IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FIREWALL TECHNOLOGIES , TYPES AND ITSAPPLICATIONS

Authors :

1. Mayuri Bapat
2. Ritesh Rakshe
3. Rugved Tingare
4. Abhishek Yadav

ABSTRACT :-

Interest and knowledge in computer security is increasing day by day with increasing needs. This interest is not clear due to the growth of Internet services and the increasing number of organizations actively working and transmitting information on the Internet or the Internet. In the current situation, network security has become an important issue. It's like an evil that, once spread, affects us all within seconds. Therefore, this article examines network security from the perspective of firewalls and explores how they help protect systems and networks. A firewall is a part of a computer or network that is configured to block communication from unauthorized sources while allowing access from authorized sources. Firewall technologies and types are also discussed. This article explains firewalls and how they help with network security, businesssecurity, and personal security. He goes on to discuss the important factors in selecting, designing or configuring a firewall. Threats to firewalls are also listed at the end. Keywords: network, firewall, security, computer traffic, network, packet filter, access control list, threats.

INTRODUCTION :-

The most important thing in the system is security. There are many ideas regarding the security system. frewalls top the list of most important security strategies. A firewall can be used as software or hardware that essentially blocks illegal communications from entering or leaving the network. Many software can provide security at the system or network level. Similarly, firewall tools are also used to ensure system security. Firewalls have long been used to prevent unauthorized Internet users from accessing private systems connected to the Internet.All information entering and exiting the network passes through the firewall, which examines all packets and blocks those that do not meet certain security requirements. In general, firewalls are installed to prevent unauthorized access by third parties. This helps prevent hackers from accessing computer systems on your network. In addition, it is not easy for the firewall to block traffic from outside to inside, allowing internal users to communicate more with the outside. [2]Due to the lack of security solutions, networks are now forced to adopt multiple layers designed to create problems for criminals.

FIREWALL :-

A firewall is a computer, router, or other communications device that filters access to a protected network.A firewall is a network security device that monitors network access and decides to allow or block certain traffic based on security criteria.
Firewalls have been the first line of defense for network security for over 25 years. They create a barrier of security and control networks on the outside that can be trusted or not .
Firewalls can be hardware, software, Software as a Service , public cloud or private cloud .

FIREWALL : BASIC APPROACHES AND LIMITATIONS :-

Firewall technology can be used to protect your network by installing a security screen on a private or intranet connected to the public Internet, making it easier to secure traffic, call tracking and monitoring, and monitor access attempts. It can also be used to isolate subnets to provide an additional layer of security within an organization.
Firewalls use three methods or services to protect the Internet:
Packet filtering, circuit proxies, and application proxies. Some authors roughly divide it into two ways: transport layer and application layer

PACKET FILTERING :-

Firewalls with these features perform only very simple tasks, such as examining packet headers, validating IP addresses, ports, or both, and allowing or denying access without modification. They have the advantage of speed and efficiency due to their ease of use. Packets are filtered as incoming, outgoing, or both, depending on the type of router. Another advantage is that they do their job silently, regardless of the user's knowledge, silently or with the help of Internal and External
Gateway Systems.
They have good transparency. Packets can be filtered by some or all of the following criteria: destination IP address, destination IP address,TCP/UDP port, and TCP/UDP destination stops the boat. This type of firewall blocks connections to specific hosts, networks, and ports.

CIRCUIT PROXY :-

The second approach is the use of what is called a circuit proxy. The main difference between the circuit proxy and the packet filtering firewall is that the former is the addressee to which all communicators must address their packets. Assuming access has been granted, the circuit proxy replaces the original address (its own) with the address of the intended destination. It has the disadvantage of laying claim to the processing resources required to make changes to the header, and the advantage of concealing the IP address of the target system.

APPLICATION PROXY :-

The third way is to use so-called application proxies.
Application names are more difficult to execute than packet-filtering firewalls or
circuit proxies. The application agent understands application requirements and information, and interacts with application-specific information. Based on the information submitted for evaluation, the application agent can identify the user and determine what information may pose a threat. The price to pay for this better performance is that customers have to make frequent revisions, sometimes complex procedures leading to a loss of transparency. Application names are called service names, and the hosts running them are called application gateways.

PACKET INSPECTION APPROACH :-

Unlike the methods described so far, this approach involves analyzing the content and content of the package. Audit firewalls perform audits using an audit system that understands and can inspect data sent to all layers, from the network layer to the application layer. It performs analysis by collecting all the data collected from each layer in a single analysis and then analyzing it. Rocket can also record the state of each connection it hosts and act on that information. Examples of stateful firewalls are Checkpoint's "Firewall-1" [5] or the stateful packet filters in Network Associates' Gauntlet.

FIREWALL LIMITATIONS :-

The firewall cannot prevent the user or attacker from entering and exiting the internal network using the modem, thereby bypassing the firewall and its protection.

Firewalls cannot enforce your password or prevent password errors. Your password policy is important in this area as it defines valid behavior and determines the consequences of non-compliance.

As discussed in Chapter 1, "There Are Hackers Here", firewalls are ineffective against malicious risks such as social engineering.

Firewalls cannot prevent internal users from accessing websites containing malicious code, so user education is crucial.

Firewalls can't protect you from bad decisions.

Firewalls can't protect you when your security policies are gone.

Key Features of a firewall :-

before learn about how a firewall functions, we have to comprehend what a firewall can and can'tdo. A wide range of a firewalls share some broad highlights and capacities to distinguish what afirewall can do. In fact a firewall must have these essential capacities:

- Control and arrange tra c
- Authentication access
- Protect organization reources
- Maintain and provide details regarding events
- Work as a mediator
- Protect network resources from the harmful actions while accessing internet.
- Assure protected and secure access to your internal assets to outside users
- May increase performance of network system.

A firewall is only an exterior layer of protection so it cannot do everything. It is just an artificial machine

Types of firewall techniques :-

Firewalls are regularly used to stay away from unlawful Internet clients from getting to individual systems that are connected to the Internet. There are a few firewall procedures and every firewall mayutilize at least two than two methods in show. One of the significant problems that any organization encounters while tries to verify their sensitive information is finding the correct apparatuses for theactivity. Even for a typical instrument, for example, a firewall, numerous organizations probably won'thave an unmistakable thought of how to locate the correct firewall for their requirements, how to design those firewalls, or why such firewalls may be vital. The initial phase in finding the correct firewalls to ensure your organization's information is to comprehend what sort of firewalls there are. At this moment,
there are five distinct sorts of firewall models, comprehensively:

1.) Packet-filtering firewall

2.) Stateful inspection firewalls 3.)

Circuit-level gateways

4.) Proxy or Application-level gateways firewalls 5.) Next-

generation firewalls

1.) Packet-filtering firewall

This technique is the oldest type of firewall model. Packet-filteringfirewalls essentially make a checkpoint at a traffic switch or router. The firewall directly check theinformation packets passing through router or switch for example, the source and destination IPaddress, packet number, port number, and other data without opening up the packet to investigate itsinformation. It works on network layer of network model. This technique applies a lot of principles(in view of content of IP and transport header fields) on every packet and dependent on the result,chooses to either transfer or dispose of the packet. For instance, a rule could determine to hinder all approaching traffic from a specific IP address or deny all traffic that utilizes UDP protocol. In the event that there is no match with any predefined rules, it will make default move. The default activity can be to 'dispose everything' or to 'acknowledge all packets'.

2.) Stateful inspection firewalls:

This technique is also called 'Dynamic Packet Filtering'. Statefulfirewall basically keeps track ofthe status of active links and uses this information to decidewhich packet should be allowed through it. In this approach, firewall keeps a record of dynamicTCP and UDP sessions information in tabular form including session's sender and recipient IP,port numbers, and also TCP sequence number. Records are made for only those UDP or TCPconnections that fulfill characterized security criteria's; packets related with these sessions areallowed to go through the firewall. Sessions that don't coordinate with any policy are denied,similar to any packets got that don't coordinate a current table section.Stateful inspection is more secure than packet filtering because it just permits information havinga place with current session. For example, instead of allowing any host to send any kind of TCPtraffic, it can verify the client when the session is built up, it can decide if the packets truly carryHTTP.

3.) Circuit-level gateway firewalls:

Circuit level firewalls are operated at the Session layer of thenetwork model and they monitor TCP (three way handshake) connection to verify that requested connection is authenticated or not. It goes about as a virtual association between theremote host and the inner clients by making another association among itself and the remote host.It additionally changes the source IP address in the parcel and puts its very own location at thespot of source IP address of the bundle from end clients. Thusly, the IP locations of the innerclients are concealed and verified from the outside world.

4.) Application gateways:

Application firewalls review network packets to check whether data isvalid (at the application layer) before allow making a connection. It investigates the dataencapsulated in all packets going through network and after that it provides complete connectionstate. These firewalls also validate other security information like user passwords and servicerequests. Application or proxyservices are used for specific reason in order to control traffic suchas FTP or HTTP. These services can provide increased access control , detailed checks needed fordata validity, and they can generate summary report about the traffic to identify and track trafficIt is otherwise called Proxy server. It works as:

Step-1: User contacts the application door utilizing a TCP/IP application, for example, HTTP.

Step-2: The application door or gateway gets some information about the remote host with whichthe client needs to set up an connection or association. It likewise requests the client id and secretkey that is required to get to the administrations of the application door.

Step-3: After confirming the genuineness of the client, the application door gets to the remotehost for the benefit of the client to convey the packets.

5.) Next-generation firewalls:

A next-generation firewall is a network security device that providescapabilities beyond a traditional, stateful firewall. Some regular highlights of next-generatio firewall architectures contains application awareness and control, deep-packetinspection(checking the genuine contents of the data packet), TCP handshake checks, and integratedintrusion prevention that automatically stop attacks against your network.Anyway, which firewall design is the correct one for your business?The packet filter firewall or circuit-level firewall, which gives basic security that, has minimumperformance impact.The stateful firewall structure that combines the abilities of both of the past two choices, but has abetter performance impact.A proxy application firewall or next-generation firewall that provides better security in exchangefor extra cost and considerably higher performance impact?theperimeter and separating different resources on your system.
Having extra firewalls makes yoursystem harder to break by making extra resistance top to bottom that secludes distinctiver esources—influencing it so attackers to need to perform additional work to achieve the majorityof your most delicate data. The specific firewalls that you will need to utilize will rely upon the abilities of your system, important consistence necessities for your industry, and the assets youhave set up to deal with these firewalls.

Choosing and Configuring a Firewall :-

The Internet is a risky spot loaded up with a consistent blast of automated outputs that scrub theInternet for vulnerable targets. When distinguished, these vulnerable targets get diversity of attacks. A large number of the attackers have no clue that possesses the targets, and a definitive objective relies upon both the attacker and the kind of target. Choosing a suitable firewall shields your network system from the Internet and vice versa.

Important points to consider while Selecting a Firewall :-

Software and hardware firewall:

With the use of software firewalls, you introduce the program over a current Windows or Linux server, which at that point turns into your devoted firewall. Some of the examples of software firewall are Microsoft ISA Server orSmoothwall. Hardware firewalls are devices with their own operating systems and dedicated hardware. These are designed by Linksys, Cisco, Netgear, Watchguard, and SonicWall. To secure your individual system, software firewall is enough but at network level, hardware firewall is required. For high security, You need to use both hardware as well as software firewall since hardware firewall protects your system only in a LANor private network within an organization whereas software firewall protects the system outside the organization also.

Network size:

A firewall device should have sufficient processing power to deal with various connections with respect to size of your network.

Network topology:

The numbers of networks you have installed on your system need a level of protection. Suppose you have four networks, for example, one for the employees, one for the public access, and one for wireless access point and another for your servers. In this situation you require a firewall with four Ethernet ports and a port or your web connection. But the firewall you have selected has three ports then you could manage a second firewall or a managed switch to provide separation between these different kinds of subnetworks.

Threats to Firewall :-

Even when a firewall is installed, and updated with latest vulnerability patches, still it can create problems if the firewall's configuration settings create conflicts. This may degrade performance and may fail to provide security on your company's networkLess advanced firewalls may just check the packet's source of origin and destination before approving or denying a request therefore, it is easy for an attacker to get access on network's firewall.

Default password creates every security problem imaginable, including accountability issues when network events occur.

Firewalls can mitigate some types of DDoS attacks, they can still be overloaded by protocol attacks.

Attackers can get access to the firewall though unencrypted HTTP connections, as this may be exploited by an outsider connecting to the same network, in case of an open wireless network.

The host of software firewall should be updated on timely basis. Hardware firewalls

are costly and hard to upgrade.

REAL LIFE CASE STUDY :-

Steelcase is a **well-known furniture manufacturer.** Founded in 1912, Steelcase **provides critical user** research **and design solutions** for **commercial organizations worldwide. The** company has **more than 10,000 employees and** a global **distribution** network that includes company-owned and independent **dealers** as well as direct **customers.**

Steelcase is currently **building** a cloud-based e-commerce platform, requiring the team to **strengthen**

security **management.** The organization **hopes** to **make a significant difference** in Microsoft products, including **lack** of **control, external access, or crude rockets** for **access products.**

Steelcase's cloud security architect **Frank Stevens said: "Security management** and visibility **through** the cloud **platform is simple** and **inaccessible under our law."**

Cov. The company's use of the Fortinet FortiGate next-generation **firewall provides** additional security for its e-commerce platform. **Firewalls** help target and **block unwanted** traffic, **giving companies** a clearer **view** of customer behavior.

- It makes sense to use a firewall for both Microsoft and Amazon cloud service platforms: **doing** so **provides** the protection and economies of scale we **need because we don't** have to learn and **manage** two different **systems," said** Stuart Berman, **Global Security Architect, Steelcase .**

Conclusion :-

As the Internet becomes more a part of business, firewalls are becoming an important element of an overall network security policy. It plays an important role in computer system security against viruses, spyware, Trojans and other malwares attacks from outside of network. A good firewall provides full security to our network and system
without making any influence on the speed of computer system and network access. In order to provide security, one should always keep some points in mind: One should never install any software from suspected sources. Always download from the respected sites available on internet. Secure your firewall firstly and then use it to monitor all
information that we want to transfer over the internet. On each PC a firewall software must be installed else it will to become infected and very fast it will impact all PCs connected to that network.