FIREWALL

For specific organizations, Internet access is no longer a choice. Although internet connectivity allows an entity with advantages, it helps the exterior community to enter and communicate with local network infrastructure. This establishes the organization's hazard. While any device and server may be fitted with robust, secure functionalities like intrusion prevention on the premises network, this solution is not realistic. The option is the firewall, which is commonly acknowledged.

A firewall is a term used for a network security system that protects unauthorized access to or from a network. A set of security rules are defined, and following this set, it tracks incoming and outgoing traffic and then allows or blocks communication packets. The firewall just works like a barrier in between the incoming traffic and external sources. It secures mischievous traffic that includes unauthorized access from hackers and viruses. A firewall is often suitable for obtaining virtual access to a private network via secure authentication credentials and certificates to restrict access to clients' devices and networks.

Firewall Working

Firewalls are full of pre-set rules that carefully look after the incoming traffic. Firewalls filter the traffic that approaches from unsecured sources. Firewalls also block the specific traffic coming from suspicious sources. The firewall functioning aims to prevent the system attached with the network from attacks.

The firewall guards are residing at the computer's entry point known as "ports," which are the points where data communication occurs with the other devices. In computer networking, internet protocol (IP) is just like a house number in an address, and a port number can be considered a room number in the house's address. With this example, we can clear that we allow only trusted people in the house (destination address) and only allowed people to visit the room (destination ports). However, the owner has access to visit any room of the house (any port) while guests and children can access a defined list of rooms (specific ports).

Types of Firewall:

Firewalls are categorized into eight main types concerning their general structure and operation behaviour. All the types are listed and briefly described below.

1. Packet Filtering
2. Circuit Level Gateways
3. Stateful Inspection
4. Application Level Firewalls
5. Next Generation
6. Software Firewalls
7. Hardware Firewalls
8. Cloud Firewalls

1. Packet Filtering:

As the “simple” and “earliest” firewall architecture type, packet-filtering gateways essentially create a barrier at a communication router or switch. The gateway performs a fast analysis of the data packets passing through the router without manipulating the packet to determine its structure, evaluating data such as the destination and source IP address, packet sorting, port number, and other surface-level information. If the data packet does not fulfil the requirements it will be dropped in that case.

With these gateways, what’s odd is that they are not a much stronger cause. This means they do not have an overwhelming influence on the performance of the system and are relatively required. However they are also relatively simple to bypass, like firewalls with more efficient inspection characteristics.

2. Circuit Level Gateways:

Circuit-level gateways serve as a key gateway group by testing the consensus of the transmission control protocol (TCP) that is designed to allow or deny data easily and effectively without needing considerable computational power. This quest for TCP contact is intended to guarantee that the packet is from a valid link.

Though extremely resource-efficient, these gateways don’t test the data packet itself. So if a packet is harmful, but had the correct TCP arrangement, it must pass through it positively. Therefore, circuit-level firewalls are not adequate to secure the entity alone.

3.Stateful Inspection:

The above two firewall categories and TCP protection are combined to create a degree of protection stronger than both of the previous two kinds. However, these defence technologies also place a great deal of pressure on processing resources. This will slow down the distribution of legitimate packets, in comparison to the other alternatives.

4. Application Level Firewall:

The type of filter is present between the clients' network and the source where incoming traffic will be filtered. The firewall operates at the application layer. That is why the type of firewall is known as an application-level gateway. The functionality of such kinds of firewalls can be achieved through clouds or proxy devices. Proxies develop a connection with the traffic source and evaluate the data packets, then dispatch each packet after verification to the destination. Stateful inspection firewall evaluates the packets in the same manner that monitors both the data packets along with TCP protocol.

5. Next Generation Gateway:

The recent or advanced products related to gateways are declared as next-generation products. However, no parameters exist to evaluate whether a firewall belongs to the next-gen or not. The next generation prominent features are given below.

1. Deep Data Packet Inspection
2. TCP Handshake Evaluation
3. Surface-Level Packet Inspection

The next generation's firewalls may also involve other innovations such as IPSs, which automatically protect threats against your network. It is necessary to learn about next-generation firewalls' capabilities as there is no unique definition of such firewalls.

6. Software Firewalls:

On a clients' system, a software firewall is configured that prevents the specific unit. This facilitates coordination with internal security. It may be customized, giving clients more flexibility about its functionality and security characteristics, including restricting links to some network websites. Since software firewalls are simpler to mount, many homes and SMB clients prefer them. Whereas application layer gateways perform analysis in deep layers to evaluate that the data is real, there is nothing like malware.

7. Hardware Firewalls:

A unique physical device is used to secure the whole network from an unsecured environment. Although it is possible to buy a stand-alone tool, hardware firewall systems are often placed between the computer network and the internet. This system detects data packets as they are exchanged and then blocks or exchanges the data according to pre-set guidelines. To mount and commit maintenance and control; subsequently, hardware firewalls need specialized IT expertise. Because of this hardware, more prominent organizations usually employ firewalls where privacy is a significant concern.

8. Cloud Firewalls:

In the advanced era of technology, the cloud provides services for firewall functionality. Such firewalls have similar patterns as compared with the application or proxy firewalls in many aspects. Cloud servicing is mostly used in application-level gateways. Moreover, the cloud-based gateways are easy to implement on the organizational level. The requirement of cloud servicing gateways can be enhanced as the traffic load increases. Just like hardware gateways, cloud firewalls provide security at the perimeter level.

Firewall, a tool, is also a part of operating systems (OS). All the OS of Microsoft advanced than XP contains Windows Firewall, a freeware that monitors suspicious activities. Moreover, it has the power to detect and block viruses and hackers that perform unauthorized activities.

Firewall Characteristics:

Major characteristics related to firewall protection are described below.

1. Various protection levels
2. Wireless network (Wi-fi) Protection
3. Internet and network access
4. Blockage against unauthorized access
5. Protection against malware
6. Provide access only to valid data packets
7. Provision of different configurations
8. Provision of numerous security policies
9. Allowing to pass authorized traffic that fulfils a set of rules
10. Firewall functions like an immune system for malware and unauthorized access; therefore, it ensures a secure system and an OS.

Firewall Security Techniques:

The firewall employs four different techniques for controlling access and ensuring the security policy for web clients. A brief detail of the related security policy is given below.

1. Service Control
2. Direction Control
3. User Control
4. Behaviour Control

1. Service Control:
Service control shall specify the form of internet services available, inbound, or outbound. It is enabled to funnel data using IP address and TCP port, have a proxy application that collects and translates each service request before transmitting it or host the web server itself, like web or mail.

2. Direction Control:
The control defines the path in which a complex service request can be launched and passed across the firewall.

3. User Control:
It regulates access to a program that the customer attempts to enter.

4. Behaviour Control:
It regulates how specific services need to be employed.

Firewall Capabilities:

A firewall uniquely identifies the level of congestion, which prevents unwanted clients off the secure network, forbids the entry or leave of possibly compromised services, and defends them from different forms of IP spoofing and networking assaults.

A firewall includes a space for the protection of events related to security. Assessments and warnings on the firewall framework may be introduced. A

firewall is a suitable interface for many operations not relevant to security. A firewall will act as an IPsec framework.

Firewall Categories:

Firewalls are classified into eight different categories. A list of all the categories and their functionality is described below.

1. Stateless Firewall
2. Stateful Firewall
3. Packet-filtering Firewall
4. Proxy Firewall
5. Address Translation Firewall
6. Host-based Firewall
7. Transparent Firewall
8. Hybrid Firewall

1. Stateless Firewall:

Early firewalls are developed to examine packets to confirm if they are fulfilling standards declared in the firewall, with the ability to move forward or block packets. This method of packet filtering is referred to as stateless filtering. Each packet is screened based on specific characteristics in this kind of firewall, like ACLs screen packages.

2. Stateful Firewall:

The idea of a stateful firewall was proposed in 1989 by AT&T Bell Labs. Data flows through the firewall as the information is stored in it. This category of firewall decides if a packet is part of an ongoing data flow. The support minimizes DoS attacks utilizing secure connections across a networking system. This firewall facilitates the features for dynamic packet filtering. The stateful firewall performs functionality on the OSI model layers. They tend to monitor the networking traffic on OSI layers 4 & 5.

3. Packet Filtering Firewall:

Packet filtering firewalls can filter the data packets at OSI layers 3 & 4. The firewall category employs an access control list (ACL) for monitoring the traffic; either it should be permitted or denied based on the IP address of sender and receiver, their port number, and kind of packet. These firewalls are commonly composed of a router firewall.

4. Proxy Firewall:
The proxy or application firewall monitors and filters the data at OSI layers 3-7. Mostly a software program is used to manage and filter this category of the firewall.

5. Address-Translation Firewall:
A firewall form that exceeds the number of accessible IP and disguises a developed address network.

6. Host-based Firewall:
In this category of firewall, devices have a firewall program and operationally performing functionality on the device.

7. Transparent Firewall:
Transparent firewalls monitor the traffic at layer two and do not perform router hop for the connected systems. It performs the filtering of IP traffic among network interfaces.

8. Hybrid Firewall:
The hybrid firewalls are formed by combining different categories of the firewall.

Firewall Advantages:

Firewalls perform initial protection against potential attacks, ransomware, and hackers attempting to reach the details and networks. The ordinary benefits of the firewalls are as given below.

1. Keeps a close look on network traffic:
All the advantages of firewall protection commence with network traffic monitoring. Information from and in clients' applications provides ways to disrupt the activities. Firewalls use pre-set guidelines and filters to retain the networks secure by tracking and evaluating network traffic. Users should control the security rate with a skilled IT team depending on the details of the data in and out from the firewall.

2. Significant obstacle against viruses:
Nobody will close the digital activities quicker and more resonantly than an intrusion by viruses. Thousands of potential attacks are developed daily; web users must maintain and protect their systems from such attacks. The potential to

monitor the access points on the device and avoid malware attacks is one of the most apparent advantages of firewalls. Depending on the type of malware, the risk to the devices can be enormously considerable.

3. Secures from Hacking:

With the evolution of technology, firms' patterns are shifting further into digital activities, but criminals and spammers are also moving towards digital trends to perform harmful jobs. Firewalls have become ever more relevant with increasing computer fraud and offenders retaining rehabilitation systems because they prohibit hackers from obtaining unwanted access.

4. Prevents from Spywares:

Quite an advantage in a data-driven environment is to avoid spyware from having access and coming through the networks. When networks get increasingly sophisticated and robust, hackers often utilize entrances to achieve greater access to the systems. Unneeded individuals have access to spyware and malware—programs to hack the networks, manipulate the machines, and steal the data—is one of the most popular methods. Firewalls act as a significant barrier to these harmful systems.

5. Promotion of Privacy:

The promotion of privacy is an overall advantage. Acting efficiently and effectively to maintain the data and consumers' information secure, we create a privacy framework that the users will trust. Nobody prefers to steal their private details, mainly if this evidence should have been taken to avoid intrusion. In comparison, improved data security technologies will give enterprises and consumers a strategic edge and sales point. The profit improves the sensitivity of the businesses' data.

Firewall Disadvantages:

Orthodox solutions, nevertheless, have weaknesses and disadvantages. These disadvantages can not only risk the defence but also place an unnecessary burden on the assets. A few of the common disadvantages of firewalls are discussed below.

1. Limitation related to awareness about the application:

Traditional firewalls are not as deep as NGFWs that permit the consumer to monitor which programs are employed in the network and empower the

opportunity. The capability to monitor connectivity to this depth is not possible with a conventional firewall.

2. Speed is a challenge:

Often conventional firewalls establish a data inspection model, which may consume the users' resources, including speed, time, and budget. This is not suitable with activities that plan to grow, incorporate new regulations, procedures, and safety protocols.

3. Logistical Matters:

Most conventional firewalls cannot be tailored to the changing element of enterprise applications and activities. They can be glitchy, need extensive supervision and servicing, and have trouble adjusting to cloud context.

4. Deficiency of Evolution Capabilities:

The security threat ecosystem is continually evolving, and regular new threats emerge. It is almost difficult to keep up to date to facilitate successful assistance and security without seriously restricting the teams or company capability. Rebooting new implementations for all platforms is disruptive, time-consuming, and introduces vulnerability possibilities that are out of date.

Summary & Facts:

The firewall is located between the network and the device to provide a protected connection and create an additional defence barrier. This boundary aims to secure the network from Internet attacks and give a single stumbling block for protection and investigation. The firewall may be a single device or a group of multiple cooperating systems for a firewall.

How does the firewall work?

Firewalls are full of pre-set rules that carefully look after the incoming traffic. Firewalls filter the traffic that approaches from unsecured sources. Firewalls also block specific traffic coming from suspicious sources.

Enlist the types of firewalls?

1. Packet Filtering
2. Circuit Level Gateways
3. Stateful Inspection
4. Application Level Firewalls
5. Next Generation
6. Software Firewalls
7. Hardware Firewalls
8. Cloud Firewalls

What are the critical characteristics of a firewall?

1. Various protection levels
2. Wireless network (Wi-fi) Protection
3. Internet and network access
4. Blockage against unauthorized access
5. Protection against malware
6. Provide access only to valid data packets
7. Provision of different configurations
8. Provision of numerous security policies
9. Allowing to pass authorized traffic that fulfils a set of rules
10. Firewall functions like an immune system for malware and unauthorized access; therefore, it ensures a secure system along with an OS.

Name the four security techniques used in the firewall?

1. Service Control
2. Direction Control
3. User Control
4. Behaviour Control

Write down all the categories of the firewall?

1. Stateless Firewall
2. Stateful Firewall
3. Packet-filtering Firewall
4. Proxy Firewall
5. Address Translation Firewall
6. Host-based Firewall
7. Transparent Firewall
8. Hybrid Firewall

What are the significant advantages of firewalls? Write the major points related to advantages.

1. Keeps a close look on network traffic
2. Significant obstacle against viruses
3. Secures from Hacking
4. Prevents from Spywares
5. Promotion of Privacy

What are the disadvantages of firewalls? Write the major points related to the disadvantages.

1. Limitation related to awareness about the application
2. Speed is a challenge
3. Logistical Matters
4. Deficiency of Evolution Capabilities

References:

1. https://www.webopedia.com/TERM/F/firewall.html
2. https://www.forcepoint.com/cyber-edu/firewall
3. https://www.compuquip.com/blog/the-different-types-of-firewall-architectures
4. https://www.pandasecurity.com/homeusers/downloads/docs/product/help/up/2010/en/530.htm
5. http://www.brainkart.com/article/Firewalls–design-principles,-characteristics,-Limitations,-Types_8372/
6. https://www.orbit-computer-solutions.com/firewall-explained/
7. https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-general-config/intro-fw.pdf
8. https://www.fortinet.com/it/resources/cyberglossary/firewall-benefits–the-importance-of-firewall-security