A MINI PROJECT REPORT

ON

Comparative Study of Web application and Network Layer Firewalls

Submitted in fulfilment of the requirement of

Computer Communication Lab

By

Uppu Manikanta [RA2011003011182]

Bheema Shyam Kumar [RA2011003011174]

Sai Harshith Yaddala [RA2011003011173]

Ganesh Chappi [RA2011003011170]

T Bhavana [RA2011003011123]

Under the Guidance of

M. Rajalakshmi

Department of Computer Science Engineering

SRM Institute of Science and Technology, Kattankulathur

JUNE 2022

CERTIFICATE

This is to certify that Computer Communication Lab Mini Project entitled "**Comparative Study of Web application and Network Layer Firewalls**" Submitted by "Uppu Manikanta [RA2011003011182] Bheema Shyam Kumar [RA2011003011174] Sai Harshith Yaddala [RA2011003011173] Ganesh Chappi [RA2011003011170] T Bhavana [RA2011003011123]" for the partial fulfilment of the requirement for Semester IV Subject of Computer Communication Lab to the SRM Institute of Science and Technology, is a bonafide work carried out during Semester IV in Academic Year 2021-2022.

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

TABLE OF CONTENT

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 their financial 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.

Objective of the Project

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 be a threat to the trusted network, it controls the incoming network traffic based on the security rules. Any harmful packet or traffic will be denied entry to the trusted network to prevent any harm.

There are attackers and intruders whose main motivation is to steal information for their financial gain and access network which they are not authorised to do so. Attackers find any possible means to get information or gain access. Attacks can occur on Network Layer and Application Layer, there are attacks that occur on network layer such as Packet Sniffing, IP Spoofing, Denial of Service Attack, Syn Flood, Ping Flood. The attacks that occur on web application is SQL Injection, XML Injection, Cross Site Script, Cookie Poisoning, Zero Day Attack, Buffer Overflow. 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 traffic on web application or web servers.

Introduction

The purpose of this project is to do relative study of Network layer firewalls and Web Applications. Firewalls have a vital role in our network system and this project gives us a critical analysis of importance of firewalls in web applications. Traffic or the packets that can be harmful for a trusted network are protected through firewalls. On the basis of security rules, the traffic coming to a network is controlled. Web Application firewall operates at application layer and it is designed to protect the web application from web-based attacks. To control and examine the incoming traffic on web applications and webservers firewalls are implemented. Based on IP address of source and destination Network firewall examines IP packets and decides whether to accept or not.

There are hackers and the attackers that try to access to networks to which they are not authorized for their personal interests and they use any mean to get that information. Internet works on different layers starting from the application layer to network layer Most of the attacks are done on the network layer such as packet sniffing, IP spoofing, Denial of Service Attack, Syn Flood, Ping Flood. SQL Injection,XML Injection, Cross Site Script, Cookie Poisoning, Zero Day Attack, Buffer Overflow are the type of attacks that can occur on web applications.

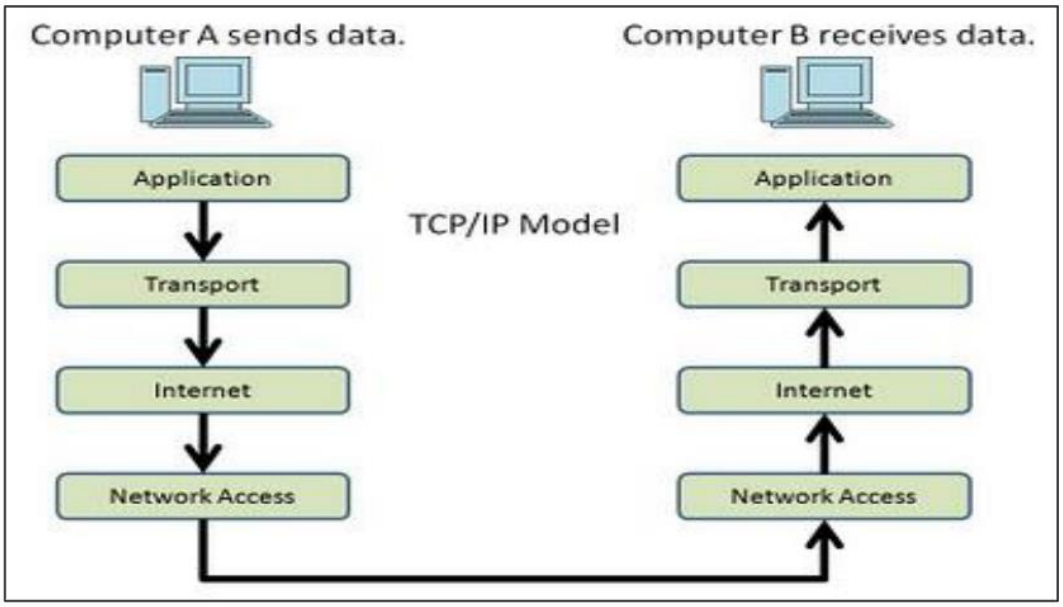
❖ TCP/IP Communication for Firewalls:

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 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. 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 9 OF 80 layer does this by sending bits signals through wire or wireless. The protocols that function on Network access layer are Ethernet, Frame delay.

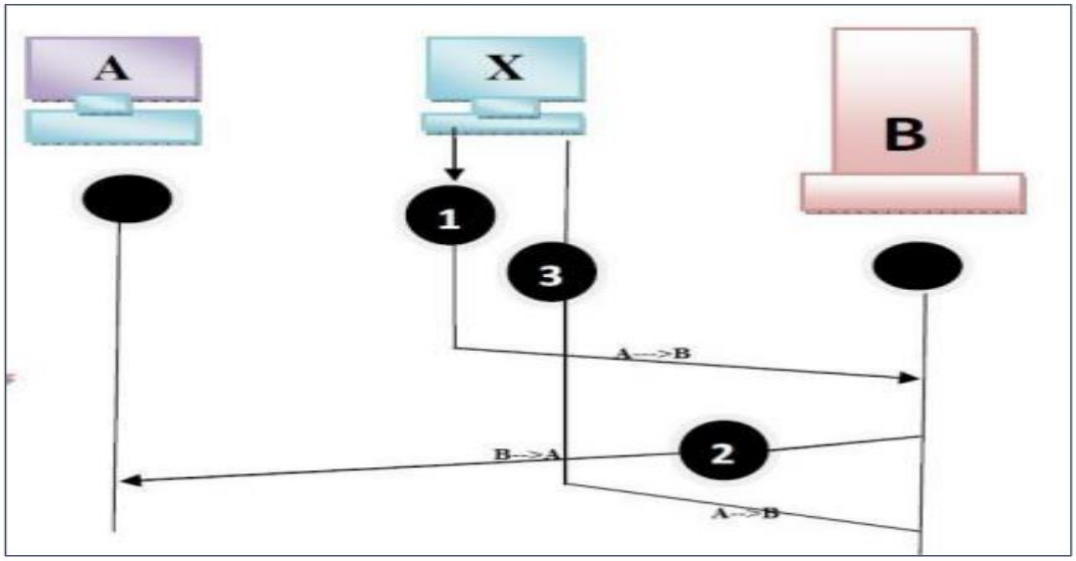


The Figure shows the Data Flow through TCP/IP Communication takes place within the TCP/IP Model when the application sends a data in. As soon as Computer A send the data, the data moves down to Transport Layer, where UDP or TCP adds the source and destination port numbers on the data and then passes 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.

❖ Common Network layer attacks:

1) IP Spoofing Attack

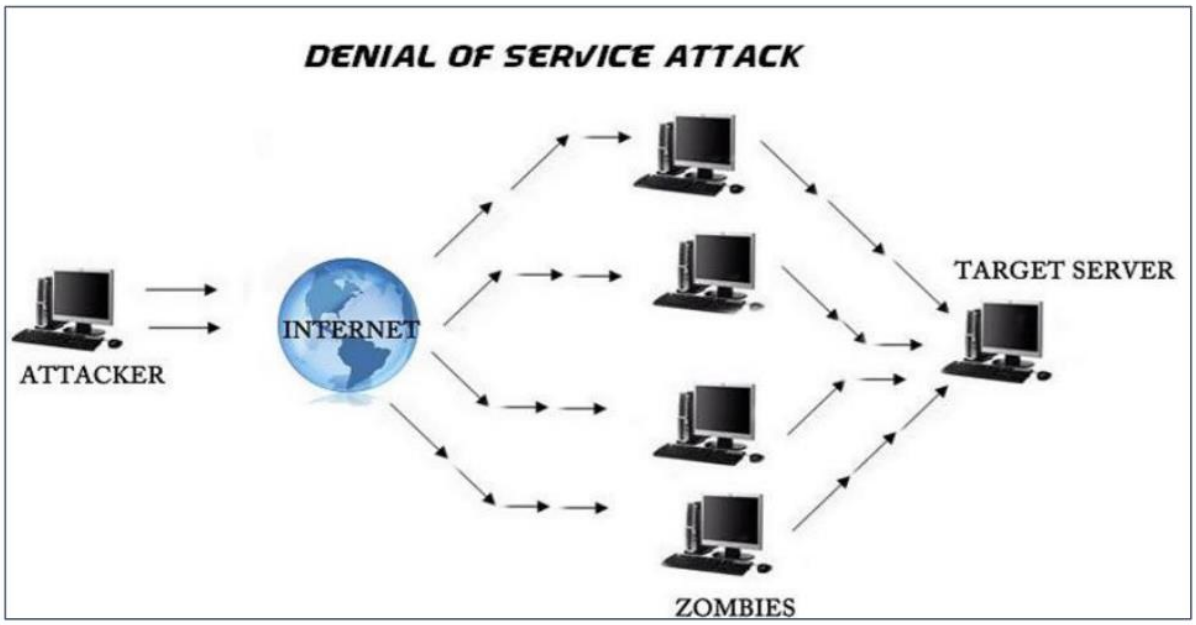
IP Spoofing attack is an attack occurs network/transport layer where the attacks transmit packets from the outside with a source address field containing an address of an internal host. The attacker expect that the use of a spoofed address will permit penetration of systems that employ simple source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



Example of IP Spoofing is given above in this 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 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.

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. 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.



❖ Common Web application attacks

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.

Attacker input SQL Injection on Web application

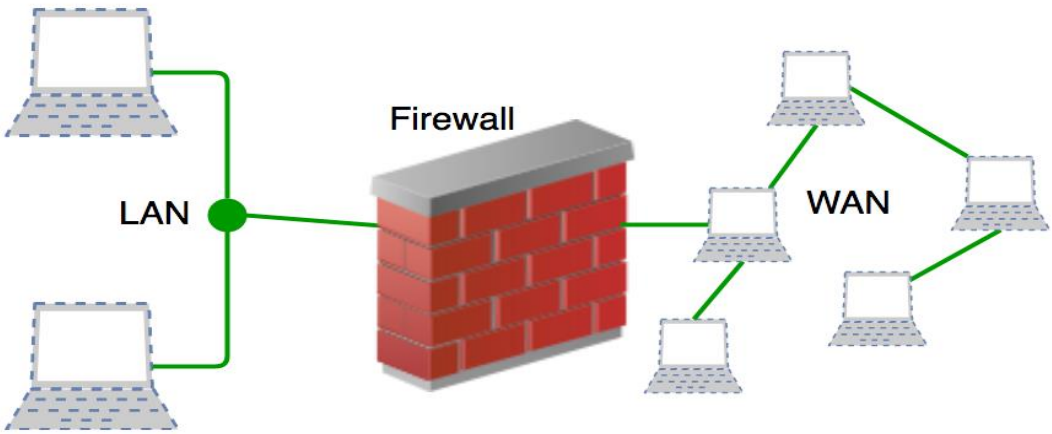
One of the basic malicious commands of SQL Injection attack is 'OR '1' = 1'. As shown in Figure If the web application is vulnerable, by inserting this malicious code will allow the attacker to login as the first user who last logged in.

Attacker has successfully used SQL Injection on Web application

After the malicious code has been successful, the attacker is able to get into someone's account which in the example given in Figure, 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.

❖ Functionality analysis of network layer firewalls.

- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
- **Accept :** allow the traffic
  Reject : block the traffic but reply with an "unreachable error"
  Drop : block the traffic with no reply
- A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

❖ Functionality analysis of web application firewalls

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe. Just as a proxy server acts as an intermediary to protect the identity of a client, a WAF operates in similar fashion but in the reverse—called a reverse proxy—acting as an intermediary that protects the web app server from a potentially malicious client.

WAFs can come in the form of software, an appliance, or delivered as-a-service. Policies can be customized to meet the unique needs of your web application or set of web applications. Although many WAFs require you update the policies regularly to address new vulnerabilities, advances in machine learning enable some WAFs to update automatically. This automation is becoming more critical as the threat landscape continues to grow in complexity and ambiguity. A WAF analyzes Hypertext Transfer Protocol (HTTP) requests and applies a set of rules that define what parts of that conversation are benign and what parts are malicious. A WAF can take two approaches to analyzing and filtering the content contained in these HTTP requests or a hybrid combination of the two:

- **Whitelisting:** A whitelisting approach means that the WAF will deny all requests by default and allow only requests that are known to be trusted. It provides a list of what IP addresses are known to be safe. Whitelisting is less resource-intensive than blacklisting. The downside of a whitelisting approach is that it may

unintentionally block benign traffic. While it casts a wide net and can be efficient, it may also be imprecise.

- **Blacklisting:** A blacklisting approach defaults to letting packets through and uses preset signatures to block malicious web traffic and protect vulnerabilities of websites or web applications. It is a list of rules that indicate malicious packets. Blacklisting is more appropriate for public websites and web applications since they receive a lot of traffic from unfamiliar IP addresses that aren't known to be either malicious or benign. The downside of a blacklisting approach is that it is more resource-intensive; it requires more information to filter packets based on specific characteristics, as opposed to defaulting to trusted IP addresses.
- **Hybrid security:** A hybrid security model uses elements of both blacklisting and whitelisting.

Regardless of the security model a WAF uses, it ultimately works to analyze HTTP interactions and reduce or, ideally, eliminate malicious traffic before it reaches a server for processing.

❖ Benefits and limitations of network layer firewalls.

The benefit of Network layer firewall are:

- Network Firewalls can focus extended logging of network traffic on one system
- Network Firewalls filters protocols that are not needed to ensure it is secured from exploitation.
- Network Fi rewalls do not reveal the names of the internal system which makes information become less available to the outside host
- Network Firewalls are normally quicker than other firewall technologies because
- Network firewall performs very less evaluation.

The limitations of Network layer firewall are:

- A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce your password policy or prevent misuse of passwords. Your password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.

- Firewalls are ineffective against nontechnical security risks such as social engineering, as discussed in Chapter 1, “There Be Hackers Here.”
- Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.
- Firewalls cannot protect you from poor decisions.
- Firewalls cannot protect you when your security policy is too lax.

❖ Benefits and limitations of web application firewalls

The benefits of web application are:

- 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 web servers to be protected with high security procedures.
- 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.
- 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.
- Web application firewall offers a software security solution for the network infrastructure threats in an organization.

❖ Firewall attack mitigation techniques

1. Avoid becoming a bot:

Let’s say your internal website (or database or any such resource) which is not open to the public is down due to DDoS attack. What’s the catch? No employee would possibly attack their own company asset. Hence, the possible chances are that few of the employees’ systems are compromised and are being used as bots. So, the employees must be educated on how not to be exploited.

They should be aware of basic security measures such as

- Using a strong password
- Configuring local firewall and managing the same
- Not open random attachments
- Always use antivirus to scan anything before opening
- Apply timely security patches and keep the machine up to date
- If they doubt that they could be compromised, then install some network monitor like glassware to monitor the traffic
- But what if they've become a bot?. Then the machine needs to be isolated, detached from the network and cleaned up before it is reconnected to the network

2. Reducing Attack Surface:

Reducing the surface that can be attacked limits the options for attackers. This is one of the methods.

- You will have to separate and distribute assets in a network so that it's harder to be targeted. For example, you can have your web servers in the public subnet, but the

underlying database servers should be in a private subnet. Also, you can restrict access to database servers from your web servers and not from other hosts.

- Using Firewalls and Network Access Control Lists to allow only necessary traffic, to necessary ports from necessary hosts. In the case of web servers, you basically allow traffic from anywhere to port 80 of your webserver. And in such cases, you further take other protective measures like the ones we've listed here.
- Even for sites that are accessible over the internet, you can reduce the surface area by restricting traffic to countries where your users are located

3. CDNs:

A Content Delivery Network (CDN) distributes your content and boosts performance by minimizing the distance between your resources and end-users. It stores the cached version of your content in multiple locations and this eventually mitigates DDoS attack by avoiding a single point of failure, when the attacker is trying to focus on a single target. Popular CDNs include Akamai CDN, Cloudflare, AWS CloudFront, etc.

4. Black Hole Routing:

As the name suggests, blackhole routing (similar to /dev/null in Linux) without any filtering routes both legitimate and malicious traffic to a null route or black hole where it's going to be dropped from the network. Based on the pattern, if you could identify the attacker, then you could filter those packets and route them to the black hole.

5. Rate Limiting:

Limiting the number of requests a server will accept over a certain time window from an IP is a way of mitigating denial of service attacks, similar to that of IPtables connlimit. However, in the case of DDoS, rate-limiting alone wouldn't be sufficient. Nevertheless, it's useful for DDoS protection.

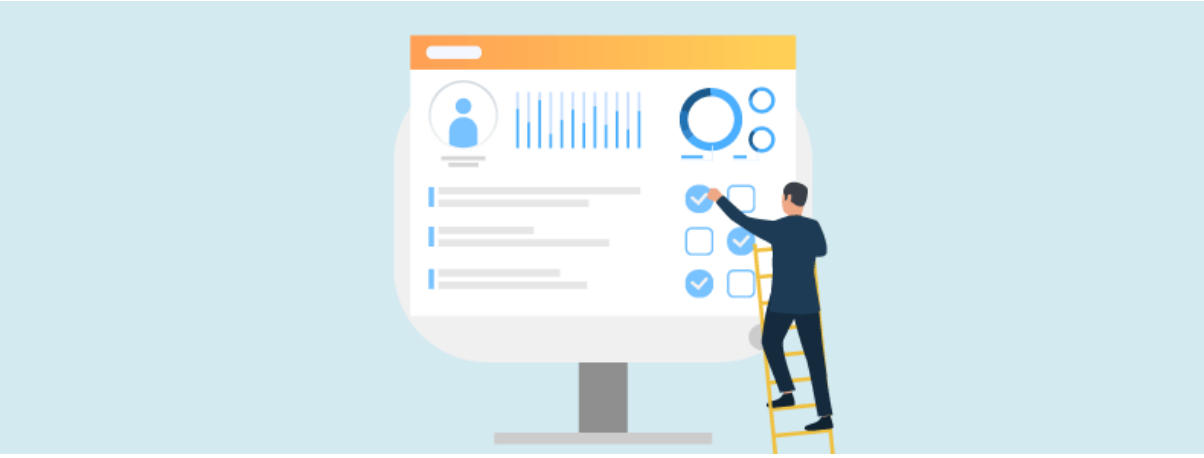
6. WAF:

A Web Application Firewall (WAF) is a tool that can assist in mitigating the Layer 7 DDoS attack. You can place a WAF in between the internet and origin server and WAF can act as a reverse proxy protecting the server from exposure by making the clients pass through them before reaching the server. Using WAF, you can quickly implement custom rules in response to an attack and in turn, mitigate them, so that the traffic is dropped before even reaching your server, thus taking an offload from the server. Depending upon where you implement WAF, it can be implemented in one of the three ways

- Network-based WAF
- Host-based WAF
- Cloud-based WAF

7. Scale:

In this method, you scatter the DDoS traffic across a cluster of nodes so that it's handled like any other legitimate traffic. For example, consider you have implemented auto-scaling of your web resources when the incoming connection requests are beyond a certain number.



Now, this autoscaling will ensure new web servers are being spawned to handle the connection requests. You can set up alerts so that you're notified when more than a certain number of instances are spawned. By doing so, you will know that there's some issue with it and you can further implement the mitigation techniques to block those traffic and bring the server back to its normal functioning. This totally depends on

- the size of the attack
- the efficiency of the network (Transit capacity)
- compute resources (Server capacity)

Now that you're aware of some of the techniques to mitigate DDoS, let's look at the stages of DDoS mitigation that help in the implementation of the techniques.

❖ Security requirements with Firewall analysis

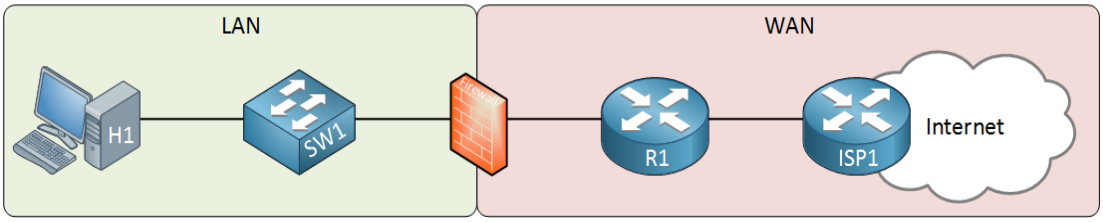
To start, a firewalled system analyzes network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept. It does this by allowing or blocking specific data packets — units of communication you send over digital networks — based on pre-established security rules. A firewall works like a traffic guard at your computer's entry point, or port. Only trusted sources, or IP addresses, are allowed in. IP addresses are important because they identify a computer or source, just like your postal address identifies where you live.

A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies. Before a firewall policy is created,

some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured—including which types of traffic can traverse a firewall under what circumstances.16 This risk analysis should be based on an evaluation of threats; vulnerabilities; countermeasures in place to mitigate vulnerabilities; and the impact if systems or data are compromised. Firewall policy should be documented in the system security plan and maintained and updated frequently as classes of new attacks or vulnerabilities arise, or as the organization's needs regarding network applications change. The policy should also include specific guidance on how to address changes to the ruleset. Generally, firewalls should block all inbound and outbound traffic that has not been expressly permitted by the firewall policy—traffic that is not needed by the organization. This practice, known as deny by default, decreases the risk of attack and can also reduce the volume of traffic carried on the organization's networks. Because of the dynamic nature of hosts, networks, protocols, and applications, deny by default is a more secure approach than permitting all traffic that is not explicitly forbidden. This section provides details on what types of traffic should be blocked. Section 4.1 discusses policies for packet filtering and stateful inspection based on IP addresses and other IP characteristics. Section 4.2 covers policies relating to application-specific traffic. Section 4.3 covers access based on user identity, and Section 4.4 describes policies triggered by network activity.

❖ Firewall deployment with LAN access control.

The firewall is the barrier between a **trusted and untrusted network**, often used between your LAN and WAN. It's typically placed in the forwarding path so that all packets have to be checked by the firewall, where we can drop or permit them. Here's an example:



Above we have our LAN that has a host computer and a switch. On the right side, there's a router that is connected to the ISP which offers Internet connectivity. The firewall sits in between to protect our LAN. The router is optional, it depends on your connectivity to the WAN. For example, if your ISP offers cable then you probably have a cable modem with an Ethernet connection that you can connect directly to your firewall. When it's a wireless connection, you probably need the router there for the connection. You will also probably need the router if you do any (advanced) routing like BGP. Most firewalls support some basic routing options: static routes, default routes and sometimes routing protocols like RIP, OSPF or EIGRP.

❖ Firewall deployment with application-level control:

An application firewall is a type of firewall that governs traffic to, from, or by an application or service. Application firewalls, or application layer firewalls, use a series of configured policies to determine whether to block or allow communications to or from an

app.Traditional firewalls control data flow to and from the CPU, examining each packet as it passes through. An application firewall takes it further by controlling the execution of files or code by specific applications. This way, even if an intruder gains entry to a network or server, they can't execute malicious code. Application firewalls can be active or passive.

Active – Active app firewalls actively inspect all incoming requests—including the actual message being exchanged—against known vulnerabilities such as SQL injections, parameter and cookie tampering, and cross-site scripting. Only requests deemed "clean" are passed to the application.

Passive – Passive app firewalls act in a similar way to an intrusion detection system (IDS) in that they also inspect all incoming requests against known vulnerabilities, but they don't actively reject or deny those requests if a potential attack is discovered.

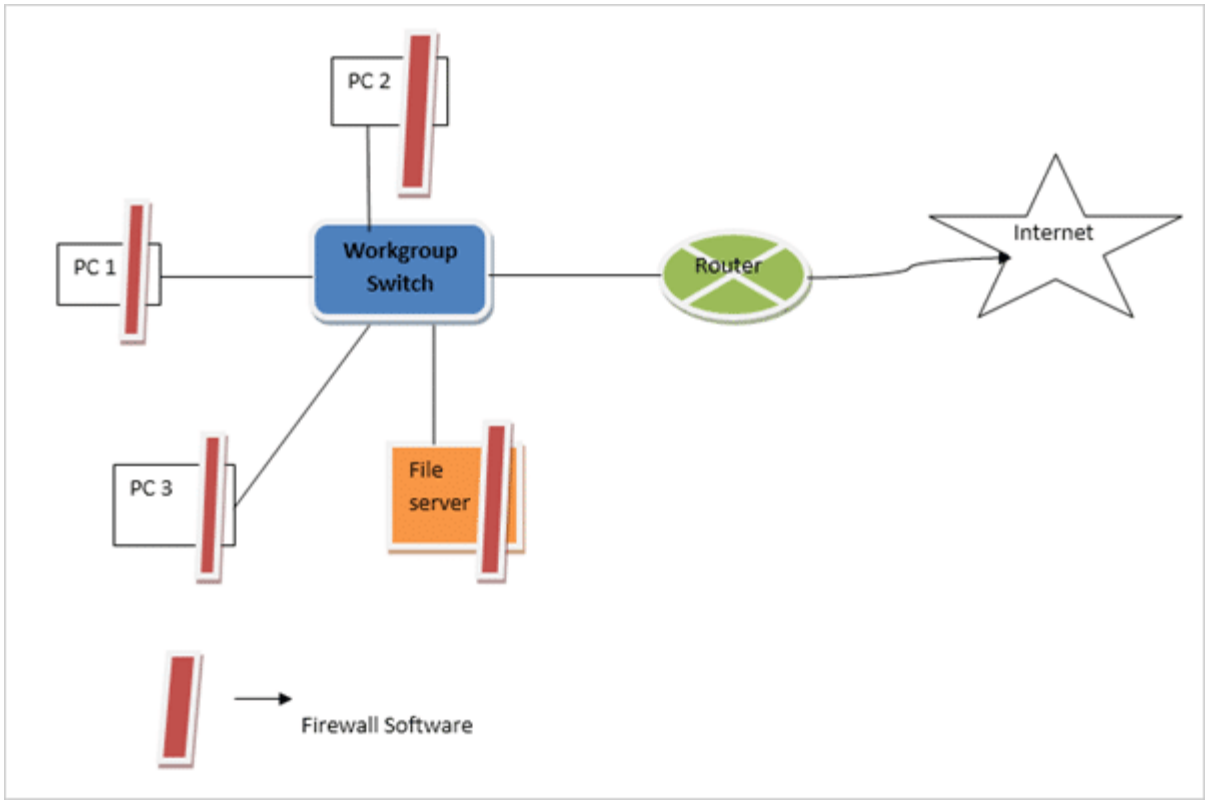
Application firewalls are generally remotely updateable, which allows them to prevent newly discovered vulnerabilities. They're often more up to date than specific security-focused code included in applications, due to the longer development and testing cycles required to include such code within applications. Today, you'll most commonly see *web* application firewalls (WAFs) to filter, monitor, and block HTTP/S traffic to and from a web application, specifically.

❖ Firewall deployment with Comprehensive server security

In small networks, we can make each of our network device secured by ensuring that all the software patches are installed, unwanted services are disabled, and security software are properly installed within it.

In this situation, as also shown in the figure, the firewall software is mounted on each machine & server and configured in such a manner that only listed traffic can come in and out of the device. But this works efficiently in small-scale networks only.

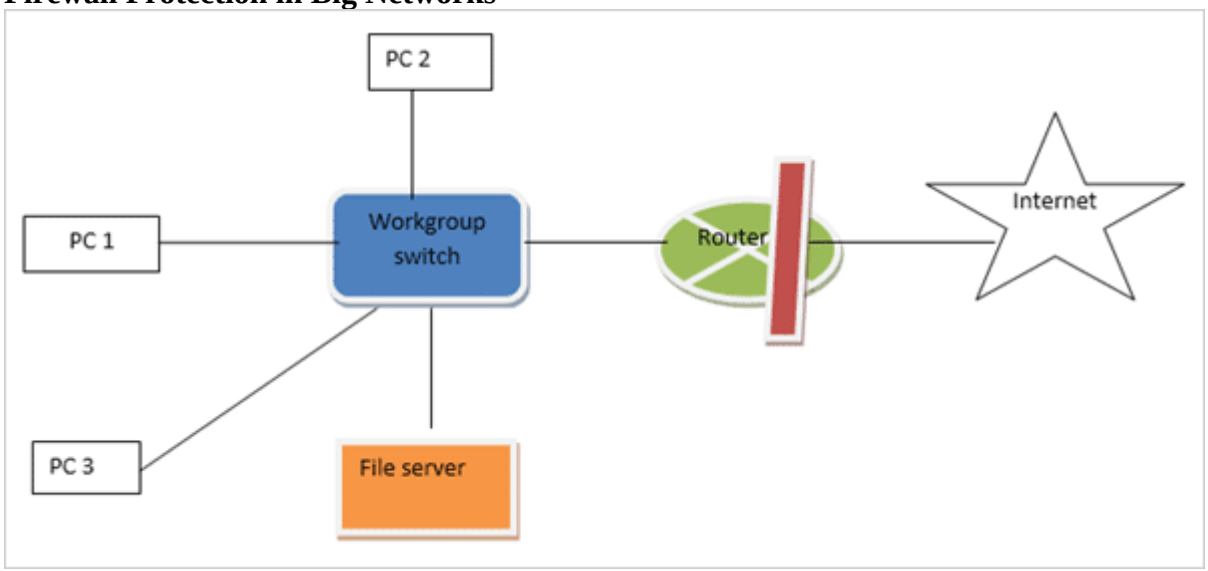
Firewall Protection in Small Scale Network



In a large-scale network, it is almost next to impossible to manually configure the firewall protection on each node.

The centralized security system is a solution to provide a secure network to big networks. With the help of an example, it is shown in the below figure that the firewall solution is imposed with the router itself, and it becomes simple to handle security policies. The policies of traffic come in and out into the device and can be handled solely by one device.This makes the overall security system cost-effective.

Firewall Protection in Big Networks

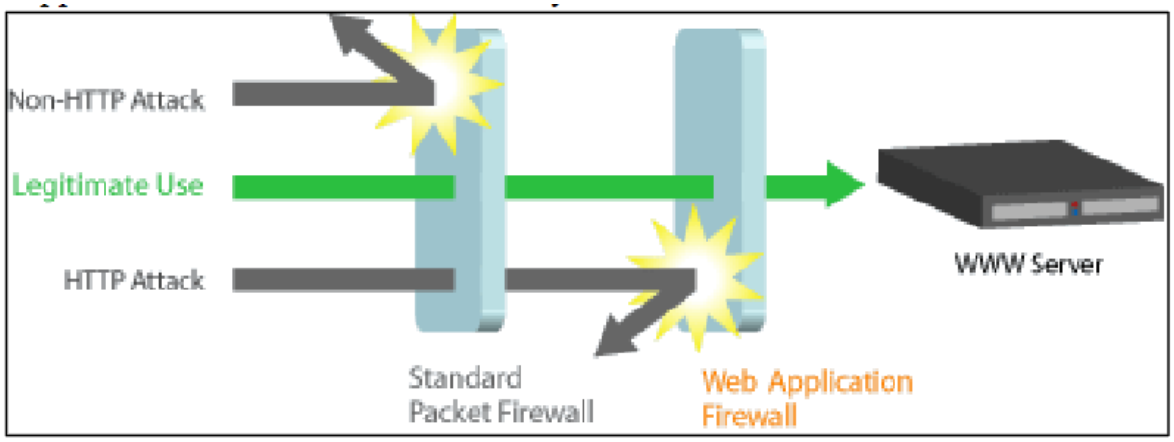


The concept of the firewall was introduced to secure the communication process between various networks. A firewall is a software or a hardware device that examines the data from several networks and then either permits it or blocks it to communicate with your network

and this process is governed by a set of predefined security guidelines. In this tutorial, we will explore the various aspects of the Firewall and its applications. A firewall is a device or a combination of systems that supervises the flow of traffic between distinctive parts of the network. A firewall is used to guard the network against nasty people and prohibit their actions at predefined boundary levels.A firewall is not only used to protect the system from exterior threats but the threat can be internal as well. Therefore, we need protection at each level of the hierarchy of networking systems. A good firewall should be sufficient enough to deal with both internal and external threats and be able to deal with malicious software such as worms from acquiring access to the network. It also provisions your system to stop forwarding unlawful data to another system.

❖ Benefits of combination:

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 fully secured.



Implementation of Network Layer firewall & Web Application Firewalls.

Observing the example from Fig 2:21, Network layer firewall (known as “Standard Packet Firewall” in Figure can examine non-http attack. It is easy and straight forward for network layer firewall to examine packet decide whether to accept or block data packet which are not HTTP protocols but it cannot protect HTTP Attacks, due to network layer firewall not capable of examing 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 Infront 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, I conclude that web application firewall and network layer firewall should always be implemented together. One of the most significant functions about web application firewall is that web application firewall is able to detect unknown attacks and protects unknown which the network layer firewall is not capable of doing that.

❖ Conclusion:

The aim of this project was to explore Web application firewall and network layer firewalls how it would be used to protect from attackers. Comparing the two technologies, it has been identified that Network Layer Firewall fall short in some aspect and how web application firewall is more useful. Different type of attacks has been identified on each Network and web application to ensure that there are many harmful capabilities that could affect our network or system. This project has shown two possible and harmful attack on each network and web application. The two attacks identified in Network layer are IP Spoofing and Denial of Service. The two attacks identified in Web Application are SQL Injection and Cross Site Script.

This project has also given much emphasis to conclude that web application firewall and network layer firewall should always be implemented together, in order to effectively protect our system and network from any possible attacks.

❖ References

- http://www.cisco.com/c/en/us/about/securitycenter/guide-ddos-defense.html
- http://www.acunetix.com/blog/news/barracuda-networks-breached/ 3.
- https://www.ukessays.com/essays/computer-science/advantagesand-disadvantages-of-firewalls-computer-science-essay.php
- http://www.ijircce.com/upload/2013/march/14_Network%20Attacks.pdf
- https://crypto.stanford.edu/cs155/papers/CSS.pdf