacker sends multiple malicious traffic to targeted machine preventing the machine to be accessible to any service. The machine is normally kept so busy being responsive to the traffic receiving from the attacker that would eventually have not enough resources to respond to genuine traffic on the network (Ajit Kotkar, 2013).

There is another attack under Denial of service called **Distributed Denial of service attack**. This attack similar to Denial of service but this attack send a many-to-one malicious traffic to the targeted machine. It normally includes a machine carrying a master program and many machines have been controlled as zombies. They are mentioned to be as zombies because these machines which are normally the victim of a denial of service attack unknowingly become an attacker (Ajit Kotkar, 2013).

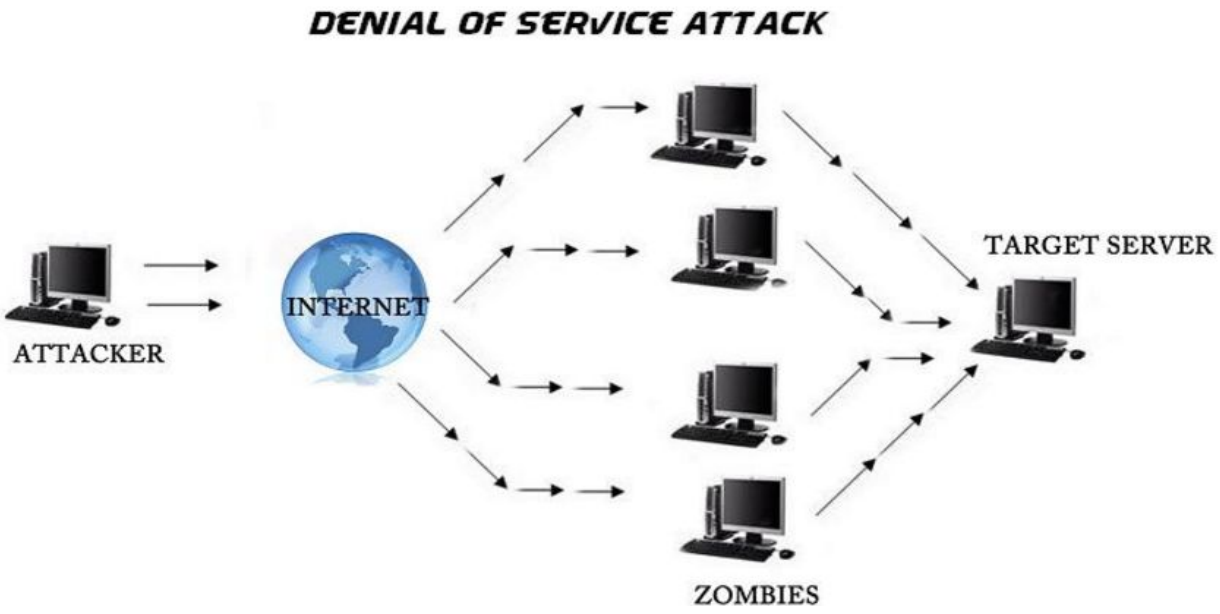
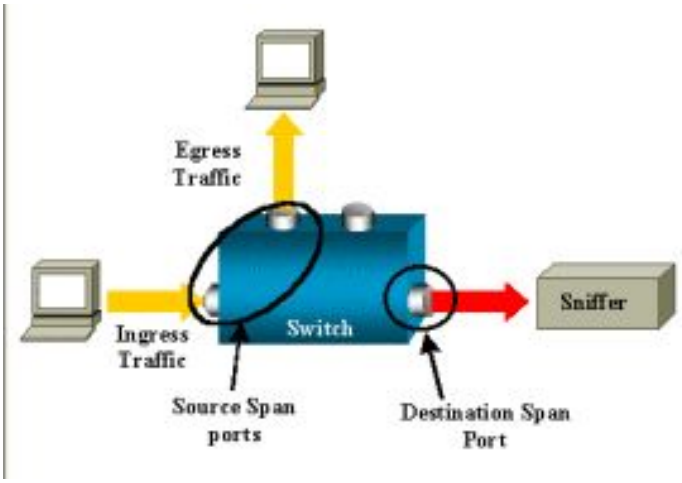


Fig 2.17 – Example of Denial of Service (How to Work DDOS Attack Protected Hosting, 2015)

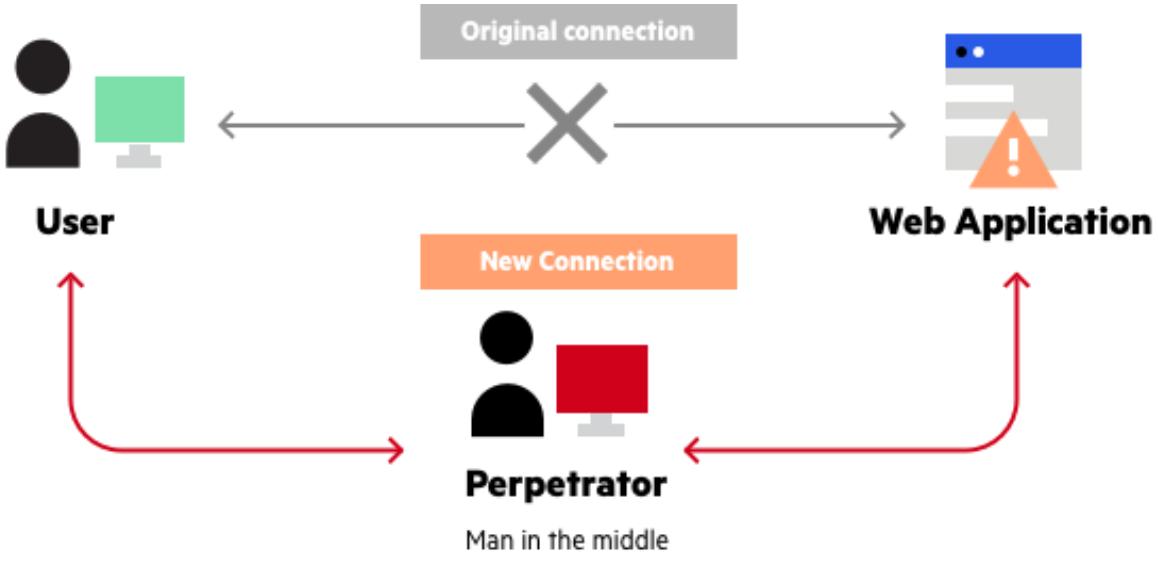
The zombie's machines exist in the victim's machine until they are directed by the main machine to attack another machine. This makes it extremely difficult to pin point the actual attacker since the attack is coming from the zombie machines which have no idea of the main attack as shown in **Fig 2.17** (Ajit Kotkar, 2013).

3.3 *Packet sniffer*

A passive receiver that records a copy of every packet that flies by is called a packet sniffer. By placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted! These packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages. some of the best defenses against packet sniffing involve cryptography.



3.4 Man-in-the-Middle Attack – As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

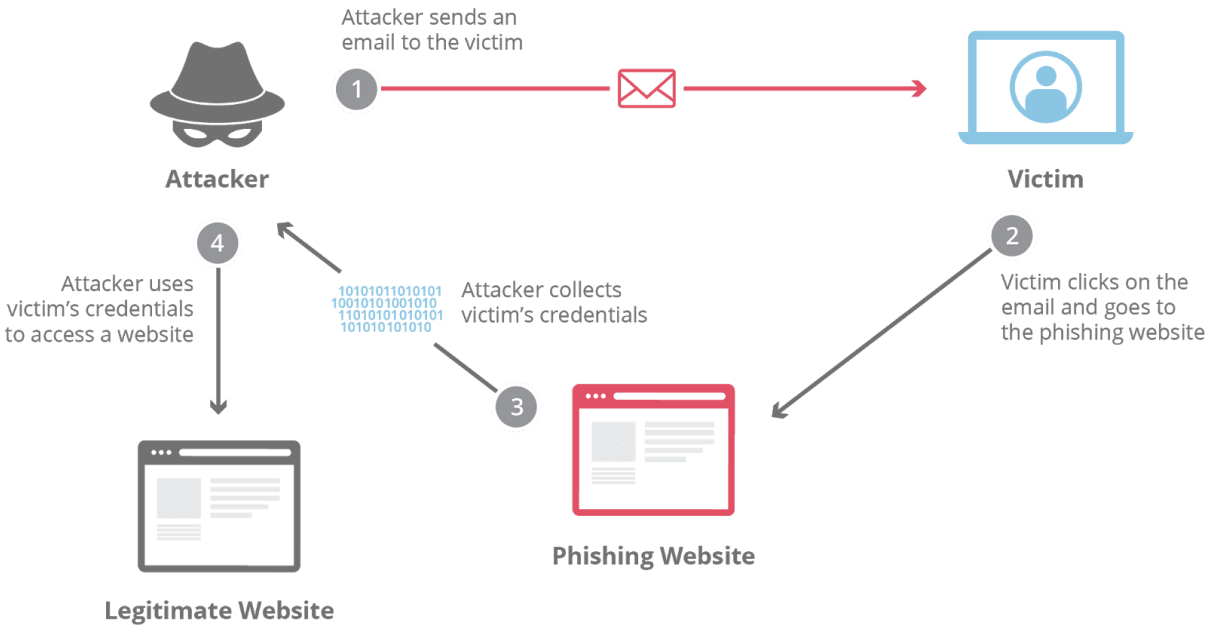


Phishing –

"Phishing" refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information. By masquerading as a

reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish.

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers is a good example of phishing.



3.5 DNS spoofing – Also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address.

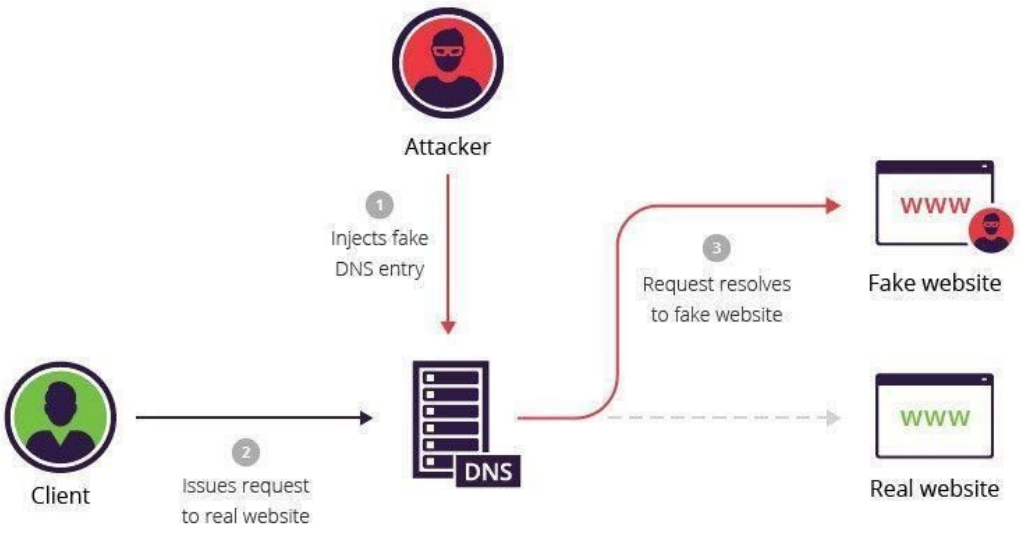
Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information. Furthermore, the malicious website is often used to install worms or viruses on a user's computer, giving the perpetrator long-term access to it and the data it stores.

Methods for executing a DNS spoofing attack include:

- Man In The Middle (MITM) – The interception of communications between users and a DNS server in order to route users to a different/malicious IP address.

- DNS server compromise – The direct hijacking of a DNS server, which is configured to return a malicious IP address.



4 Web Application Attacks

4.1 SQL Injection

SQL injection is an attack which the attacker input SQL code into a Web form on username box on web application to gain access to resources. An SQL query is a request for some action to be performed on a web application database. A successful attack gives the attacker the privileged bypassing authentication. (TechTarget, SQL Injection definition, 2006-2015)

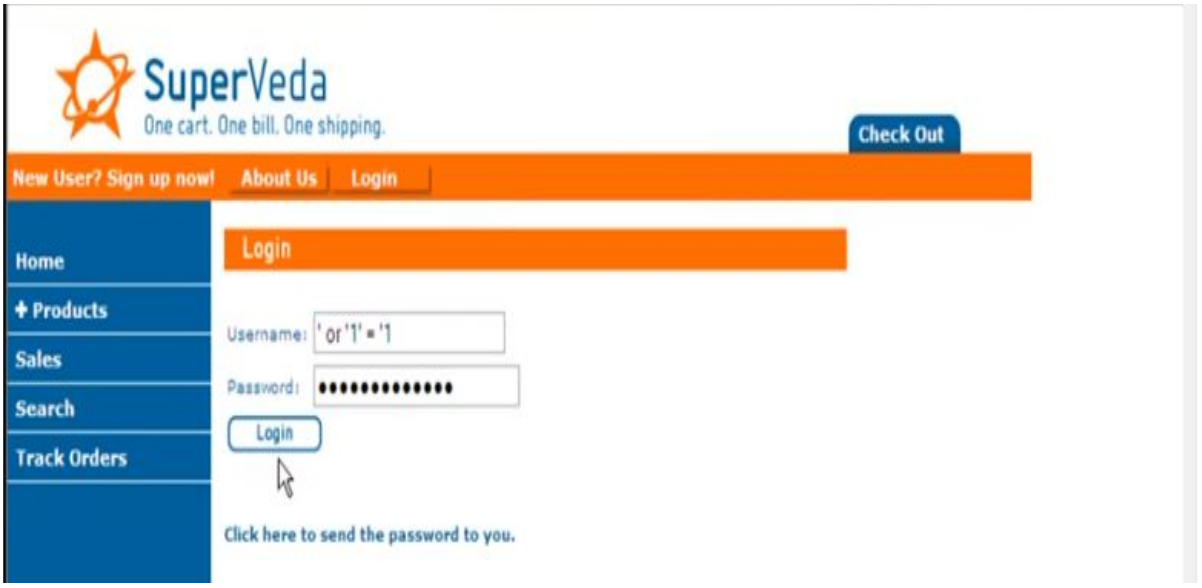


Fig.2:6: Attacker input SQL Injection on Web application (Imperva, 2009)

One of the basic malicious command of SQL Injection attack is 'OR '1' = 1'. As shown in **Fig.2:6.** If the web application is vulnerable, by inserting this malicious code will allow the attacker to login as the first user who last logged in. (Imperva, 2009)

Fig.2:7: Attacker has successfully used SQL Injection on Web application (Imperva, 2009)

After the malicious code has been successful, the attacker is able to get into someone's account which in the example given in **Fig.2:7**, it logins as "Mickey". The reason why it logins as "Mickey" is because with the malicious code the attacker has input in the

web form, the code will call the first user on the SQL Database, which enable the attacker to log in by passing the authentication process. (Imperva, 2009)

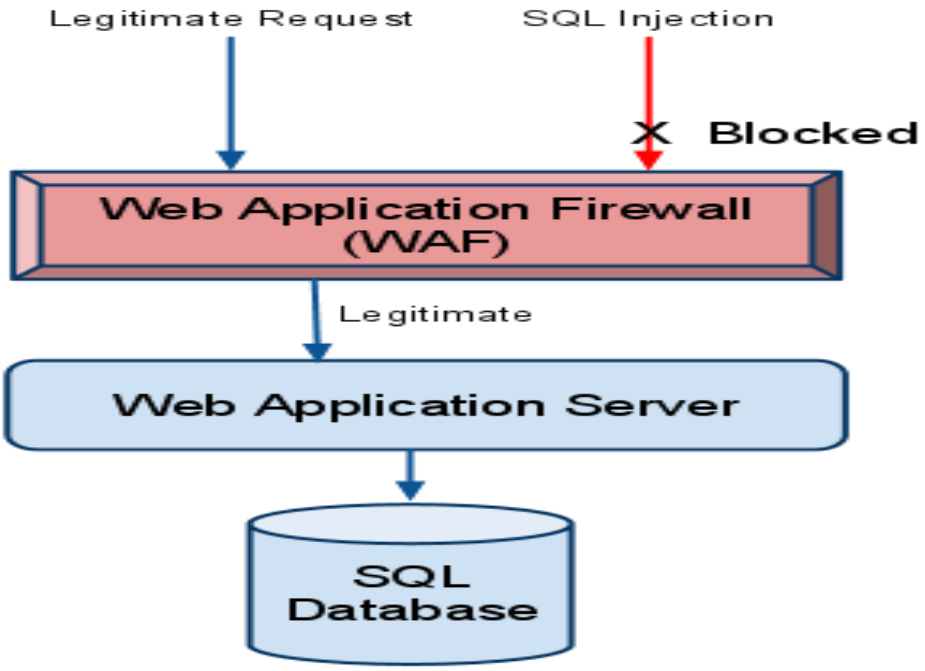


Fig.2:8 - Web Application Firewall examines & blocks SQL Injection (Acunetix, 2011)

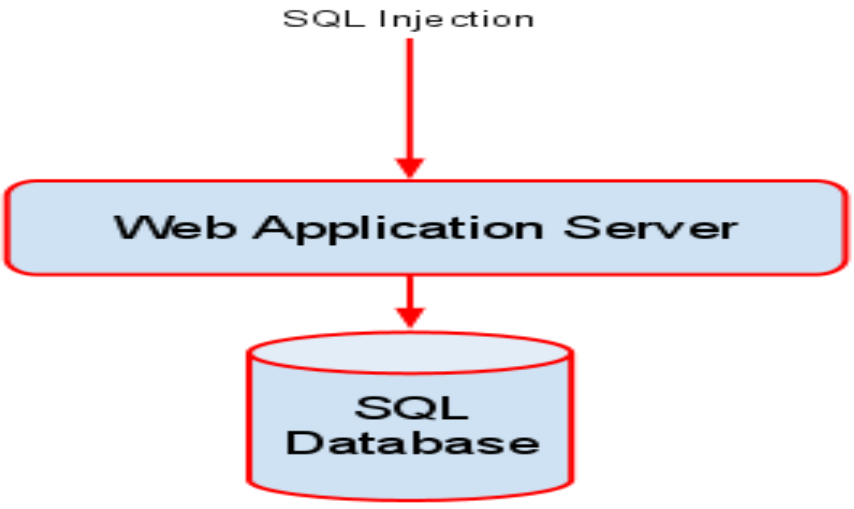


Fig.2:9 - No Web Application Firewall Implemented (Acunetix, 2011)

In the example shown in **Fig.2:9,** demonstrate how web application server is exposed and how there will be nothing to examine any incoming traffic, SQL injection attacker will have the advantage to get through the SQL Database (Acunetix, 2011).

4.2 CROSS SITE SCRIPTING

Cross site scripting is an web application attack on the privacy of user browser of a web site which can lead to a total breach of security when user browers details are stolen. Most attacks involves two parties usually the attacker and the web server or the attack and the client however the Cross site scripting attack involves three parties which are the attacker, a client and the web site (Amit Klein, 2002).

Cross-site scripting attacks normally takes place when attacker takes advantage of web applications that accept user input without validation. Most Web application are designed to customize content for the user by taking what user enters then returns input back to the user (Mark, 2014).

The customized responses are given in the **Table 2:2** below:

USER INPUT	VARIABLE THAT CONTAINS INPUT	WEB APPLICATION RESPONSE	CODING EXAMPLE
Search Term	*Search_term*	Search term provided in output	"search results for search_term"
Incorrect input	*User_input*	Error message that contains incorrect input	"user_input is not valid"
User's name	*Name*	Personalized response	"Welcome back name"

Table. 2.2: Customize Responses (Mark, 2014).

The aim of the Cross site scripting attack is to steal the client cookies, or any private information, which can recognize the client with the web site. The attacker can behave as the user in his/her interface with the site try to impersonate the user (Amit Klein, 2002).

Example of How Cross Site Scripting takes place through vulnerable web application

Fig.2:8 - Bookmark page that accepts user input (Mark, 2014).

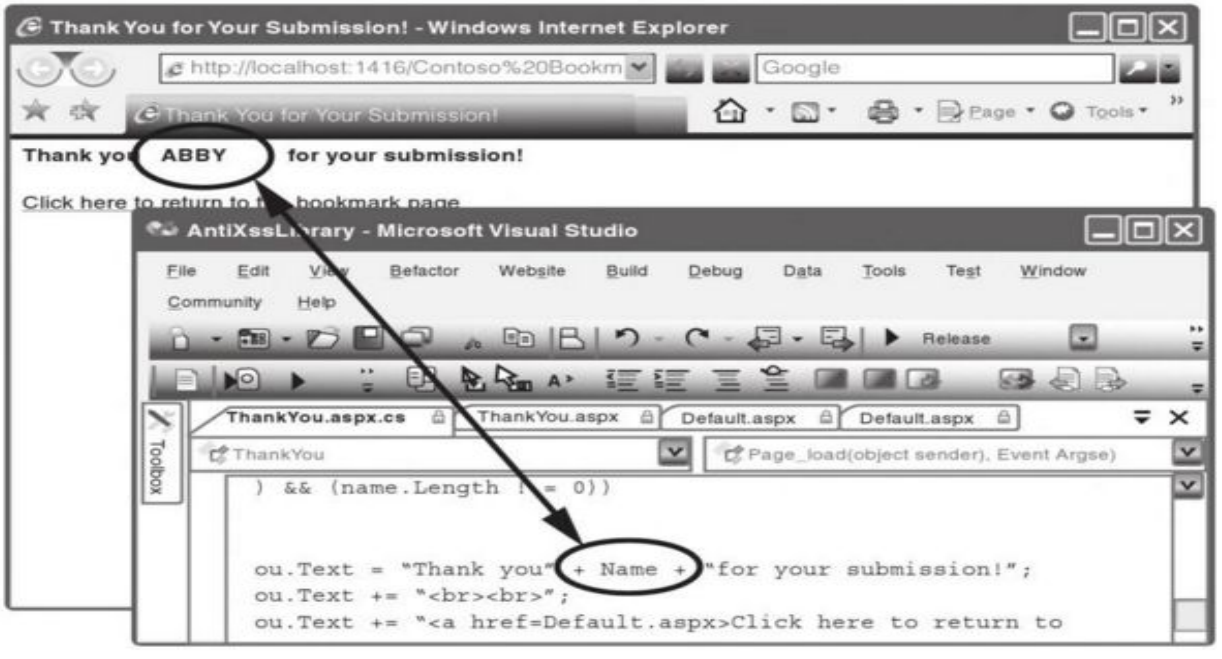


Fig.2:9 – Input used in response (Mark, 2014).

As shown in **Fig.2:8,** Web application that allows pals to share their favorite book with one another online, Browsers can input their name, input a description and insert URL of the bookmark and would then receive "Thank you" display. In **Fig.2:9,** the code that generate the "Thank You" display is demonstrated. (Mark, 2014)

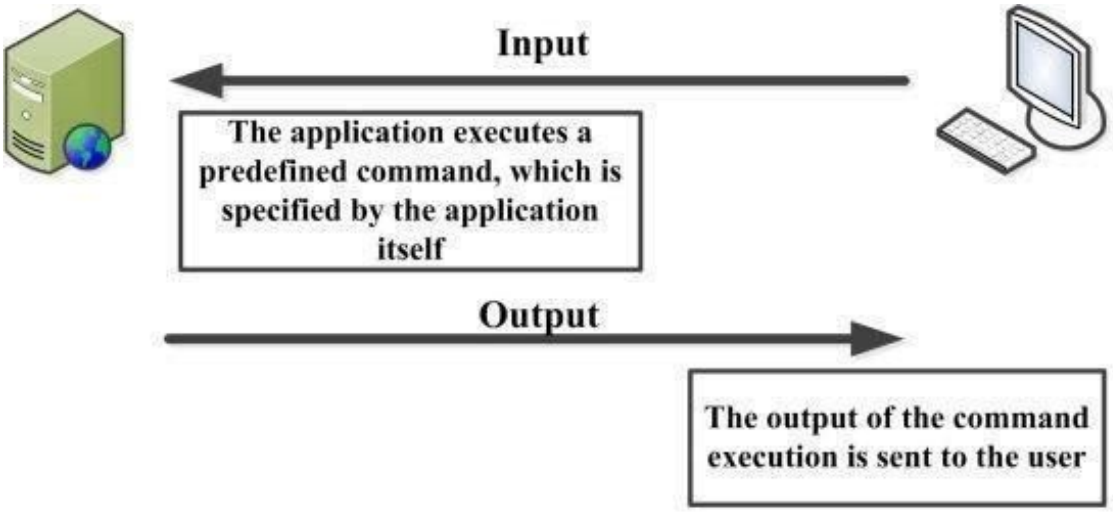
Cross Site Scripting attacks happens when the attacker benefits from a web application that approve user input without validating it and demonstrate it back to the user. When the user enters for "Name is not verified however it is automatically included in the code segment which becomes part of an automated response. The attacker uses this vulnerability in cross site scripting attack by luring a valid website into feeding a malicious script to another web browsers which will then be executed (Mark, 2014).

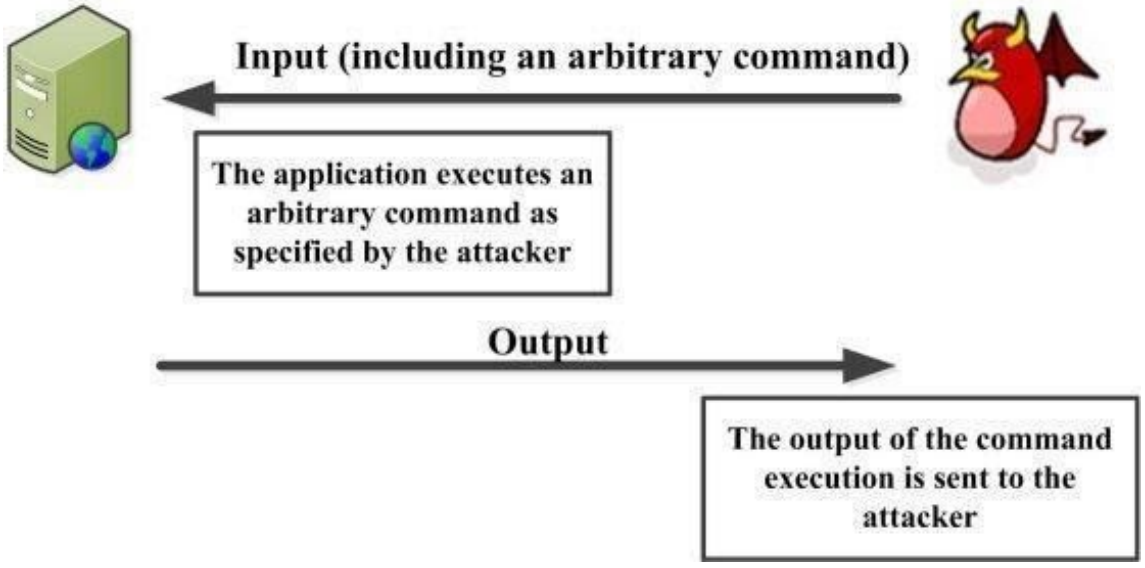
4.3 OS command injection attack

An OS command injection is when attackers input operating system (OS) commands into the server that is running the web application. It differs from an SQL injection because it enters from the server-side instead of the application-side. However, the consequences are very similar to an SQL injection attack, where attackers can take full control of the application. Attackers can command the application to display sensitive information, as well as modifying and deleting data. The application can also be utilized to compromise other parts of the corporate network, leading to further attacks within the organization.

Command injection is more likely to occur in a web application with possible vulnerabilities. Under this attack, notorious hackers inject operating system commands acting as pseudo system shell, which will then be executed through a web application. With the help of this attack, a hacker can use its pseudo system shell as an authorized user to gain access to critical data. This can occur due to a lack of proper input validation system.

Whitelist validation will help you to avoid command injection. And the most efficient way is to avoid "exec" out to the operating system if it is not required.





5 NETWORK LAYER FIREWALL

Network layer firewalls operates at Network Layer and Transport Layer (Layer 4) of the TCP/IP Model and Network layer firewall has the capability of making decisions on both Network and Transport layers. One of the signficant thing is that, it makes an important distinction about many network level firewalls when they route traffic directly through them. Which in that sense means, it can scan for source and destination information and accept or deny packets based on this information (Maxon, 2000).

Network firewalls are normally used when speed is needed. Packets are not passed to the application layer due to this the packets of its content is not examined, packets can be processed more rapidly. This is an advantage for firewalls that scan for connections to web and email servers, particularly the one that have high amounts of traffic. This is due to the risk of delays when it comes to people accessing a website. This provides a layer of protection to the network and does not slow down the connectivity. Network firewalls are generally a cheaper option. Network layer firewalls functions under one of the following categories: packet filters and circuit layer gateways (Maxon, 2000).

5.1 Packet filter

Packet filter is a basic firewall which just examine packet then accept or deny based on the criteria given. It accepts or denies packet based on the source and destination IP address or source and destination port numbers based on the rule implemented (Maxon, 2000).

The two main functions of packet filter are Stateless Packet filter firewall and Stateful Packet filer firewall.

Stateless Packet Filter

Stateless Packet filter firewall just examines the packets based on source and destination, after the packet has been examined it accepts or denies packet. It does not understand the concept of TCP, it does not keep track of the packet that has already passed by. (Sharma, 2010) It is easy for an attacker to go through by indictating “reply” on the packer header (TechTarget, 2000- 2015).

Stateful Packet Filter

Stateful Packet filter firewall on the other hand examines packets down to the application layer. Stateful packetful record every session information such as IP addresses and port numbers since stateful packet filtering understanding the TCP concept (TechTarget, 2000-2015).

Circuit Layer Gateways

Circuit layer gateways operate mainly in Transport Layer (layer 4). They make basic authorization decisions based on source and destination IP address as well as protocol type and port. This delivers a higher level of flexibility in that Circuit layer gateways decides whether inbound requests to ports are valid. Devices in VLSI Device like routers and switches have the capability of functioning like Network firewall (Maxon, 2000).

Network Firewall Architecture

Network Firewall architecture demonstrate how network firewall components are organized to deliver effective protection against users who are not authorised to access a network, network

firewall is normally defined after the network security policy has been defined because it is supposed to be a model that enforces the security policy (Wiley, 2004).

The network security policy is imposed at secure boundaries within the network called perimeter networks (Wiley, 2004).

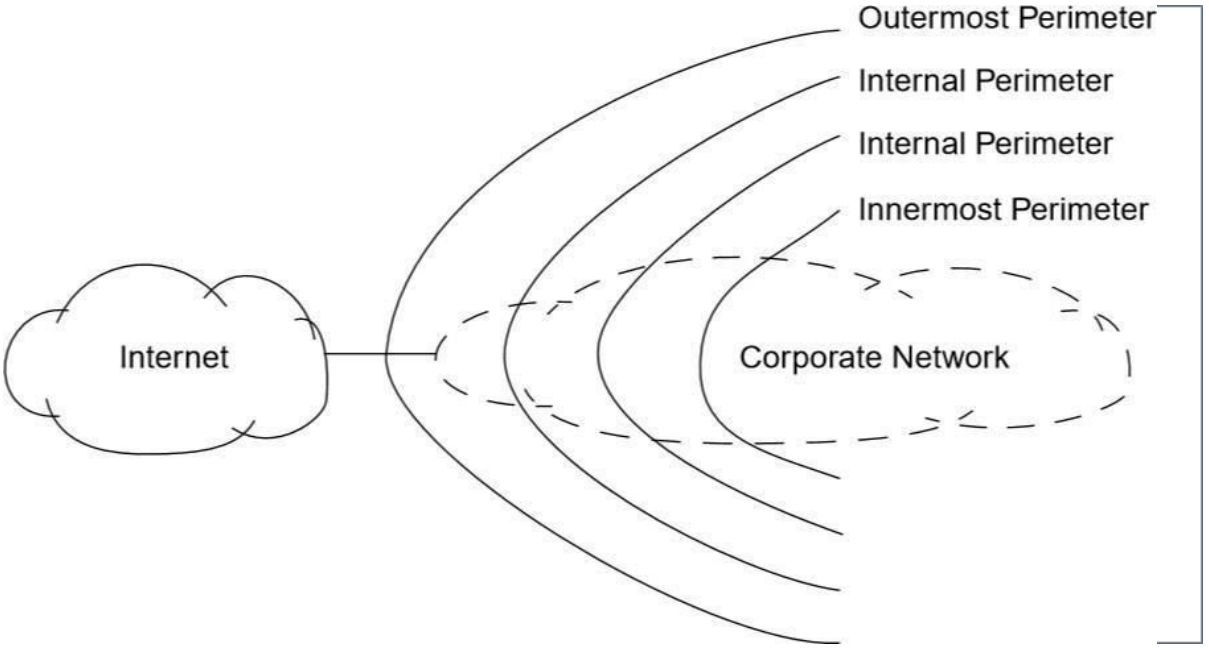


Fig.2:10 – Perimeter Network (Wiley, 2004)

In **Fig 2.10,** it demonstrates the possible firewall configuration, it shows that not all networks have three levels of perimeter networks. It is a neccesity to configure network firewalls to set network security policy or rules (Wiley, 2004). The architecture used in this Network firewall are:

- Screening Router
- Dual Home Gateway
- Screened Host Firewall
- Screened Subnet Firewall

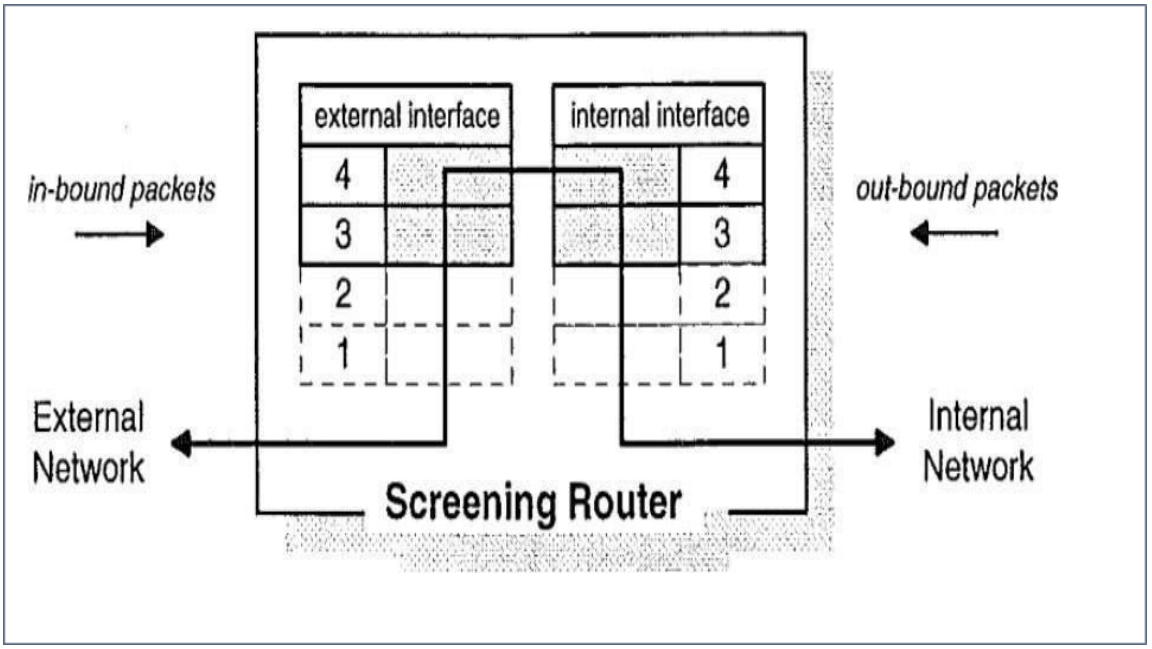
5.2 SCREENING ROUTER

A screening router is a basic element of firewall architectures and regularly consists of a commercial router. There are some cases routing can be host-based, normally on hosts using the UNIX operating system. Screening routers filter the datagrams passing between the network connections in accordance with a previously defined routing table. Filtering is normally performed on IP datagrams based on these following fields(Harris, 1998).

- Source IP address
- Dual-Homed Host Firewall
- Destination IP address
- TCP/UDP Source port

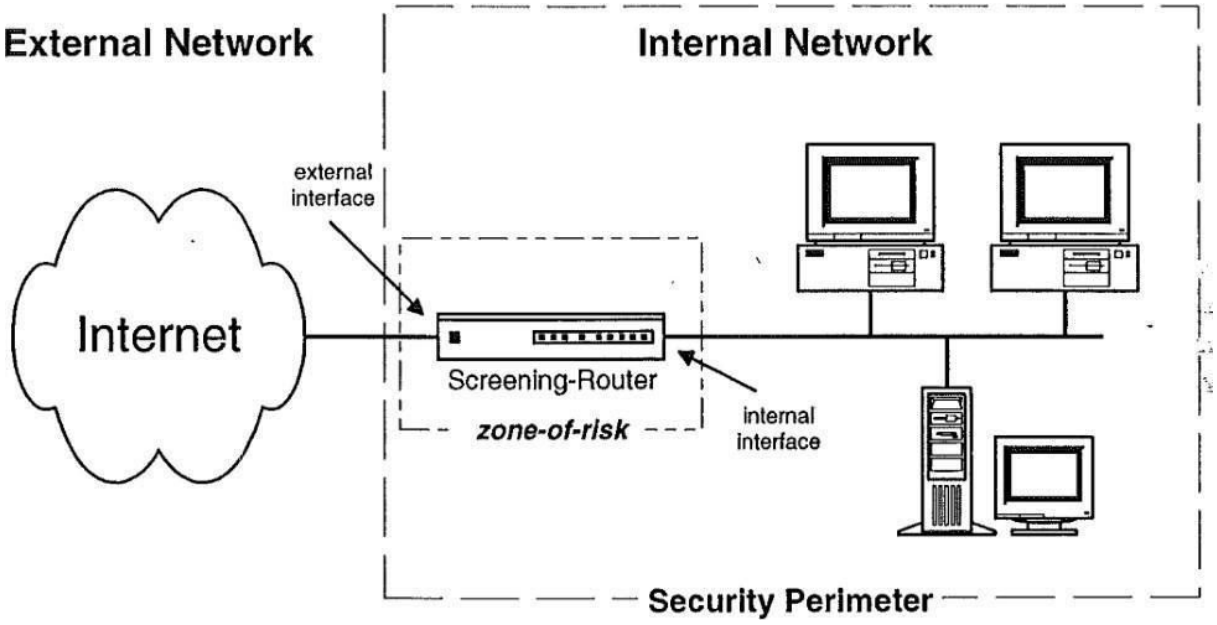
  TCP/UDP Destination port

Furthermore, some routers have the capability to differentiate which network interface a datagram arrives on and use this information to make decision how the router should be filtered. It is very useful when traffic needs to be segmented from the exact networks and in removing IP address spoofing. Datagram arriving at the external interface are known as inbound packets and datagrams arriving at the internal interface are known as outbound packets (Harris, 1998).



Screening Router functioning at the TCP/IP Model (Harris, 1998).

it demonstrates how the Screening Router operates in the TCP/IP model which is Network layer (Layer 3) and Transport (Layer 4). The grey color in boxes of the TCP/IP protocol stacks shows the layers on which the filtering rules largely operate. The flow of traffic is demonstrated by the double headed arrow as the flow of traffic passes between the internal and external interfaces (Harris, 1998).



Screening Router in firewall architecture (Harris, 1998).

In **Fig 2:12**, demonstrates the screen router based firewall architecture and distinguishing between the external and internal networks (Harris, 1998).

There is a straight communication paths between several hosts on the internal and external networks like the Internet. In a usual operation, the Zone of risk is visible and exposed to the number of hosts on the internal network and the number of peer-to-peer connections to the external network. The increase of hosts and connections make it very difficult to locate all the potential threat should be the Screen Router compromised (Harris, 1998).

The Screen router simply denies connections from to hosts or networks and also denies connections to exact ports. The capability of filtering on both UDP and TCP add an extra flexibility setting security policies (Harris, 1998).

Filter rules are usually implemented using a table of conditions and actions which are applied to each datagram until a deciding where to route or drop is reached. When the datagram has met all criteria stated in the row of the table, the action stated in that row of the table performs its duty, some systems apply the rules in a systematic manner from first to last. The rest impose an order based on the criteria in the rules, such as source and destination address (Harris, 1998).

A simple example of the screening-router, assume that University of Bedfordshire is breo.beds.ac.uk signified by the internal network shown in **Fig 2:12**, needs a mail connection to the University of Bedfordshire study.beds.ac.uk. A mail connection is regarded by a destination port number of 25, and a source port 2 $\geq$ 1024. The breo.beds.ac.uk mail connection is acknowledged by the 2 tuple "<IP number= 223.21.21.12, port 2 $\geq$ 1024>", however the study.beds.ac.uk mail gateway is acknowledged by the 2-tuple "<IP number= 192.15.18.5, port= 25>" (Harris, 1998).

The routing table requires to allow the type of connection as shown in **Table 2:4** (Harris, 1998).

CTIO N	OURCE IP ADDRE SS	ORT NUMBE R	D ESTINATIO N IP ADDRESS	OR T NU MB ER S	COMM TS
llo w	23.21.21. 12	1024	1 92.15.18.5	5	Connecti from breo.beds.ac.uk to study.beds.ac.uk mail gateway

llow	92.15.18.5	5	2 23.21.21.12	1 0 2 4	Allow replies from the ma gateway study.beds.ac.uk to breo.beds uk
eny			-		If none o the above rules matches deny access to all other datagrams.

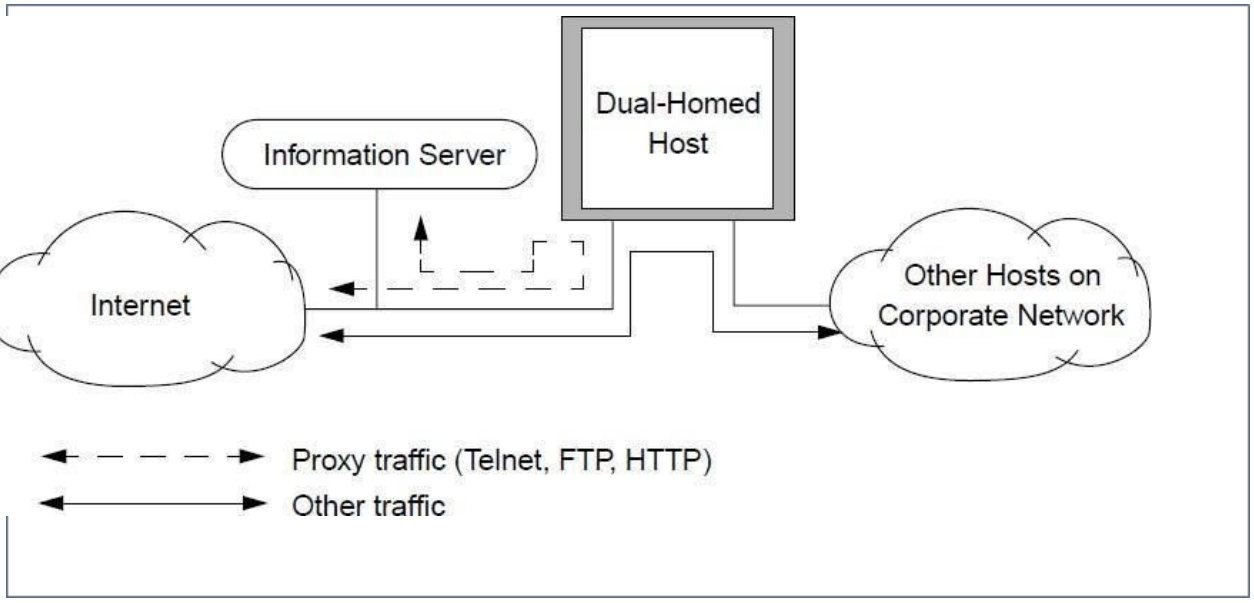
Table – Routing Table (Harris, 1998).

Dual-Homed Host Firewall

In the dual homed host firewall, the host usually have two interfaces, one of them is connected to the private network (Internal Network) and the other one is connected to the Internet where it can get untrusted network (External Network). It is a must that all IP traffics passes through the firewall before arriving at a host in the private network (Internal Network).

The same way an internal host communicates with external hosts in the internet through the dual homed host. Straight communication that bypass or avoid the dual homed host is denied. This is done to ensure that IP packets from one network will not be directly routed to the other network. The dual homed host do not function as a router.

However, restricting IP packet forwarding makes sure the Internet and the private network are reasonably disconnected so even when system problems occur the firewall cannot fail exposed. IP packet can only be allowed through the firewall is through its application proxies itself not through the operating system layer (Wiley, 2004).



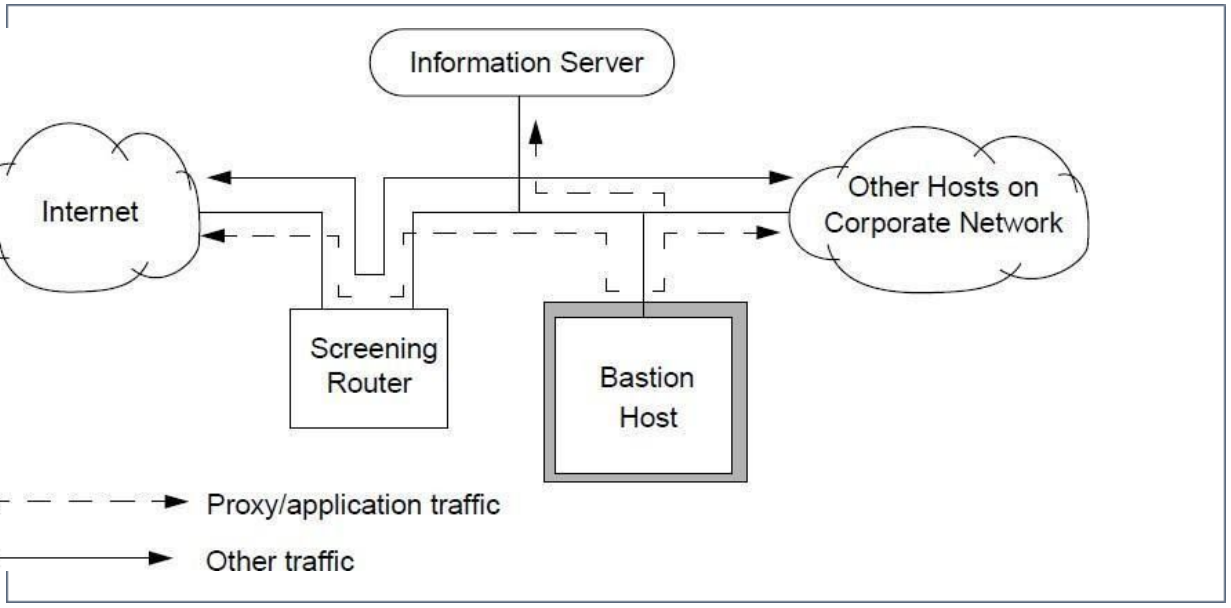
Dual Home Gateway Architecture (Wiley, 2004)**.**

The dual homed host blocks entries to the private network(Internal network) when it delivers proxy services like HTTP, FTP, the server offering the main service is placed between a packet filtering router and the dual-homed host which is present. This arrangement stops intruders from getting into the systems which securely protected by the dual-homed host (Wiley, 2004).

Screened Host Firewall

Screened Host firewall somehow differs from the dual-homed host firewall architecture, the dual home gateway permits the host firewall to be connected to two networks however the screened host firewall architecture rather permits the host providing the firewall to connect to the private network (Internal Network) only. A distinct screening router is located between the Internet and the host. The screened host firewall is a combined functionality of a packet filtering router and an application gateway (Wiley, 2004).

The screening router implements a packet filtering functionality and it configures which make the bastion host the only host in the private network (Internal Host) that can be examined from the Internet (External Network). Additional security can be implemented in the screening router by configuring it to decline traffic to exact ports on the bastion host as it shown in **Fig 2.14** the screening router is configured to accept or block connections between internal hosts and the Internet. The simplest 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.



Screen Host firewall Architecture (Wiley, 2004)**.**

Screened Subnet Firewall

The screened subnet firewall is described as an extension of the screened host firewall. Similarly like screened host firewall, it normally uses both a bastion host and screening router but this firewall which could also be referred as the Demilitarized Zone. This gives an additional layer of security by including a perimeter network that further separate the private network (Internal Network) from the Internet (External Network). The firewall determines a Demilitarized Zone demarcated by the outer router and an internal router (Wiley, 2004).

The internal router and the outer router has Demilitarized Zone which is an inner screened subnet bounded. The information server and bastion host are placed within the Demilitarized Zone, as shown in **Fig** The Demilitarized Zone is considered a separated network between the private network (Internal Network) and the Internet (External Network). The outer router prevents the network from external attacks by blocking entry to systems in the Demilitarized Zone (Wiley, 2004).

It also declines traffic to the external network from unauthorized sources in the internal network. The internal router controls Demilitarized Zone access to the internal network by passing traffic from the bastion host to the hosts in the internal network that are not in the Demilitarized Zone. Enable for an attack to get to any internal host placed outside the Demilitarized Zone, it must break through both routers (Wiley, 2004).

This architecture discloses only the Demilitarized Zone network to the outside

world and retains the private network hidden (Wiley, 2004). Since application layer firewall deals with web traffic protocols such as HTTP. Web application firewall has been implemented to take responsbile for web traffic such as HTTP, HTTPS traffic and HTML and prevent any web based attacks to the network.

WEB APPLICATION FIREWALL

There are many Web applications of all kinds, some are in form of online shops or partner portals, attackers try any possible means to gain access or steal information for financial gain. The attackers use different methods which are mainly aimed at exploiting potential weak spots in the web application. Network layer firewall are not capable of detecting web based attacks on web application (Maximilian Dermann, 2008).

Implementing web application firewall enhance extra layer of security since Web Application Firewalls protects web applications from web-based attacks, Web application firewalls examines HTTP traffic which comes in and out of web applications. The most significant problem of web application is SQL Injection. However the solution to this problem is to implement web application firewall. (Maximilian Dermann, 2008)

Web Application Firewall Architecture

There are different type of web application deployment and operating mode depending on the security of policies. This project will elaborate on the most significant deployment and operating mode of Web Application Firewall Architecture.

Appliance-based Web Application Firewall

Appliance-based Web application deployments stand behind the firewall and in front of organizational web servers (Beechey, 2009). Application-based Web Application are normally installed closest to the application and sometimes joined into the application code itself.

One of the example of Appliance based Web Application firewall used in this project to protect from web based attacks is ModSecurity, which normally installed as a module in Apache. An application can benefit of the features permitting the overhead to be held by the local server. The cost of deploying an application-based Web application firewall is usually low. (TechTarget, Introduction to Web application firewalls in the enterprise, 2000-2016)

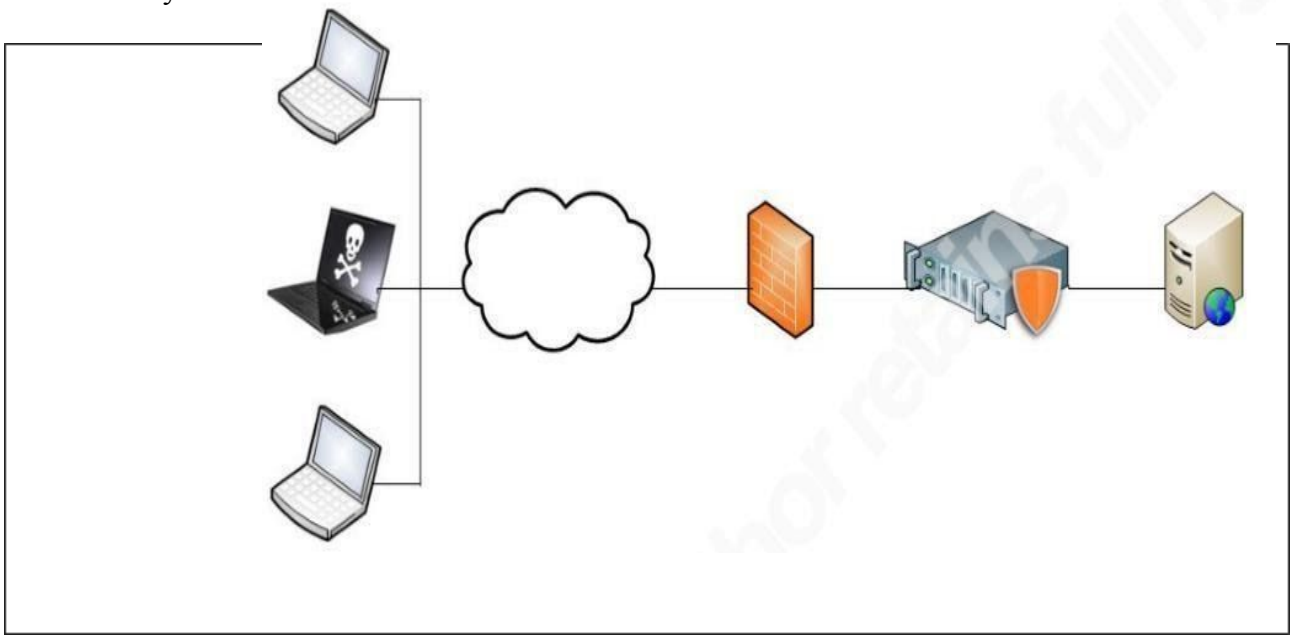
Operating Mode in Web Application Firewall Architecture

The Important operating modes Web Application Firewall are:

- Reverse Proxy
- Layer 2 Bridge
- Network Monitor/Out of Band
- Host/Server Based
- Internet Hosted/Cloud (**New**)

Reverse Proxy

In this mode, the Web application firewall has an IP address and stands inline. Any incoming connection to the application is forwarded to the web application firewall which makes a distinct request to the web server. Encrypted connections are ended at Application Layer allowing the web application firewall decrypt and examine the web traffic. **Fig 2:2** illustrates the architecture of the Web Application firewall and the position of the Reverse Proxy Serve



server. (Pubal, 2015)

Reverse Proxy Mode (Pubal, 2015)

Layer 2 Bridge

In this mode, the Web application firewall stands inline and performs as a Switch (Layer 2). The Web application firewall does passive SSL decryption, and is capable of blocking traffic by simply dropping the harmful packets. This permits for higher performance than reverse proxy with much less network changes (Pubal, 2015) but it does not offer an advanced services like other Web application firewall modes may offer.

Network Monitor/Out of Band

In this mode, the Web application firewall is not inline. It receives a copy of the traffic through the identifying port. It can inactively decrypt SSL traffic. The Web application firewall's ability to block traffic is quite limited, it only sends TCP-reset packets to interfere traffic. This mode has the minimum amount of effect on the network

and application. It allows the Web application firewall to be configured to only alert on malicious traffic removing the danger of blocking false-positive detection and causing application (Pubal, 2015). The architecture shown in **Fig.** demonstrate how the web application firewall standing as a switch and examines the traffic by receiving a copy of traffic passing to the web server. (Pubal, 2015)

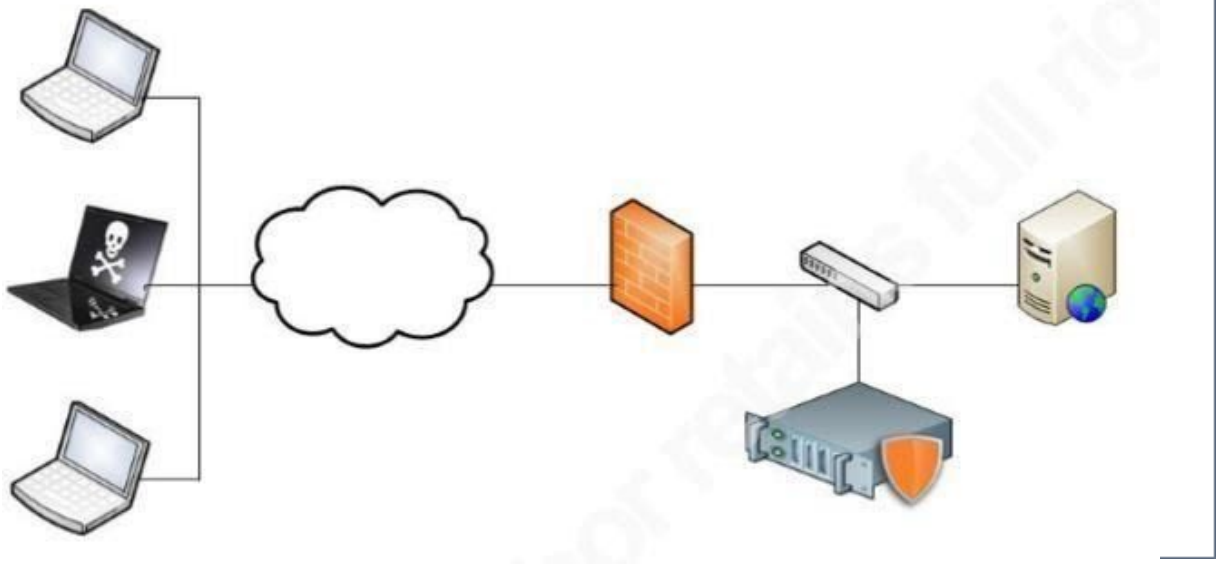


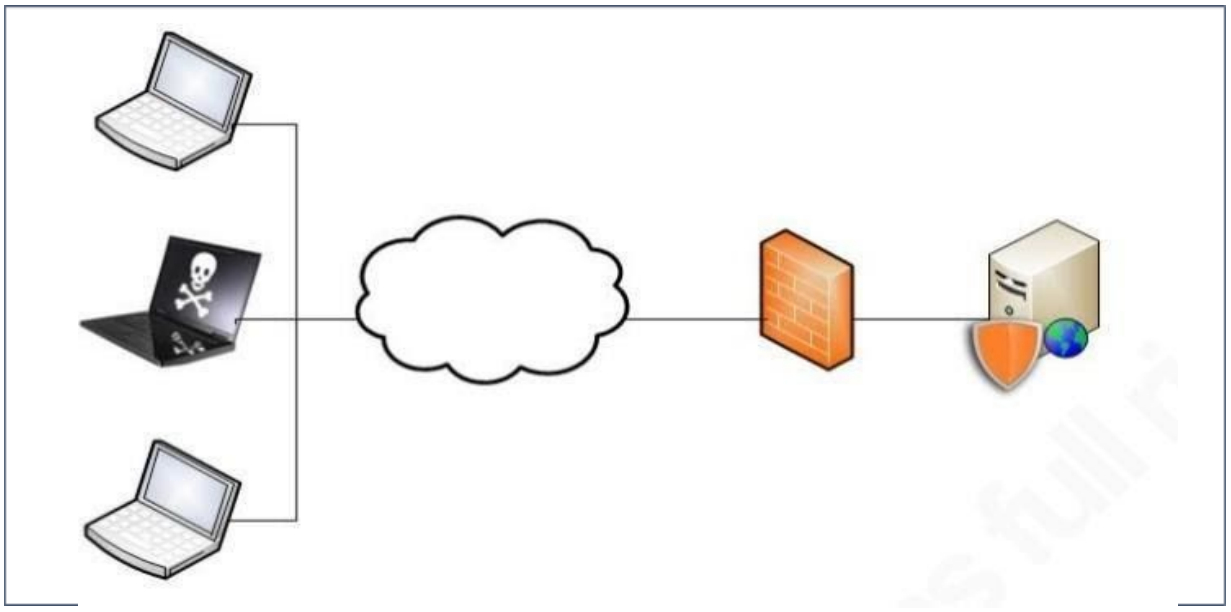
Fig. - Out of Band Mode (Pubal, 2015).

Host/Server Based

A server based web application firewall is a software application implemented and installed on the web server. It is usually installed as an independent application or a web server plug-in. It puts additional load on the server.

The architecture shown in **Fig.** demonstrates how the web application firewall functions as a software on the web server which represented as shield. (Pubal, 2015)

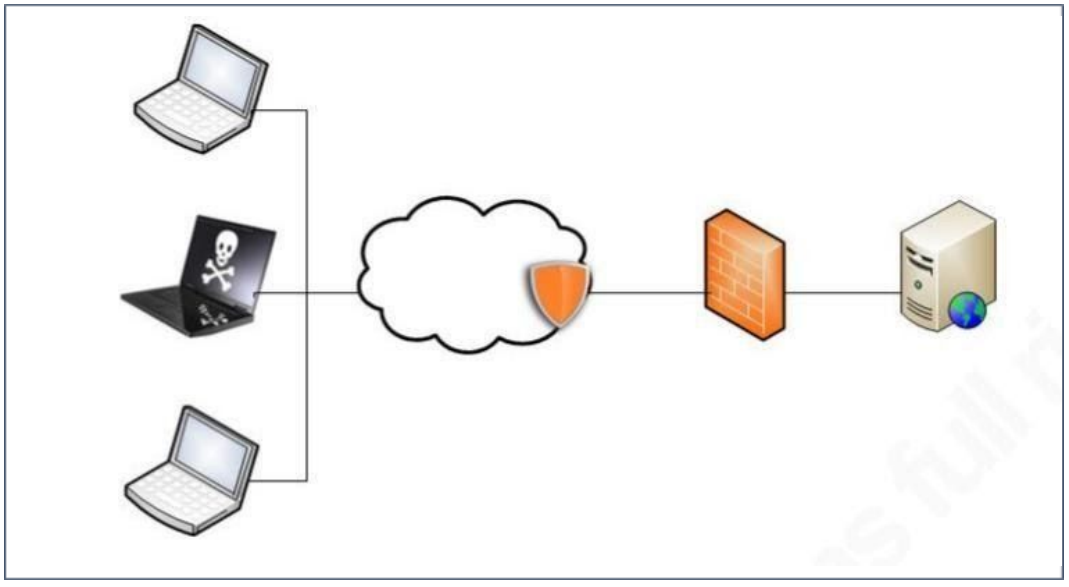
– Host/Server Based Mode (Pubal, 2015)



Internet Hosted/Cloud (New)

This is a new Web Application firewall mode which the cloud provider implement web application firewall solutions. It is not widely used today but Gartner one of the world leading information technology and advisory company has predicted that more than 50% of public web application will be protected by Internet Hosted/Cloud web application firewall in 2020. It has been proved that less than 10% of public use internet hosted/cloud web application firewall today. This newly mode works more like reverse proxy, public DNS will be configured to point the cloud service, this will then establish another connection to the web application property (Pubal, 2015).

The architecture shown in **Fig.** demonstrates how the web application firewall represented as a shield in the cloud functions as a software as a service.



Benefit of Network Layer Firewall

The benefit of Network layer firewall are:

1) Network Firewalls can focus extended logging of network traffic on one system (Smith, 2009).
2) Network Firewalls filters protocols that are not needed to ensure it is secured from exploitation (Smith, 2009).
3) Network Firewalls do not reveal the names of the internal system which makes information become less available to the outside host (Smith, 2009).

Network Firewalls are normally quicker than other firewall technologies because Network firewall performs very less evaluation.

. Limits of the Usefulness of Network Layer Firewall (Packet Filtering):

In cases where a packet filter restricts access to a resource based on the source IP address attempting to access that resource, the packet filter cannot verify whether the packets originate from the real device or from a host or router spoofing this source address. A transparent proxy illustrates this problem perfectly. A transparent proxy frequently runs on a masquerading or NAT host which is connected to the Internet. This machine intercepts outbound connections for a particular protocol (e.g, HTTP), and simulates the real server to the client. The client may have a packet filter limiting outbound connections to a single IP and port pair, but the transparent proxy will still operate on the outbound connection.

This is an innocuous example, indeed. A potentially more threatening example is an ssh server which accepts connections only from an IP range. Any router between the two endpoints which can spoof IP packets will be able to pass the packet filter, whether it is a stateful or a static packet filter. This should underscore the importance of solid application layer security in addition to the need for judiciously employed packet filtering.

A packet filter makes no effort to validate the contents of a data stream, so data passed over a packet filter may be bogus, invalid or otherwise incorrect. The packet filter only verifies that the network layer datagrams are correctly addressed and well-formed [35]. Many security devices, such as firewalls, include support for proxies, which are application aware. These are security mechanisms which can validate data streams. Proxies are often integrated with packet filters for a tight network layer and application layer firewall.

Tunnels are one of the most common ways to subvert a packet filter. They come in wide varieties: ssh tunnels which allow users to transport TCP sessions into or out of a network; GRE tunnels, which allow arbitrary packets to be encapsulated in an IP packet; UDP tunnels; VPN tunnels; TAP/TUN tunnels; and application layer transport tunnels, such as RPC over HTTP/HTTPS. Some of these tunnels are very difficult to prevent with packet filtering, while others are trivial to block.

8 BENEFITS OF WEB APPLICATION FIREWALL

A WAF proactively protects websites and applications against fraud or data theft; blocking any suspicious activity. Inspecting every web request for cross-site scripting, SQL injection, path traversal and 400+ other types of attack, this protection ensures that your data, and your customer's data, remains secure.

WAFs Protect against:

- SQL injection, comment spam
- Cross-site scripting (XSS)
- Distributed denial of service (DDoS) attacks
- Application-specific attacks (WordPress, CoreCommerce) and many more
- OWASP top 10

Other benefits include:

- Automatic protection from diverse threats, with strong default rule sets and extensive customization providing Layer 7 protection that is fully integrated with DDoS mitigation
- Real-time reporting and robust logging lets you see what's happening instantly

Automated Patches

It's a good idea to be running vulnerability scans regularly. Ideally, if you are an ecommerce business you would be running scans once a quarter or several times a month. Consider what you might happen if you discover a vulnerability in your website or application; you might have the resources to patch the application or fix the problem quickly, but most businesses won't have the expertise or skill immediately available. If your company falls into the second group, then your company is at risk as long as that vulnerability is present. Some WAFs have the ability to use your scan findings to temporarily patch your application for immediate protection. This temporary patch isn't a full solution, but it's enough to mitigate risk until you've prepared a permanent fix.

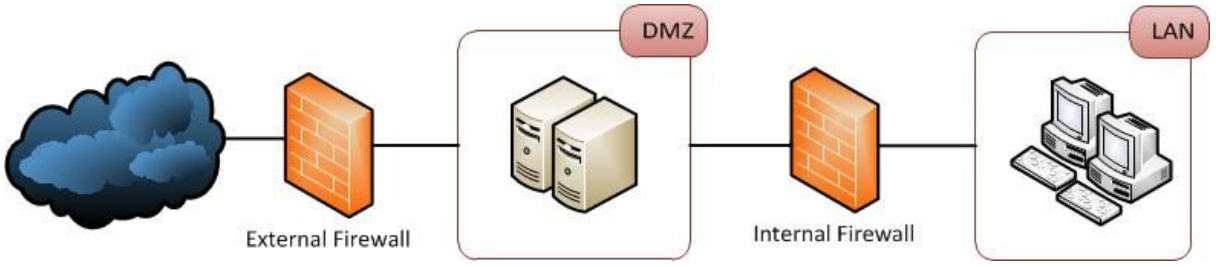
Stops Data Leakage

Hackers can gather data in a myriad of ways. Unless you know you've been compromised, detecting them can be tricky. Data leakage can be caused by something as insignificant as a malicious error message presented to a user, so if your application is harbouring critical data, such as source code or credit card numbers, then it's very easy to become subject to a leak. And any kind of leak can turn into a disaster. A WAF would scan every request to your Web application users, and if something appears unusual, the WAF stops it from leaving your network. Most WAF's have high-level behavioural signatures looking for credit card numbers and social security numbers already built-in. But you can customise, and add any additional signatures, such as specific files, information or code.

Cloud based WAF's

To provide more extensive website protection, WAFs are deployed in the cloud or in corporate Demilitarized Zones (DMZs). They can perform SSL termination to conduct deep inspection of applications traffic at layer 7. The WAFs go beyond matching signatures, analyzing application behavior and detecting deviations from baselines of acceptable behavior.

Cloud-based WAFs in an IaaS deployment can be deployed as a software appliance or virtual machine. The WAF can also be deployed as an extension of an existing CDN, providing WAF-as-a-Service, with no need to deploy hardware or software.



This service is typically set up by changing your DNS records to point to WAF cloud services, which will in turn proxy back to your actual web properties.

Limitations of web application firewalls

when a WAF inspects traffic, they have only limited contextual information to work with as they only see one raw packet at a time. This individual packet won't mean a lot from an inspection perspective. Does it have any bearing on the previous one? Is it related to the one afterward?

What's more, when analyzing packets WAFs use a set of patterns to analyze incoming packets against. Depending on their configuration WAFs can either be overly permissive or worse, overly protective, generating false positives or false negatives.

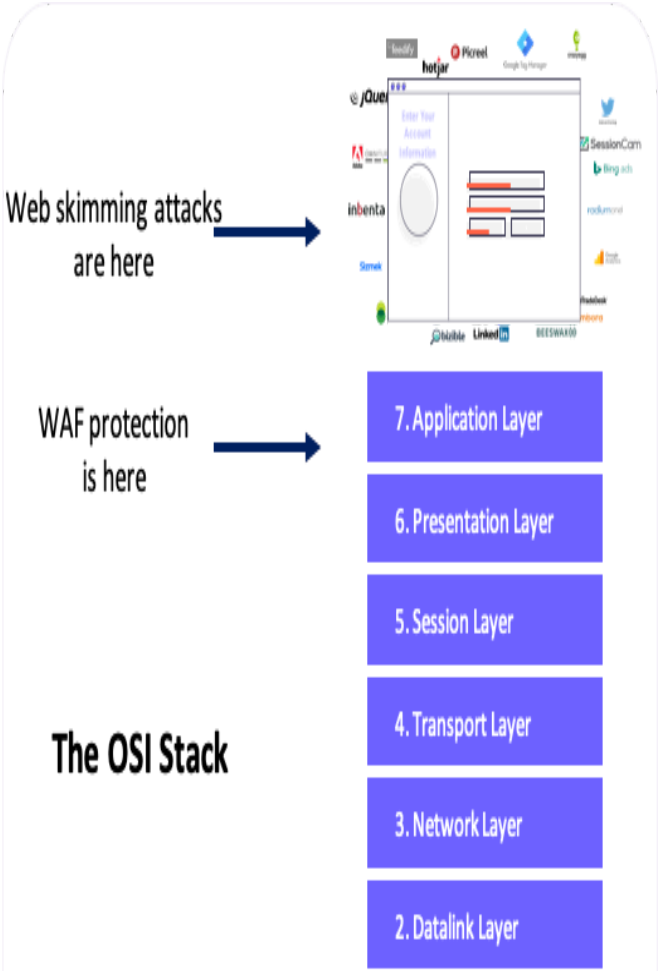
Consequently, using WAFs for application protection can be a rather brute-force — or *blunt* — approach. What's more, they are hard to configure, unless you're a security or networking expert, something not many software developers are. Then, in addition, firewall configurations need to be maintained. It's not a set-and-forget affair.

But, they have the potential to block up to 62% of current attack vectors, such as SQL injection, Cross-Site Scripting (XSS), and Cross-site Request Forgery (CSRF).

WAF is an OSI layer 7 defense mechanism against attacks known as application-layer attacks, and it protects services that user-facing web applications use to present data. WAF is not protecting browser-level user interface itself. If a web application and its user experience is a house, then WAF protects walls, not the furniture or electronics inside.

Drive-by skimming

Steals data of hundreds of websites in one hit



Sideloading

WAF does not protect against skimming performed by a sideloaded JavaScript code.

Third-party JavaScript code

Attackers load skimming code on target web pages using legitimate scripts and tools

Multi-stage attacks

Skimming code uses anti-forensics or loads only on target web pages

Supply chain attacks

It's often a lot easier to add skimming code to a third-party JavaScript code because it's not part of internal security oversight. Additionally, attacking third-party tools allows hackers to penetrate almost all the customers of the target third-party. This type of attack is commonly called "drive-by skimming."

Protocol attacks

A protocol attack focuses on damaging connection tables in network areas that deal directly with verifying connections. By sending successively slow pings, deliberately malformed pings, and partial packets, the attacking computer can cause memory buffers in the target to overload and potentially crash the system. A protocol attack can also target firewalls. This is why a firewall alone will not stop denial of service attacks.

One of the most common protocol attacks is the SYN flood, which makes use of the three-way handshake process for establishing a TCP/IP connection. Typically, the client sends a SYN (synchronize) packet, receives a SYN-ACK (synchronize-acknowledge), and sends an ACK in return before establishing a connection. During an attack, the client only sends SYN packets, causing the server to send a SYN-ACK and wait for the final phase that never occurs. This, in turn, ties up network resources.

Can Easily Be Bypassed

Now what about being able to bypass the protection which a WAF offers? Remember, that most WAFs use software, which in turn may have vulnerabilities, which can be abused. WAFs commonly do what’s referred to as fail open or fail close in the event of too much traffic.

A fail open is where the WAF reverts to monitoring only, or less, effectively letting all traffic through. A fail close is the opposite. All traffic is blocked. In either case, either by implementing a DoS or a DDoS attack, you could break through the WAF, or cause it to prevent access to the application entirely.

9 Firewall attack mitigation techniques

9.1 Conserve Resources in Use, While Maximizing Available Ones

During an attack, these filters work by passing traffic intended for a target through high-capacity servers and networks to filter out the “bad” traffic.

Types of filtering that support DDoS mitigation include:

- connection tracking;
- IP reputation lists;
- deep packet inspection;
- blacklisting/whitelisting; and
- rate limiting.

Separate the firewall from the router, so there is no single point of attack. Beef up firewalls and routers with compute power and memory where possible also helps. You can turn off logging (for example, on consumer routers and equipment) so that log writes do not eat up resources when traffic accelerates during an attack. As mentioned before, setting up a Response Rate Limiter (RRL) will limit how many responses servers will send to requests. RRLs will also stop/block zombie computers that keep requesting data without acknowledgment requests. This functionality is particularly useful during spoofing attacks.

Another step involves placing an on-premise filtering device in front of the network. However, it’s recommended that DDoS mitigation not rely on on-premise solutions alone, precisely because these limit capacity. Homespun and on-premise anti-DDoS measures work best alongside anti-DDoS emergency response providers like Arbor Networks, Akamai, CloudFlare, or Radware and/or services from cloud providers like Verisign and Voxility.

9.2 Ramp Up the Defenses

Finally, there are some general steps you can take to be ready for an attack before it happens. We’ll summarize below.

- Configure your data center to shut a connection and reboot after an attack.
- “Change the “TTL” or “Time to Live” to 1 hour. You’ll need to redirect your site once it comes under attack; (the default is three days).

- Make sure you've got backups, and where possible, a means to create offline copies.
- Stay up to date on security and software updates with any Content Management System (CMS) you may be using.
- Monitor your site's availability with a service like UptimeRobot, Pingdom, or Monitis to check your it periodically and alert you (via SMS or email) if your site goes down.

9.3 If You've Been Infected—and Become a Bot:

- Reinstall your machine or restore your VM from a safe snapshot. Make sure to reinstall your anti-virus and anti-malware and do a full scan.
- Change your passwords.
- Change your habits. Be wary of all the possible vectors for malware, including:
  - dodgy email attachments;
  - risky websites;
  - download sites and networks like TOR—to name a few.
- If you must browse to a download site, or something with content that could be risky, install a virtual machine—and browse from there.
- If you're downloading something from even "reputable" sites like CNet or Downloads.com, don't trust anything implicitly. Make sure you scan everything you download.

10. Security requirement with firewall analysis

❖ The firewall must employ filters that prevent or limit the effects of all types of commonly known denial-of-service (DoS) attacks, including flooding, packet sweeps, and unauthorized port scanning.

Not configuring a key boundary security protection device such as the firewall against commonly known attacks is an immediate threat to the protected enclave because they are easily implemented by those with little skill. Directions for the attack are obtainable on the Internet and in hacker groups.

❖ The firewall must deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).To prevent malicious or accidental leakage of traffic, organizations must implement a deny-by-default security posture at the network perimeter. Such rulesets prevent many malicious exploits or accidental leakage by restricting the

traffic to only known sources and only those ports, protocols, or services that are permitted and operationally necessary.

- The firewall must be configured to use filters that use packet headers and packet attributes, including source and destination IP addresses and ports, to prevent the flow of unauthorized or suspicious traffic between interconnected networks with different security policies (including perimeter firewalls and server VLANs).

- The firewall must generate traffic log entries containing information to establish the outcome of the events, such as, at a minimum, the success or failure of the application of the firewall rule.

Without information about the outcome of events, security personnel cannot make an accurate assessment as to whether an attack was successful or if changes were made to the security state of the network.

- The firewall must immediately use updates made to policy enforcement mechanisms such as firewall rules, security policies, and security zones.Information flow policies regarding dynamic information flow control include, for example, allowing or disallowing information flows based on changes to the Ports, Protocols, Services Management [PPSM] Category Assurance Levels [CAL] list, vulnerability assessments, or mission conditions. Changing conditions include changes in the threat environment and detection of potentially harmful or adverse events.

12 Firewall deployment with application level control

12.1 A DEFINITION OF APPLICATION CONTROL

Application control is a security practice that blocks or restricts unauthorized applications from executing in ways that put data at risk. The control functions vary based on the business purpose of the specific application, but the main objective is to help ensure the privacy and security of data used by and transmitted between applications.

Application control includes completeness and validity checks, identification, authentication, authorization, input controls, and forensic controls, among others.

- Completeness checks – controls ensure records processing from initiation to completion
- Validity checks – controls ensure only valid data is input or processed
- Identification – controls ensure unique, irrefutable identification of all users
- Authentication – controls provide an application system authentication mechanism
- Authorization – controls ensure access to the application system by approved business users only
- Input controls – controls ensure data integrity feeds into the application system from upstream sources
- Forensic controls – controls ensure scientifically and mathematically correct data, based on inputs and outputs

Simply put, application controls ensure proper coverage and the confidentiality, integrity, and availability of the application and its associated data. With the proper application controls, businesses and organizations greatly reduce the risks and threats associated with application usage because applications are prevented from executing if they put the network or sensitive data at risk.

12.2 FEATURES AND BENEFITS OF APPLICATION CONTROL

Companies have grown increasingly dependent upon applications in day-to-day business operations. With web-based, cloud-based, and third-party applications at the core of today's business processes, companies are faced with the challenge of monitoring and controlling data security threats while operating efficiently and productively. Most

application control solutions include whitelisting and blacklisting capabilities to show organizations which applications to trust and allow to execute and which to stop. With application control, companies of all sizes can eliminate the risks posed by malicious, illegal, and unauthorized software and network access.

KEY FEATURES AND BENEFITS OF APPLICATION CONTROL:

- Identify and control which applications are in your IT environment and which to add to the IT environment
- Automatically identify trusted software that has authorization to run
- Prevent all other, unauthorized applications from executing – they may be malicious, untrusted, or simply unwanted
- Eliminate unknown and unwanted applications in your network to reduce IT complexity and application risk
- Reduce the risks and costs associated with malware
- Improve your overall network stability
- Identify all applications running within the endpoint environment
- Protect against exploits of unpatched OS and third-party application vulnerabilities

A BETTER UNDERSTANDING OF DATA ENVIRONMENTS WITH APPLICATION CONTROL

Most application control solutions also allow for visibility into applications, users, and content. This is helpful for understanding the data your enterprise owns and controls, its storage locations, which users have access to it, the access points, and the data transmission process. These steps are required for data discovery and classification for risk management and regulatory compliance. Application control supports these processes and allows organizations to keep their finger on the pulse of what is happening within their network.

Application control gives companies and organizations knowledge about key areas regarding applications, web traffic, threats, and data patterns. Users can also benefit from application control by gaining a better understanding of applications or threats, applications' key features and behavioral characteristics, details on who uses an application, and details on those affected by a threat. Organizations also gain knowledge about traffic source and destination, security rules, and zones to get a complete picture of application usage patterns, which in turn allows them to make more informed decisions on how to secure applications and identify risky behavior. While they are making those decisions, the application control solution is automatically protecting the network with whitelisting and blocking capabilities.

12.3 Deploy Web Application Firewalls

Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

Asset Type	Security Function	Implementation Groups
N/A	N/A	2, 3

Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

Inputs

1. The inventory of authorized software

Operations

1. Enumerate all in-house owned and operated software (i.e. applications in the software inventory that are developed in-house and/or acquired) for which there is an application-level firewall technology exists
2. Enumerate all application-level firewalls (including WAF and host-based firewalls)
3. For each application-level firewall, enumerate covered software applications
4. Complement the set of software applications identified in the first operation with the covered software applications

Measures

- M1 = Enumerated list of all software in the inventory for which an application-level firewall technology exists
- M2 = Enumerated list of all application-level firewalls
- M3 = Enumerated list of applications covered by application-level firewalls
- M4 = Enumerated list of applications not covered by software applications (fourth operation)
- M5 = Count of software for which an application-level firewall technology exists (count of M1)
- M6 = Count of application-level firewalls (count of M2)
- M7 = Count of applications covered by application-level firewalls (count of M3)
- M8 = Count of applications not covered by software applications (count of M4)

Metrics
Coverage

Metric	The ratio of the number of applications covered by an application-level firewall to the number of eligible applications in the enterprise.
Calculation	M7 / M5

13 Firewall deployment with comprehensive server security

INTRODUCTION Virtualization is the dominant technology employed in enterprise data centers and those used for offering cloud computing services. This technology has resulted in what is called a virtualized infrastructure. From a computing and communication point of view, the two forms of virtualization that have made significant impacts are Server (or Hardware) virtualization and Operating System (OS) virtualization. Server virtualization is enabled by software called a Hypervisor —functionally, an operating system kernel with some additional kernel modules that provides an abstraction of the hardware, enabling multiple independent computing stacks called virtual machines (VMs), each with its own OS and applications, to be run on a single physical host. While access to CPU and memory (to ensure process isolation) are handled directly by the hypervisor (through instruction set (CPU) virtualization and memory virtualization respectively with or without assistance from hardware), it handles the mediation of access to devices by calling on software modules running either in the kernel or in dedicated VMs called Device-driver VMs. This physical host is called a virtualized server or hypervisor host.

13.1. VIRTUALIZED SERVER ENVIRONMENT – A TECHNOLOGY OVERVIEW From the perspective of this manuscript, a virtualized server environment consists of the following components: • A physical host, called a virtualized server or hypervisor host, with server virtualization software (hypervisor and its associated modules), along with multiple computing stacks (i.e., Virtual Machines or VMs) running on it. The hypervisor host has hardware extensions to assist virtualization. • A virtual network, or software-defined network, inside the virtualized server, consisting of softwaredefined network devices. This network is configured with network segmentation techniques such as Virtual Local Area Network (VLAN) and overlay-based network (e.g., VXLAN) that span multiple virtualized servers and enable logical segmentation of the VMs distributed throughout the data center.

13.2 VIRTUALIZED SERVER HARDWARE FUNCTIONS As already stated, the hardware of a virtualized server provides two features to assist the virtualization function of the hypervisor: Instruction Set Virtualization and Memory Virtualization. These hardwarebased functions provided by chip vendors are mature technologies that have been utilized for more than a decade and whose known vulnerabilities have already been addressed. Therefore, no threats need to be considered for these functions.

Table 1: Hypervisor Baseline Functions & Deployment Locations

Baseline Function	Component (Software Module)	Location
VM Process Isolation (HY-BF1)	Hypervisor Kernel	Either an OS kernel (along with a kernel module) itself or a component installed on a full-fledged OS (Host OS)
Devices Mediation & Access Control (HY-BF2)	Device emulator or Device driver	Either in a dedicated VM (called Device-driver VM) or in the hypervisor kernel itself
Execution of Guest Instructions through hypercall interface (HY-BF3)	Hypervisor Kernel	Pertain to only para-virtualized hypervisors and handled by hypercall interfaces in that type of hypervisor
VM Lifecycle Management (HY-BF4)	A management daemon	Installed on top of the hypervisor kernel but runs in unprivileged mode
Management of Hypervisor (HY-BF5)	A set of tools with CLI (command line interface) or a GUI	A console or shell running on top of the hypervisor kernel

13.3. PROTECTION FOR VIRTUAL NETWORK CONFIGURATIONS To link the VMs inside a hypervisor host to each other and to the outside (physical) enterprise network, the hypervisor can define an entirely software-defined network called a virtual network. The components of this virtual network are: (a) one or more software-defined network interface cards, called virtual network interface cards (vNICs), inside each VM and (b) multiple software-defined switches, called virtual switches, operating inside the kernel of the hypervisor.

There are four common virtual network configuration areas that have a bearing on the security of the network infrastructure in a virtualized server environment [5]

- Network segmentation
- Network path redundancy
- Firewall deployment and configuration
- VM traffic monitoring

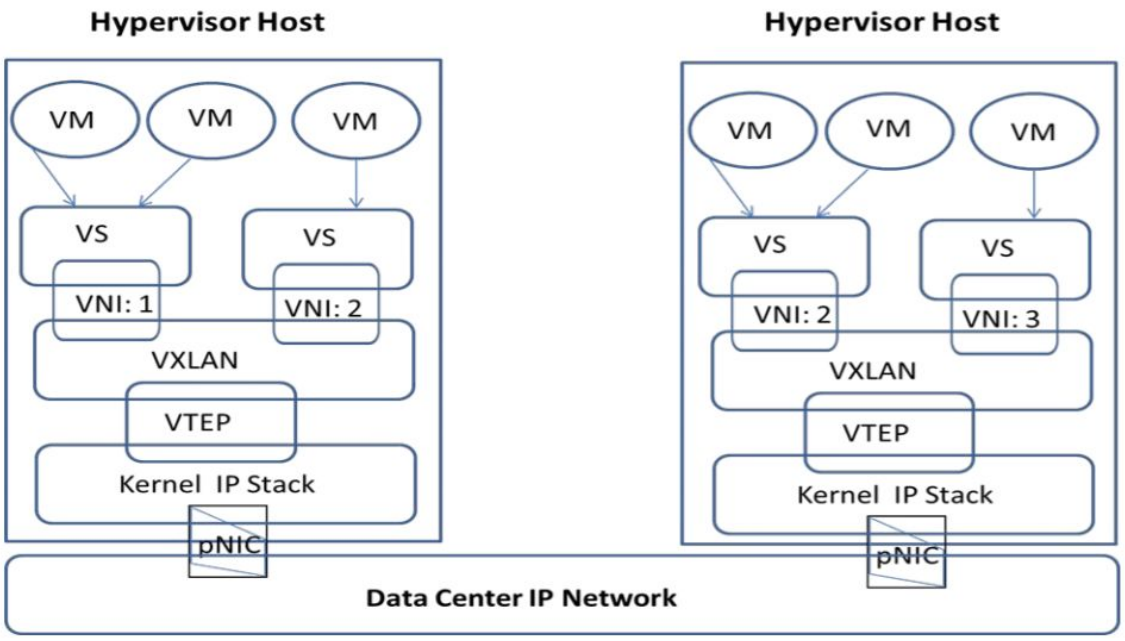


Figure 3: Virtual Network Segmentation using Overlays (VXLAN)

SECURITY ASSURANCE FOR HYPERVISOR BASELINE FUNCTIONS

Security Assurance for VM Process Isolation (HY-BF1)

To ensure the isolation of processes running in VMs, the following requirements must be met [1]:

(a) The privileged commands or instructions from a Guest OS to the host processor must be mediated such that the core function of the VMM/hypervisor as the controller of virtualized resources is maintained.

(b) The integrity of the memory management function of the hypervisor host must be protected against attacks such as buffer overflows and illegal code execution, especially in the presence of translation tables

(e.g., host page table) that are needed for managing memory access by multiple VMs.

(c) Memory allocation algorithms must ensure that payloads in all VMs are able to perform their functions.

(d) CPU/GPU allocation algorithms must ensure that payloads in all VMs are able to perform their functions

14. BENEFITS OF COMBINATION

Server or Hardware virtualization is an established technology in data centers used for supporting enterprise IT resources as well as cloud services. The core entity in this technology is a set of software modules called the hypervisor. The hypervisor provides

abstraction of the hardware resources, such as CPU, memory, and devices (the first two with some assistance with hardware extensions), and enables the running of multiple computing stacks called VMs, each with its own OS and applications, to be run on a single physical host. Such a physical host is called a hypervisor host or virtualized server. The network linking the multiple VMs within a hypervisor and with VMs located in other hypervisor hosts is a combination of a software-defined network (called virtual network) and the physical network infrastructure and constitutes the virtualized server environment.

The threats were then used as the basis for developing appropriate security assurance measures for countering each threat.

CONCLUSION/INFERENCE

As the Internet becomes more a part of business, firewalls are becoming an important ingredient of an overall network security policy. More and more people try to break in illegally and access secured data. Thus, an extensive knowledge of firewalls is needed in the industry. We have seen that there are several approaches to integrating a firewall into a network topology. The exact nature of rules and restrictions a firewall must allow is based on the level of security and freedom required.There are many possible criteria upon which decisions are made regarding whether to implement a firewall.

In this project, we tried to study and analyse the various aspects about firewalls, most notably Network Layer Firewalls and Web Application Firewalls, and their roles in preventing and securing a network from Network and Web-based attacks. We also saw various different types of Network layer attacks as well as Web Application based attacks that are possible(IP Spoofing Attack, DOS_Denial of Service Attack, Packet sniffer, Man-in-the-Middle Attack, Phishing, etc.) and how they access, manipulate and corrupt our data illegally. We tested different versions and settings in which we tried to protect and secure our network from attacks. Using these test runs and settings, we conducted a thorough functionality analysis of the firewalls. Moreover, we noted the benefits and limitations of each firewall type, giving us further insight into the depths and details of the applicability of firewalls. Mitigation techniques and security requirements were tested out. Deployment of the firewalls was tested out in required software for a hands-on experience. The deployment was carried out for different types of networks to further understand the application diversity of firewalls. However, due to restrictions in time and budget, all the deployments could not be carried out, mostly, because of lack of friendly, open-source softwares.

The firewall market is still relatively young and there are an abundance of choices (approximately 40 vendors currently offer products), so it is expected that as the market matures, the products that are successful are those that excel in these areas.

REFERENCE

1) Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". Communications of the ACM 40 (5): 94.

2) http://www.wanredundancy.org/resources/firewall/network-layer-firewall

3) http://www.tech-faq.com/firewall.html

4) http://en.wikipedia.org/wiki/Firewall_%28computing%29

5) https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

6) Google Cloud Platform (https://www.qwiklabs.com)

7) https://www.barracuda.com/glossary/network-firewall

8) https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/