Comparative Analysis of Web application and Network layer firewalls

Supervisor: Dr. B. Hariharan

Assistant Professor

Dept.of Computational Intelligence

SRMIST, Kattankuthur

COURSE PROJECT BY

Hasan Kamran (RA2011033010059)

Anubhav Vats (RA2011033010062)

Gaurav Raj (RA2011033010063)

Rimendra Ku. Agrawal(RA2011033010064)

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this project report " **Comparative Analysis of Web application and Network layer firewalls**" is the bonafide work of Hasan Kamran (RA2011033010059), Anubhav Vats (RA2011033010062), Gaurav Raj (RA2011033010063) and Rimendra Kumar Agrawal (RA2011033010064) who carried out the project work under my supervision.

SIGNATURE

Subject Staff

Designation
Department

SRM Institute of Science and Technology
Potheri, SRM Nagar, Kattankulathur,
Technology Tamil Nadu 603203

SIGNATURE

Dr.B. Hariharan

Course Cordinator
Assistant Professor,

CINTEL
SRM Institute of Science and
Potheri, SRM Nagar, Kattankulathur,
Tamil Nadu 603203

ABSTRACT

In our daily life, everyone uses internet (network) for almost everything they need for their individual purposes. People send messages across network through emails, purchase items online with their credit card through web application such as amazon, eBay etc. Moreover, confidential information is also kept on a database. There are intruders, hackers and attackers who want to steal information for theirfinancial gain and access network which they are not authorised to do so. It is very important to have security implemented in network to protect our data from these malicious attacks. The solution to prevent from these malicious attacks are firewalls. Due to heavy attacks on web application and network, web application firewall and network firewall has been implemented to protect from any form of attacks.

TABLE OF CONTENTS

Project Scope:

This project is a comparative study of Web Application and Network Layer firewalls. This project gives critical analysis why it is a necessity and important to have a firewall in our network and system. Firewall is a protective barrier which stands and protects network from any traffic or packets that seem to bea threat to the trusted network, it controls the incoming network traffic basedon the security rules. Any harmful packet or traffic will be denied entry to the trusted network to prevent any harm.

This project will emphasise on the deep aspect of both Web application and Network Layer firewalls. Web application firewall are designed to protect web applications from web-based attacks, it operates at Application Layer. Web application firewall is responsible by controlling and examining incoming trafficon web application or web servers.

Network Firewall examines IP packet and determines whether to accept or deny packet based on source and destination IP address. However, Network firewalls do not examine web traffic like HTTP, due to this it is possible for anattacker to carry out malicious code using HTTP protocol but thanks to Web application firewall, the capability of examining HTTP protocol block any malicious.

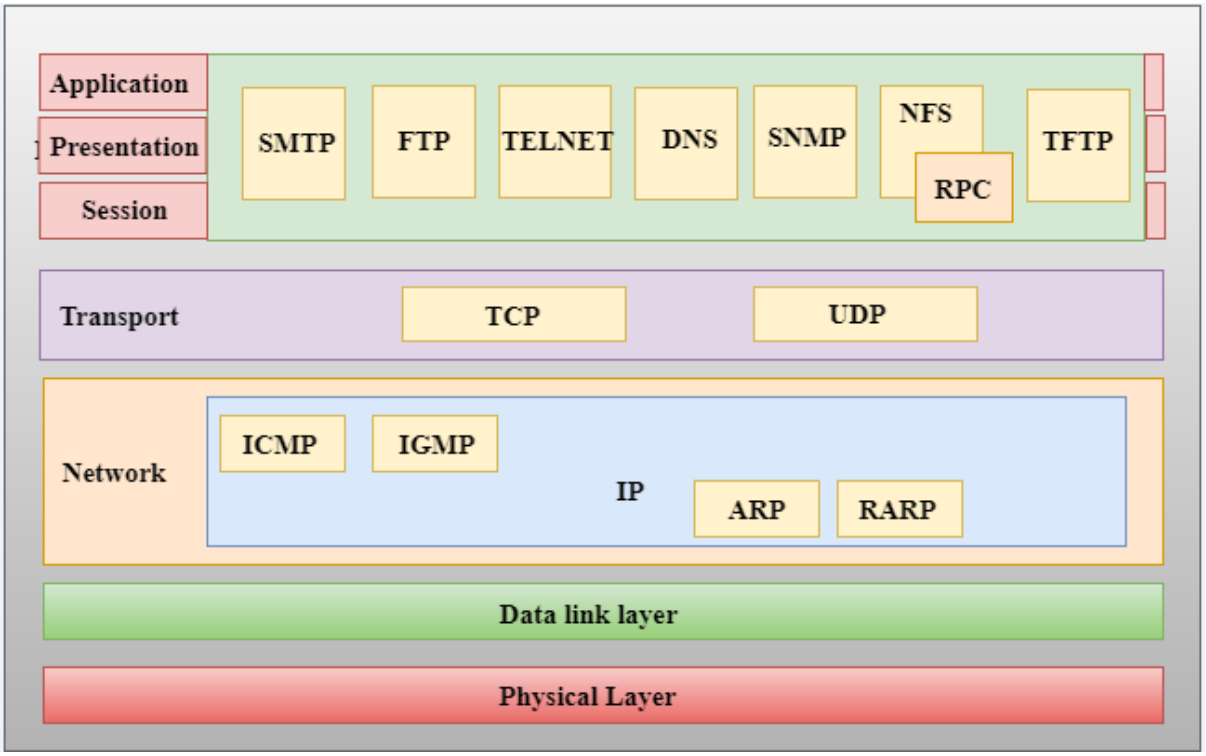
Network Layer Firewall was not created with web application traffic in mind, that's why Network Firewall do not understand web application language such as HTML and XML. Network layer Firewall cannot prevent attacks against web-based attacks such as SQL Injection and Cookie poisoning, the Web applicationFirewall can protect such attacks. One of the significant functions about web application Firewall is that Web application firewall can detect and defend unknown attacks which the network firewall is not capable of doing.

TCP/IP Communication for Firewalls:

TCP/IP is a basic communication protocol of the internet, TCP/IP are two separate protocols, 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. 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. 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.

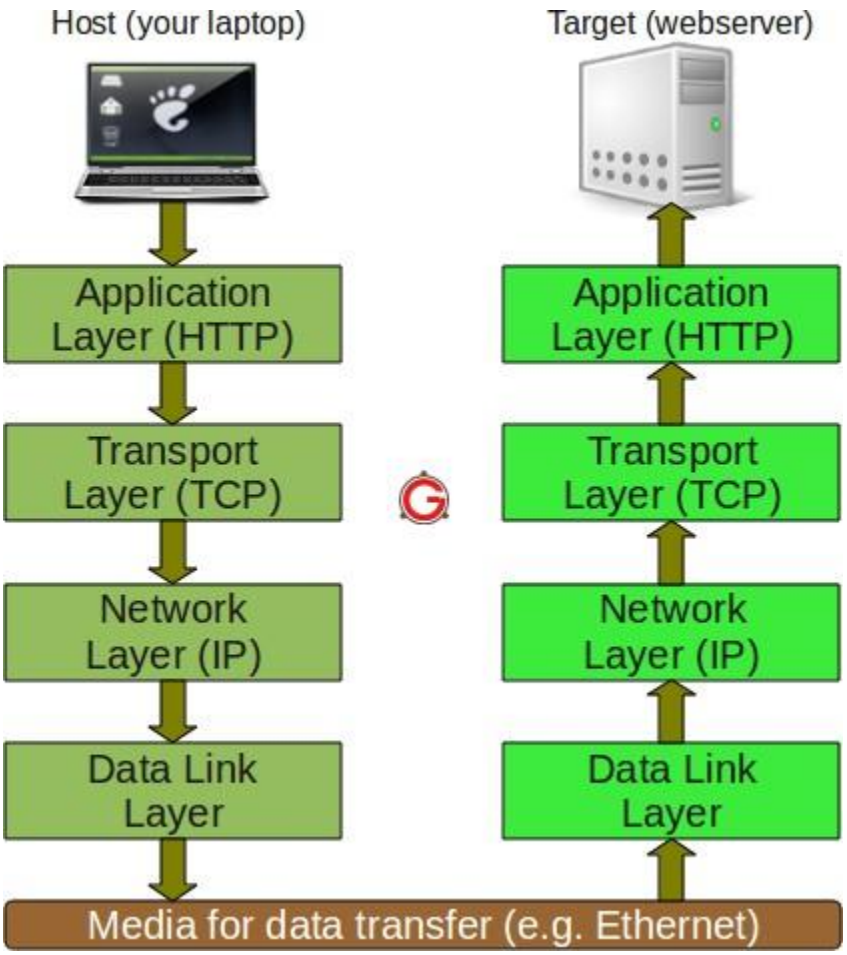
The four layers of TCP/IP Model are:

- 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. The Application protocols that function 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.

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 function on the internet layer are Internet Protocol, Internet Control Message Protocol.



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 function on Network access layer are Ethernet, Frame delay. As soon as host 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. The target receives the data on the network access layer then uses the same procedure to move the data up from network access to Application Layer.

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. 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.

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. Application-based Web Application are normally installed closest to the application and sometimes joined into the application code itself. One of the examples 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.

WEB APPLICATION ATTACKS

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. One of the basic malicious commands of SQL Injection attack is 'OR '1' = 1'. 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. After the malicious code has been successful, the attacker is able to get into someone's account which for example, it logins as "Mickey". The reason why it logs in as "Mickey"is because with the malicious code the attacker has input in the web form, thecode will call the first user on the SQL Database, which enable the attacker to log in by passing the authentication process.

COUNTERMEASURES

The Web Application Firewall inspects HTTP requests from web client to the web application. The web application firewall identifies SQL Injections then blocks it based on the security rules implemented on it. The Legitimate web traffic will be granted entry through the web application firewall to web application. Basically, 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.

BENEFIT OF WEB APPLICATION FIREWALL

The benefits of web application are:

1) Web application firewall is able to filter traffics even at the Network Layer (Layer 3) and Transport Layer (Layer 4) and at the Application level, Web application firewall can filter traffic from Session Layer, Presentation layer to Application Layer (layer 5 to 7) of OSI reference model. This enables the webservers to be protected with high security procedures.

2) The dependency on patching vulnerability with code modification is mitigated significantly. If the code is partially faulty and is likely to cause threat, web application firewall can well protect the infrastructure from such vulnerabilities temporarily until either the vendor has provided a permanent solution.

3) Web application firewall benefit the implementation of deep packet inspection as there may be an incident if the message is carrying confidential information in the data payload and if the behaviour of the packet is not in agreement with the policies defined in Web application firewall, it usually disrupts the packet from transporting it to the network. It protects any sort of data leakage from the network which can cause serious issues related to the confidentiality of the data.

4) Web application firewall offers a software security solution for the network infrastructure threats in an organization.

NETWORK LAYER FIREWALL:

Network layer firewalls operates at Network Layer and Transport Layer (Layer4) of the TCP/IP Model and Network layer firewall has the capability of makingdecisions 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.

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.

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.

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. It is easy for an attacker to go through by indicating "reply" on the packer header.

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.

Circuit Layer Gateways

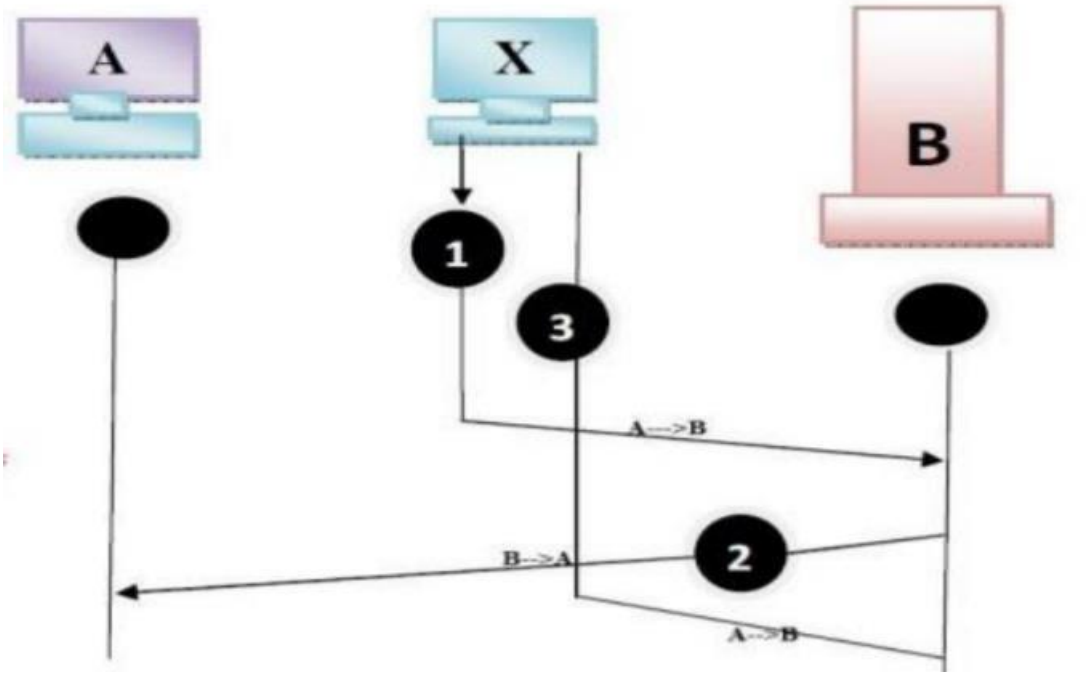
Circuit layer gateways operate mainly in Transport Layer (layer 4). They makebasic authorization decisions based on source and destination IP address as well as protocol type and port. This delivers a higher level of flexibility in thatCircuit layer gateways decides whether inbound requests to ports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

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. The network security policy is imposed at secure boundaries within the network called perimeter networks.

NETWORK LAYER ATTACK

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. In the image the IP spoofing attacker represent the “X” machine. Theattacker 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 packet that acknowledge the session number.

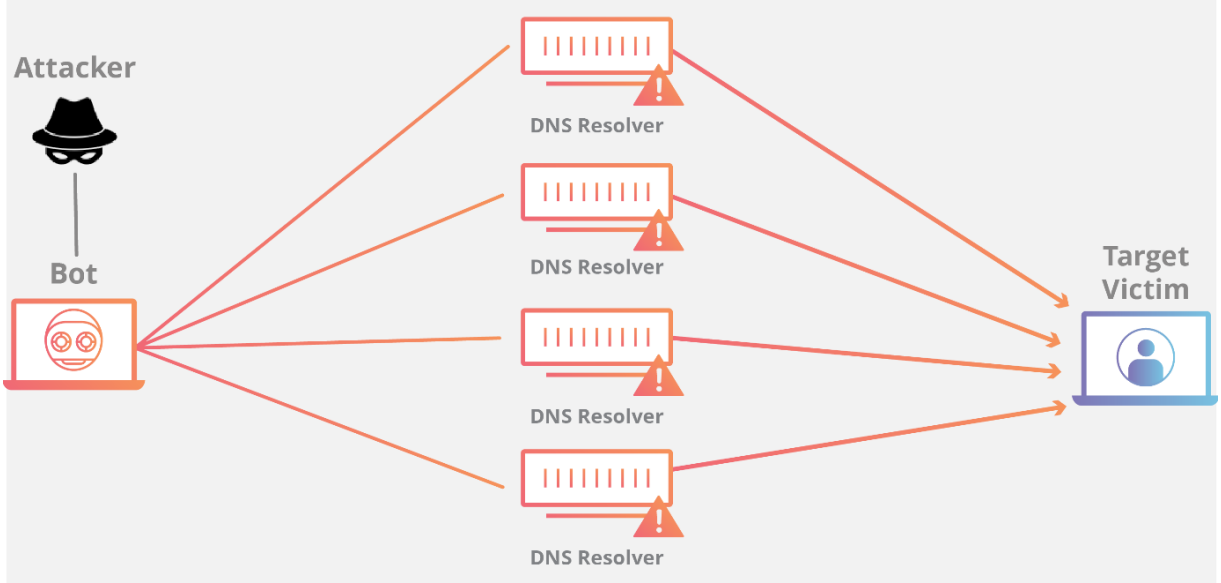
Countermeasure

Network Firewall simply discard packets with an inside source address if the packet arrives on an external interface based on the rules given to the network layer firewall, it will block all packet from outside the network. Blocking the outside will not allow the attack to address internal machine.

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.

There is another attack under Denial of service called Distributed Denial of service attack. This attack similar to Denial of service but this attack sends 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.



Countermeasure

Denial of service attack is one of the toughest network attack currently, it is very difficult to deal with because it is hard for network firewall to differentiate between the legitimate users and malicious users however network firewall only manages to deal with this by establishing a connection in its connection table for each packet.

Since Distribute denial of service attack transmits average of thousands packets per second, network firewall creates connections table and once the connection tables has exceed to its maximum capacity, it will deny extra connection to be created which would result by restricting legitimate user from opening connection as well if necessary.

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.

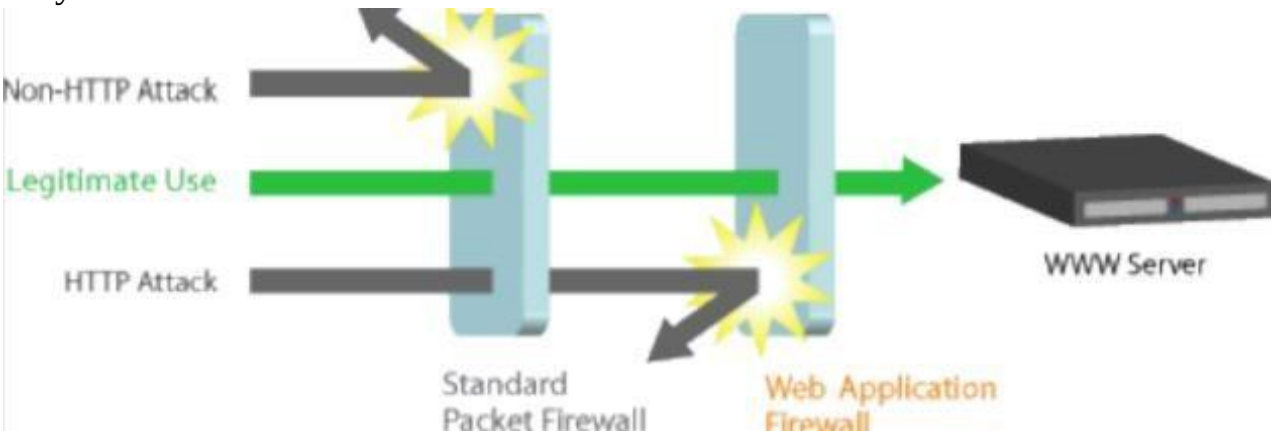
2) Network Firewalls filters protocols that are not needed to ensure it is secured from exploitation.

3) Network Firewalls do not reveal the names of the internal system which makes information become less available to the outside host.

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

BENEFITS COMBINATION OF NETWORK & WEB APLICATIONFIREWALL

Network and system are more secured and less vulnerable to attackers when use the combination of both web application and network layer firewalls. Using Network layer firewall or Web Application firewall alone is not fullysecured.



Observing the example above, Network layer firewall (known as Standard Packet Firewall) can examine non-http attack. It is easy and straight forward for network layer firewall to examine packet decide whether to accept or blockdata packet which are not HTTP protocols but it cannot protect HTTP Attacks, due to network layer firewall not capable of examine HTTP protocols, HTTP Attack is able go through Network Layer firewall easily. However, it will not be able to reach the web application or web server since web application firewall stands in front of the web servers. Web application firewall will examine the HTTP protocols, all the legitimate packet will be able to pass through network layer firewall and web application firewall to the web servers but if during the examination of the HTTP protocols, any suspicious or malicious attack was

identified, the web application firewall will block the attack. Therefore, we conclude that web application firewall and network layer firewall should always be implemented together. One of the most significant function about web application firewall is that web application firewall is able to detect unknown attacks and protects unknown which the network layer firewall is notcapable of doing that.

CONCLUSION

The basic idea of this project was to give the deep aspect of the web application and network layer firewalls, started by explaining how TCP/IP work,how each layer of the TCP/IP Model functions and how it communicates, overall explanation of firewall and how firewalls works on the TCP/IP models. Web Application firewall and network layer firewall has been explained in detailed. This project has identified one attack each on the web application and network layer and it has been critically analysed and how the web application firewall and network layer firewalls prevents those attacks. This project has explained how we can improve our network by implementing the combination of both web application and network layer firewalls. Implementing both web application firewall and network layer enhance extra layer of security and makes it extremely difficult for any attacker to harm our network since any attacks on the web application firewall are dealt with the web application firewall and any attacks on the network layer/transport layer are dealt with the network layer firewall.

REFERENCES

https://projectsinnetworking.com/comparative-study-of-web-application-and-network-layer-firewalls/

https://ieeexplore.ieee.org/document/5738566?arnumber=5738566

https://ipwithease.com/web-application-firewall-vs-network-firewall/

https://searchsecurity.techtarget.com/feature/Comparing-the-best-Web-application-firewalls-in-the-industry