FIREWALLS AND ITS SECURITY EFFECTIVENESS

RIDHDHI SANGANI[1] , AASHNA SHAH[2] AND NIR SHAH[3]
[1] NIRMA UNIVERSITY
[2]NIRMA UNIVERSITY
[3]NIRMA UNIVERSITY

ABSTRACT

A firewall is a software or a computer network security system that monitors and filters incoming and outgoing network traffic and restricts dangerous traffic in and out within a private network based on an organization's security policies. It is a virtual wall or a barrier between private and public internet. It prevents unauthorized access to a network. They are gated borders or gateways that govern the travel of permitted and prohibited web activities in a private network. This hardware-software functions by selectively blocking and allowing data packets. In this paper, we aim to summarise the working of firewalls, different types of firewalls, types of attacks that firewalls can prevent, and the evolution of firewall technology

KEYWORDS:

Firewall, Denial of services, Types of firewalls, Firewall technologies

I. BACKGROUND:

As network technology advances exponentially, so does the methodology of hackers and attackers. In this day and age, data privacy is of the utmost importance as everything is online. Firewalls play a crucial part in such protection and are vital to the network ecosystem. It is important to study the evolution of firewall technology to pinpoint significant advancements and improve upon existing features. The future of Cybersecurity is rich with many advancements on the horizon, but so is the future of threats to it. Firewalls must evolve faster than the threats they face to protect against the extremely dangerous threats which quite literally endanger the world. A minor unnoticed flaw in a firewall can mean the difference between life and death.

II. TERMS:

1. *FIREWALL*:
   They are security systems that inspects the incoming and outgoing traffic. It denies any unauthorized access to the private network from the external network. It protects the confidential data on one's system. Firewalls are collection of components between two networks that is immune to penetration. Firewall is like a frnce to a house; not allowing any trespasser to enter in the house.

2. *PACKET*:
   When a data is generated in application layer, it is relatively bigger and cannot be sent via transmission medium. Therefore, one big data is divided into many small packets of an efficient size for routing having the same source and destination address. These packets might be ordered or random according to the protocol used. For example, while any data unit is divided through TCP, TCP segments are formed which are ordered whereas when divided through UDP, UDP packets are formed and are unordered. These individual packets can be easily transmitted through transmission cables.

3. *TCP/IP*:
   TCP or transmission control protocol and IP or internet protocol are two main protocols which are responsible for transmission of data packets through any layer and through any system. TCP forms a connection with ther server of the destination network by sending a packet requesting for a connection. Server acknowledges it and forms a logical connection. This acknowledgment is referred by ACK. Client once again send the ACK. This connection establishment is known as Three-way TCP Connection Handshake. Once the connection is established data is transferred and after every packet is sent to the

server, client waits for the ACK of the received packet and then proceeds on to send next packet. Packets of whose ACK is not received are resent. This is the basis of TCP/IP protocol suite in every network system to establish logical connection.

4. *ACL:*
   ACL or Access Control List is the set of rules that helps in deciding whether to forward a packet or block it. ACL has predefined port numbers or IP addresses that are already blocked in the system. It follows the top to bottom approach; if the rule which is at the top gets hit then the bottom rules will be avoided.

III. WORKING PRINCIPLE:

A firewall is the gatekeeper of any system. It thoroughly inspects the incoming and outgoing traffic to ensure that no malicious packets have entered or left the system. It creates a safety network barrier between a private and public network and eradicates any possibility of penetration that can cause harm to the system. It protects the system from unauthorized intrusion and makes it less susceptible to cyberattacks.
A firewall filters the incoming data and determines by its value whether that particular address is allowed in the network or not. A firewall works on a set of rules (ACL) based on the details of the network packet. Only trusted network's traffic (IP Address) is allowed to enter the system. These rules either allow or denies permission.

These rules can be based on the following:

1. *IP addresses:*
   Every firewall has Blacklisted IP addresses which is the list of IP addresses that pose any threat to the network and hence are needed to be blocked. It filters out malicious IP addresses from accessing the network.

2. *Domain names:*
   Some domain names have low reputations and a very high risk of spreading harmful requests from their domains. Moreover, there might be many domains that can hinder the efficiency of the organization. Hence, all the requests by these domain names are restricted. For instance, youtube.com might be blocked by many organizations' firewalls so employees do not have access to that and cannot waste their time.

3. *Protocols:*
   Certain protocols have a very lousy connection and are blocked—for example, Transfer Control Protocol (TCP) and User Datagram Protocol (UDP). TCP forms the logical connection between source and destination and is more secure. At the same time, UDP does not form any logical connection and are considered unreliable. Due to no handshake between the source and destination when connected through UDP it is advisable to block it.

4. *Port numbers:*
   Port numbers are 16-bit numbers that are a part of addressing information that helps to identify a particular application or service on the system. Various protocols have various port numbers through which two system interacts. The firewall restricts port numbers that gain unauthorized access.
   For instance, to have remote access to any system out there computers use a pre-defined port of RDP (Remote Desktop Protocol) which is 3389. When two systems try to form a logical connection via RDP, the source connects to port number 3389 of the target system. A firewall helps prevent such RDP attacks by setting ACL policies accordingly. In this scenario, one can create a policy where no system outside the network can have the access to the systems in the organization by blocking incoming requests for the port number 3389.

PERMISSION	IP ADDRESS	PROTOCOL	DESTINATION	PORT
ALLOW	ANY	TCP	ANY	80
ALLOW	ANY	TCP	ANY	25
ALLOW	ANY	TCP	ANY	110
DENY	ANY	UDP	ANY	23
DENY	ANY	TCP	ANY	3389

Port number 80: HyperText Transfer Protocol
Port number 25: Simple Mail Transfer Protocol
Port number 110: Post Office Protocol
Port number 23: Telnet
Port Number 3389: Remote Desktop Protocol
An organization can allow 80 and 443 for normal web accessibilities but blocks 23 and 3389 to deny any remote access.

For enhanced security reasons, two types of firewalls are generally used (Fig 1):

1. Host-based firewall: A software firewall protects only one particular computer.
2. Network-based firewall: The combination of hardware and software firewall. It protects the entire system.

For the maximum safety, both firewalls are installed in the system.
There are chances that when a large number of malicious requests are sent to the network firewall they might penetrate through the network and allow malicious requests. These malicious requests can then be identified by the host firewall and block that request.

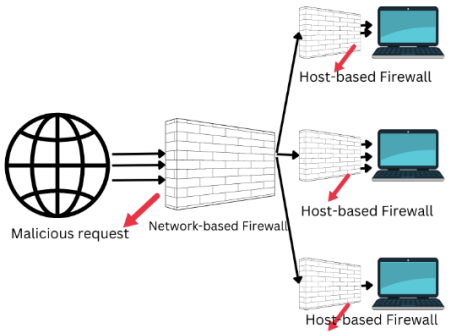

Figure 1: Even if any malicious file is allowed by network based firewall then it will be blocked by host-based firewall. Thus, providing an additional layer of security

IV. TYPES OF FIREWALLS

1. *Packet Filtering Firewall*
   It is present in the network layer of the OSI model. It checks each and every packet before allowing it into the network. Packet filtering firewall decides whether to forward or block the packet according to the pre-defined set of rules. It checks source and destination addresses, source and destination port numbers, and the protocols used. It is essential to configure the firewall rightly, or else important messages will be blocked by the firewall.
   Advantages: It is easy to implement and relatively faster than all other firewalls, as it only checks specific essential pieces of information.
   Disadvantages: it only checks the addresses and not the payload. Payload might have malicious files in them.

2. *Application Layer Firewall*
   It is present in the application layer. It filters the traffic between two applications of the system. Apart from checking the addresses and protocols it also checks the actual data(payload) and blocks any harmful files. These firewalls are generally installed as an additional layer of security.

Advantages: It has high impact on network performance.
Disadvantages: It is a complex firewall and has less transparency.

3. *Circuit Level Gateway*
   It is present in the session layer of the OSI model. It confirms that the logical connection between the two systems' transport layers is protected. It helps in providing security between TCP and UDP using the connection.
   Advantages: These firewalls are cheap and straightforward to implement.
   Disadvantages: It does not offer protection against data leakage from devices. Moreover, it needs regular and frequent updates.

4. *Stateful Multi-Layer Inspection Firewall*
   It combines the functionalities of packet filtering firewall which is examining each and every packet and circuit level gateways which is logical handshake between transport layers. It examines all seven layers of the OSI model.
   Advantages: It is an additional security level provided to any network.
   Disadvantages: It has comparatively slow transfer rate. They cannot prevent application-layer attacks.

5. *Next-Generation Firewalls*
   As defined by Gartner, Next-Generation firewalls are "deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall." In a more straightforward sense, it is the combination of working of other firewalls according to the need of the organization.
   Advantages: They provide high levels of security to the network and examines payload too.
   Disadvantages: It is difficult to design and implement.

V. TYPES OF ATTACKS:

1. *Port Scan*
   Attackers use this attack to detect weak points in a network. It can reveal information like whether active security devices are being used by the network, which services are running, which services require authentication, etc.

   How it works**:** There are various techniques to conduct a port scan. The basic idea is to send packets to destination port numbers. For example, an XMAS scan is a discrete attack method where the attacker sends packets to a port, and if it is closed, the scanner gets a response. In a Vanilla scan, the attacker tries to connect to all 65,536 ports at the same time. It is accurate but easily detected. Firewalls should notice this activity because it's unusual for a remote computer to connect to more than a few ports at one time. (Grimes and Posey)

2. *Denial of Service (DoS)*
   This attack is the main attack used for denying service. A network will be so overwhelmed with traffic that it won't be able to process legitimate requests for service, or allow legitimate traffic to reach the service (York #)(Fig. 2). This attack makes the network unable to extend its resources to users. There are several types of DoS attacks.

   Distributed DoS attack: This attack uses multiple systems to flood the bandwidth or resources of the affected system. Multiple attacking systems are more difficult to turn off as they are difficult to track. It is also difficult to figure out which traffic is legitimate and which is part of the attack since multiple sources are attacking at the same time.

   Application layer DDoS attack: Sometimes referred to as layer 7 DDoS attack, it is a type of attack that targets the application layer process. It can affect services like search functions on

websites, retrieval of information, transactions and access to databases. It is often used to distract from security breaches.

Advanced Persistent DoS attack: These attacks can go on for weeks, with the longest known attack known to last for 38 days and involving 50,000 terabits of malicious traffic (Ilascu). Attackers can tactically switch between various victims to create diversions and evade countermeasures, but ultimately focus the force of their attack on a single victim. They are characterised by their large computing capacity, persistence, simultaneous attacks able to operate at multiple layers, and tactical execution.

DoS as a service: Vendor provided DoS softwares are sold to buyers as stress testing tools. They are used to perform unauthorised DoS attacks by those technically unable to. They are also called Stresser Services, and are able to produce traffic in the range of 5 to 50 Gigabits/s. (Mubarakali et al. 1580–1592)

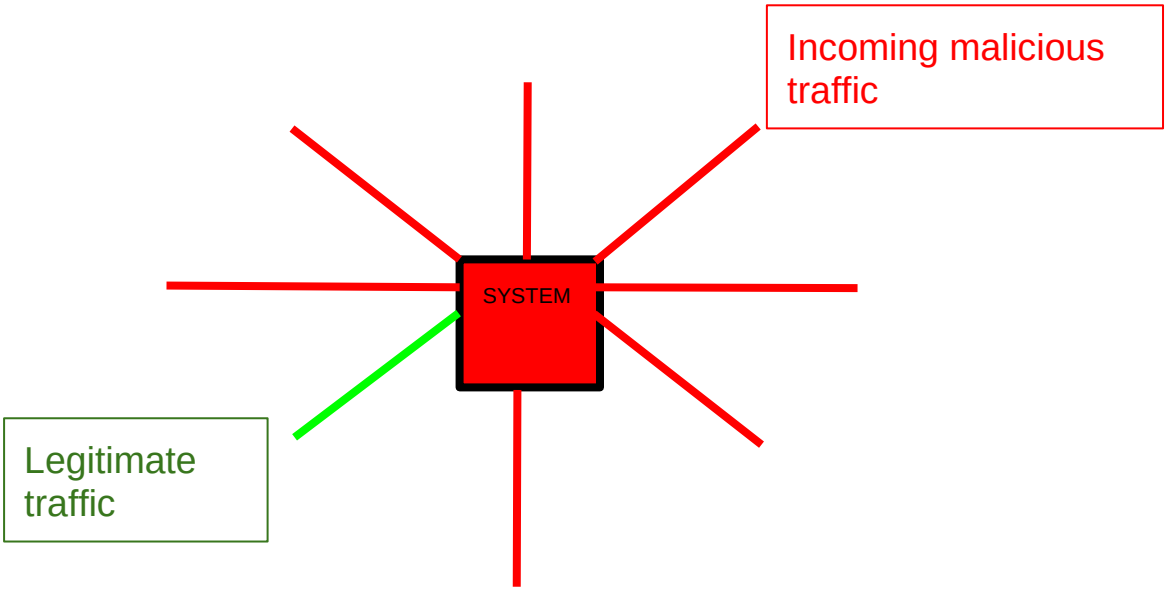

Figure 2: when a firewall is overwhelmed by too many malicious requests than there are chances that legitimate traffic can also be blocked.

3. *Spoofing attack:*
   The basic idea behind a spoofing attack is the attacker identifies as another by falsifying data (Fig. 3).

   IP address spoofing: Packets are sent to the receiver with a false IP address, which enables them to pass themselves off as another computer system. This type of spoofing is used in "Man-in-the-middle" attacks.

   DNS spoofing: This attack uses altered DNS records to direct traffic to fraudulent websites impersonating the intended destination. Users enter their details unknowingly into the fake website and unknowingly provide attackers with confidential information. These malicious websites are also used to install worms and viruses into the user's system.

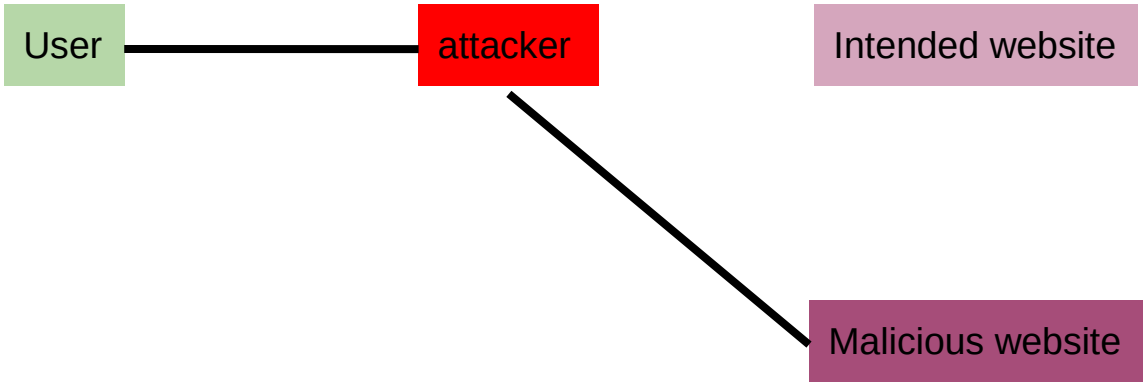

Figure 3:User is misguided to a malicious website

4. *Mixed Threat attack:*
   These attacks use several different methods to infiltrate a computer system. They are based on multiple single attacks, and are thus much more difficult to detect and protect against. While firewalls are effective to an extent against these attacks, once the attack is in the system it is very difficult to protect against. Mixed Threat attacks were utilised by the computer worms Nimda and Code Red.

5. *Tunnelling protocol attack:*
   For information flow to successfully occur over the internet, protocols are used. These protocols divide the message into two parts, one containing the actual message and the other part containing rules of transmission such as the address of the destination. This type of attack encloses a separate data packet in the datagram transmitted, containing a different communication protocol. This action creates a sort of "tunnel" which is then used to transmit data securely. Attackers can send protocols blocked by firewalls through this attack, or in recent cases malware as well.

6. *Trojan Attack:*
   This attack derives its name from the infamous trojan horse that defeated the Troys. It is a malicious program disguised as a legitimate download. Once downloaded, it opens up the entire system to many different kinds of attacks. A few types of Trojan attacks are:

   Banker Trojan: It allows attackers access to the banking accounts of the user and exposes personal financial and banking information.

   Backdoor Trojan: Creates a backdoor in the system and allows the attacker remote control. The attacker can then use the system as he sees fit and steal data. It is commonly used to create a zombie computer which sends trojan horses to other systems.

   Ransom Trojan: This attack can block data on a device and hold it for a "ransom", which the user will have to pay to access the data again.

   Downloader Trojan: This attack enables the attacker to install other malicious software onto a system to further compromise its security.

VI. LIMITATIONS:

1. *How it verifies incoming data*
   Our computer's operating system and firewall have a list of trusted programs and previously allowed programs. When a data packet arrives at the firewall, it checks whether the incoming data packet belongs to an application in the list of reputed programs. If it does, the firewall allows the data packet to pass through the computer. Hackers can easily exploit this by creating fake data packets containing trusted IP addresses to hack a computer or a computer network.

2. *Insider's Intrusion*
   Firewalls cannot enforce password policy or prevent misuse of passwords. Password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.

3. *Direct Internet Traffic*
   Any security provided by the firewall is successful only when it ensures one exit gate for the network. Presence of more than one exit gate increases the probability of an attack on the device.

4. *Firewalls trust on trusted networks*
   It cannot ensure protection against what has been authorized. In other words, it cannot protect from authorized users with malicious intentions. They can easily pass through the firewall security and do malicious activity.

5. *No protection against Masquerades*
   Firewalls cannot stop users from accessing the data or information from malicious websites, making them vulnerable to internal threats or attacks. It cannot stop internal users from accessing websites with malicious code, making user education critical.

6. *No anti-virus or anti-malware properties*
   It does not provide additional protection for our computer. Suppose some harmful files have been introduced to our computer system from some networking channels like email. A firewall cannot analyse the signature or content of any packet. Instead, it only analyses the network from where it has arrived.

VII. DISADVANTAGES

1. *Diminishing a system's performance*
   Firewall constitutes of a packet filtering software that is responsible for degrading a system's performance. This is because examining each and every packet wearisome and exhausting task.

2. *Laborious to Set-up*
   Firewall is difficult to maintain, configure and uninstall completely from a system.

3. *False sense of security*
   It somewhere encourages user to not maintain security at machine level by lending a false sense of security. In case where a network firewall fails or is improperly configured, the results could be disastrous.

VIII. ADVANCEMENTS IN FIREWALLS

One of the significant shifts in firewalls has been how they inspect traffic and allow IT teams to provide more adaptive policy rules. This essential advancement has provided better security for current user access policies, especially those related to applications, resulting in the granularity of access control.

1. *Cloud-based firewalls*
   This advancement was possible because of FwaaS(Firewall as a service), which is entirely cloud-based. It provides a layer of firewall protection irrespective of the number of links added to the network or how remotely the network is located. It makes firewall reliable, cost-effective, and cover a wider distance. It enables to widen the scope of constant improvement by automatic updation of the firewall.

2. *Lower Costs*
   The tools required to create, maintain and update firewalls are now becoming open-source and accessible. Firewall management is now becoming more instinctive because of better user interfaces.

Overall, less time is spent on managing them and less money is spent on acquiring the accessories mandatory to maintain them.

3. *Higher throughput speeds*
   Under normal circumstances, the time elapsed between requesting and receiving data increases drastically as any firewall takes action on data packets before passing them along. Users would not tolerate a slowdown because the firewall needs extra time to kick in. Therefore, the throughput speeds are getting faster in firewalls since the internet speeds are getting faster. Modern advanced firewalls process faster and reduce the time lag in retrieving information.

4. *Awareness of applications and users*
   Firewalls now provide a wider berth of coverage to protect the systems in terms of blocking and allowing access to data. This particular functionality has become indispensable for thousands of users.

5. *Third-party and multi-factor authentication systems*
   Firewalls now use multiple protocols to ensure the validity of a given user. Newer firewalls have more advanced means of authenticating: they partner with third-party authenticating systems to allow and deny access to information.

IX. CONCLUSION:

A firewall is an entry point of any system and hence is considered as a vital part of computer security against viruses, spyware, Trojans, and other malware, as well as between direct malicious attacks from outside the network and outside. Firewalls secure inner network from any unauthorized access, therefore, it is equally important to ensure that firewalls are immune to attacks.

Apart from securing the network it is also mandatory that it should not affect the transmission speed as it could lead to many delays and errors in the file and can weaken the efficiency and effectiveness of the network. To avoid any loopholes, firewalls should be regularly updated and upgraded.

REFERENCES:

1. Grimes, Roger, and Brien Posey. “External Firewall Attacks.” ITPro Today, https://www.itprotoday.com/security/external-firewall-attacks. Accessed 9 November 2022.
2. Ilascu, Ionut. “38-Day Long DDoS Siege Amounts to Over 50 Petabits in Bad Traffic.” Softpedia News, 21 August 2014, https://news.softpedia.com/news/38-Day-Long-DDoS-Siege-Amounts-to-Over-50-Petabits-in-Bad-Traffic-455722.shtml. Accessed 9 November 2022.
3. Mubarakali, Azath, et al. “Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems.” Computational Intelligence, 2020.
4. York, Dan. Seven Deadliest Unified Communications Attacks. Elsevier Science, 2010.
5. Ali, Firkhan Ali Bin Hamid. "A study of technology in firewall system." 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA). IEEE, 2011.
6. Tharaka, S. C., et al. "High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies." International Journal of Scientific and Research Publications 6.4 (2016): 504-508.
7. He, Xinzhou. "Research on Computer Network Security Based on Firewall Technology." Journal of Physics: Conference Series. Vol. 1744. No. 4. IOP Publishing, 2021.
8. Rengaraju, Perumalraja, V. Raja Ramanan, and Chung-Horng Lung. "Detection and prevention of DoS attacks in Software-Defined Cloud networks." 2017 IEEE Conference on Dependable and Secure Computing. IEEE, 2017.
9. Krit, Salah-ddine, and Elbachir Haimoud. "Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically." 2017 International Conference on Engineering & MIS (ICEMIS). IEEE, 2017.
10. Pawar, Mohan V., and J. Anuradha. "Network security and types of attacks in network." Procedia Computer Science 48 (2015): 503-506.

11. A review paper on computer firewall by Damodharan and Prabhat Kumar Srivastava
12. What is a Next Generation Firewall? Learn about the differences between .... https://digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls
13. Denial-of-service attack - Wikipedia. https://en.wikipedia.org/wiki/Denial-of-service_attack
14. Network Security First-Step: Firewalls - Cisco Press. https://www.ciscopress.com/articles/article.asp?p=1823359&seqNum=7