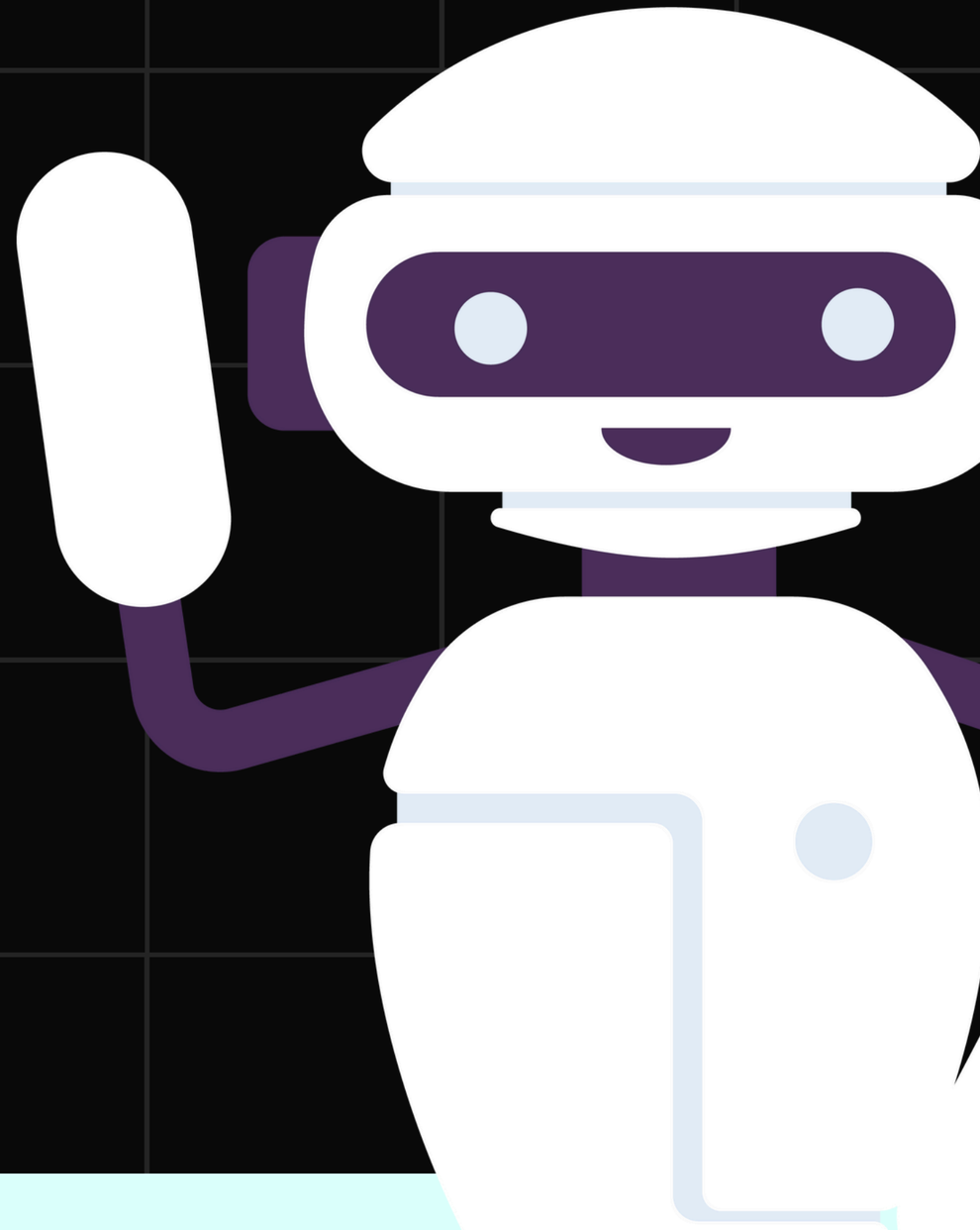
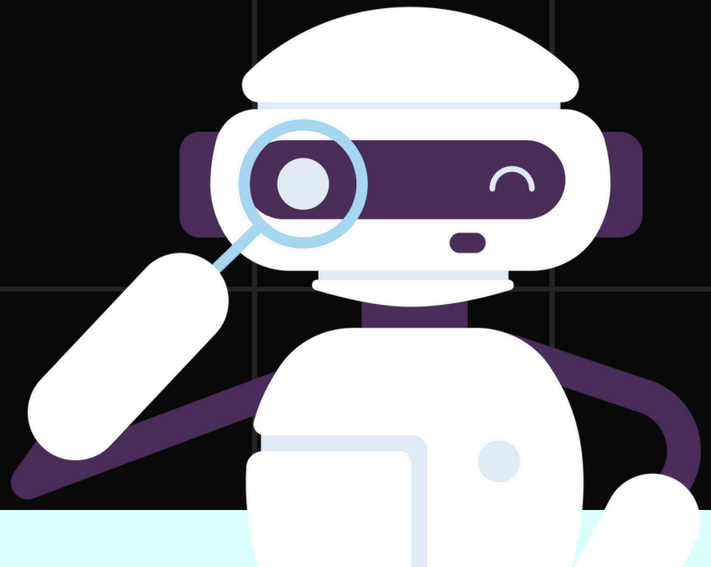
FIREWALL



BY D081 ASHIKA ASHOK
D086 AQUILA ELDHO
D090 SIMRAN GUPTA
D100 KAVYA PATEL

WHAT IS FIREWALL ?

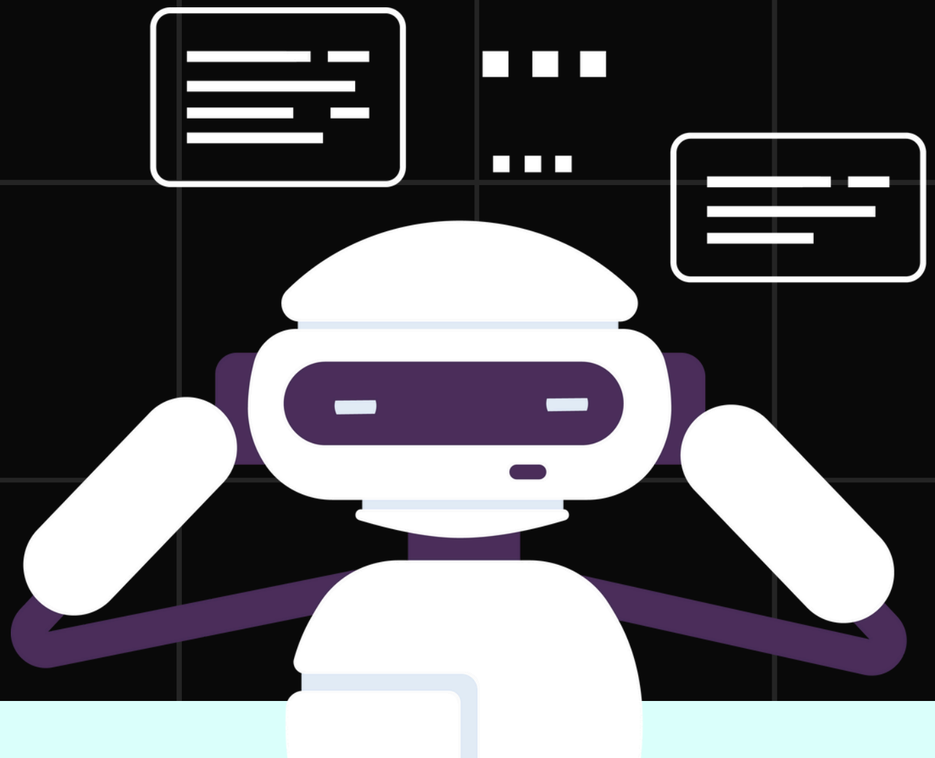


A Firewall is like a digital security guard that sits between your private network (like your home or office network) and the vast internet. Its job is to monitor and control incoming and outgoing network traffic based on predetermined security rules.

HOW DOES IT WORK?

When data tries to enter or leave your network, the firewall checks it against these rules. If the data meets the criteria (such as being from a trusted source or matching an allowed service), it's allowed to pass through. If not, the firewall blocks it, protecting your network from malicious attacks, viruses, and unauthorized access.

IMPORTANCE OF FIREWALL



Protection Against Cyberattacks:

They block unauthorized access and prevent threats like viruses and malware from entering networks.

Controlling Access:

They regulate network traffic based on security rules, allowing only authorized users and devices to connect.

Safeguarding Data:

Firewalls ensure the security of personal and sensitive information, meeting regulatory requirements and preventing data breaches.

Monitoring and Response:

Firewalls provide real-time monitoring, alerting administrators to suspicious activities and enabling swift response to potential threats

CHARACTERISTICS OF FIREWALL

1. Traffic Filtering

The primary function of any firewall is filtering incoming and outgoing network traffic based on a defined policy.

2. Access Control

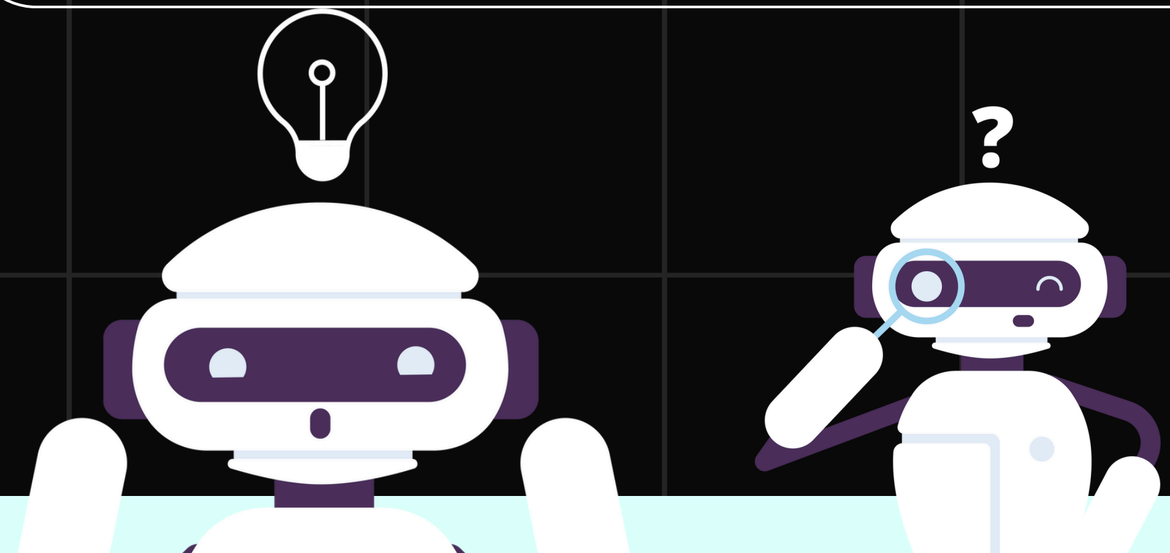
Firewalls govern access between network zones by allowing specific types of traffic to pass while explicitly denying all other traffic.

3. Multi-Purpose

A firewall has many functions other than security purposes. It configures domain names and Internet Protocol (IP) addresses.

4. Security Platform

It provides a platform from which any alert to the issue related to security or fixing issues can be accessed. All the queries related to security can be kept under check from one place in a system or network.



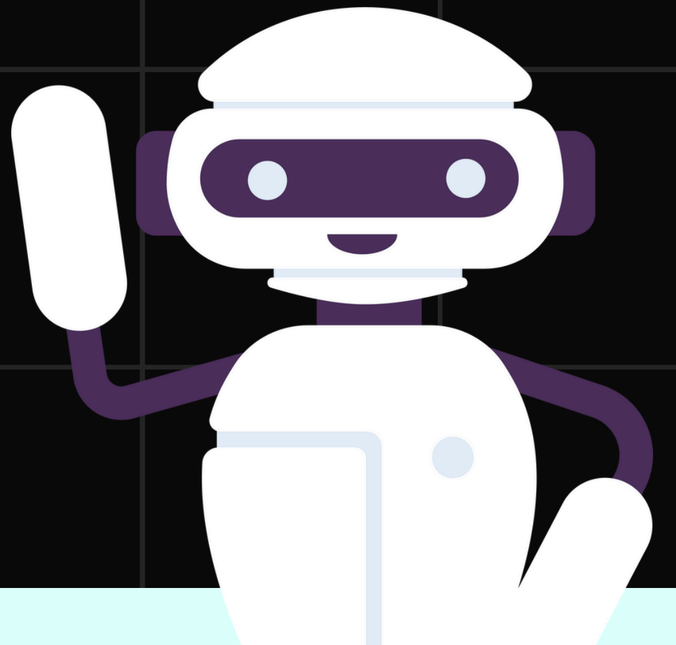
LIMITATIONS OF FIREWALL

- COMPLEXITY : Configuring firewalls involves setting rules and policies to allow or deny traffic based on IP addresses, ports, protocols, and other criteria, which can be complex in large networks and require a deep understanding of network architecture and security requirements.

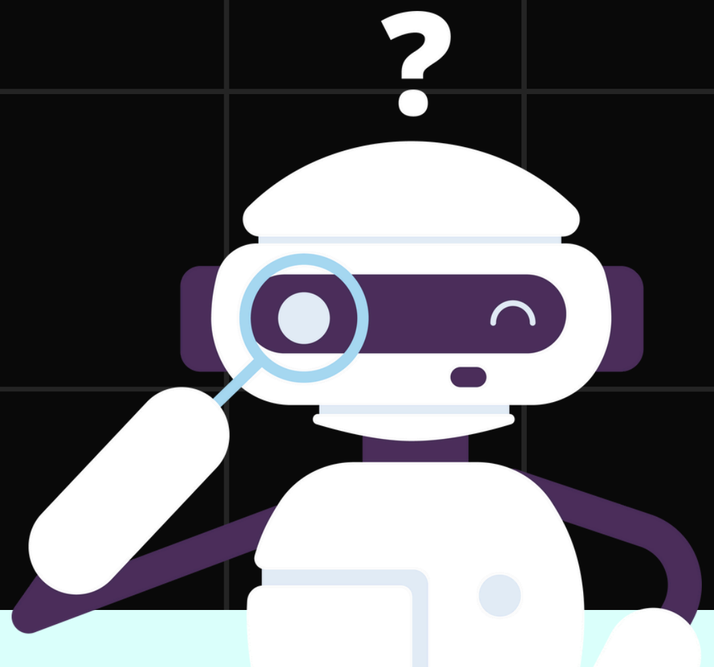
- PERFORMANCE IMPACT : High traffic volumes can overload a firewall, reducing efficiency and potentially slowing down the network, especially for organizations with heavy data flow or real-time applications.

- INTERNAL ATTACKS : Firewalls are primarily designed to protect against external threats. However, employees or other insiders with legitimate access can still cause harm, such as stealing sensitive data or introducing malware.

- COST : Regular updates, monitoring, and management require continuous investment in time and resources, and organizations may need specialized personnel for effective management.

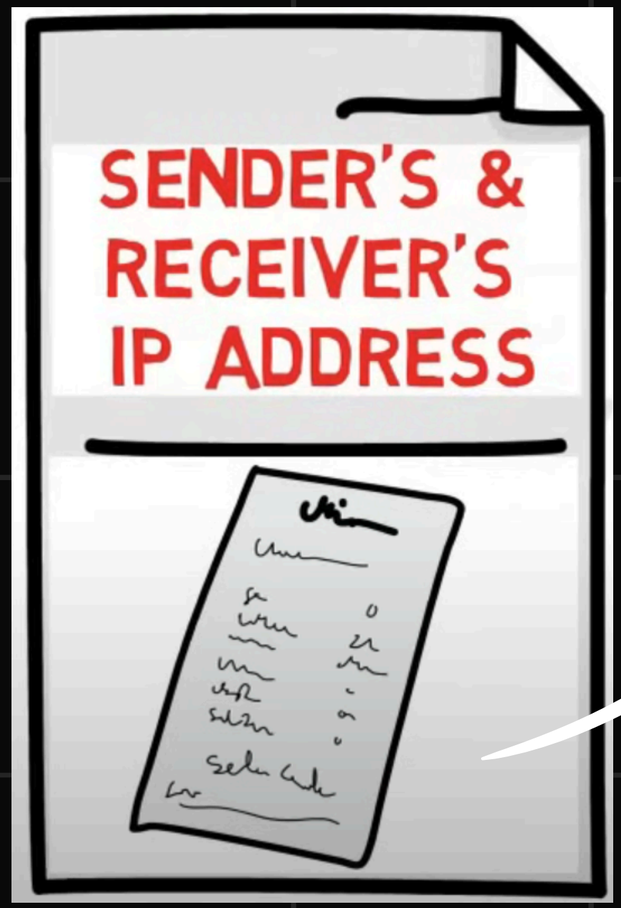


TYPES OF FIREWALL

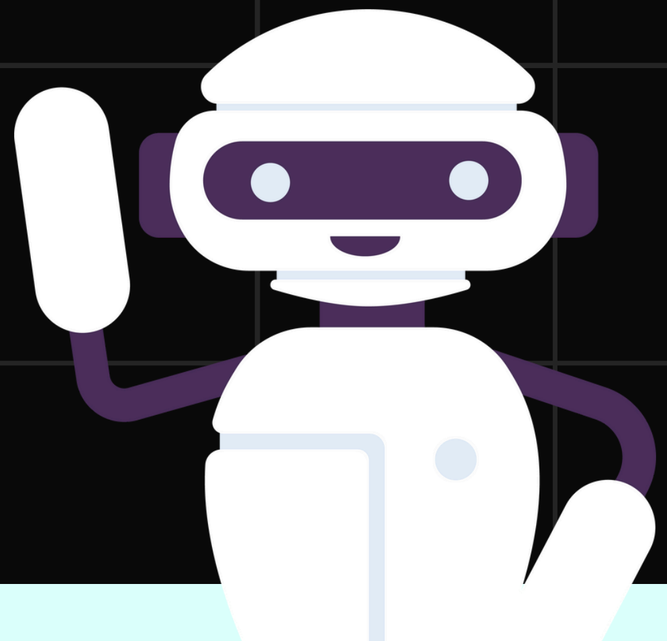


1. Packet Filtering Firewall
2. Application/Proxy Firewall
3. Circuit Level Gateway

DATA PACKETS



Payload



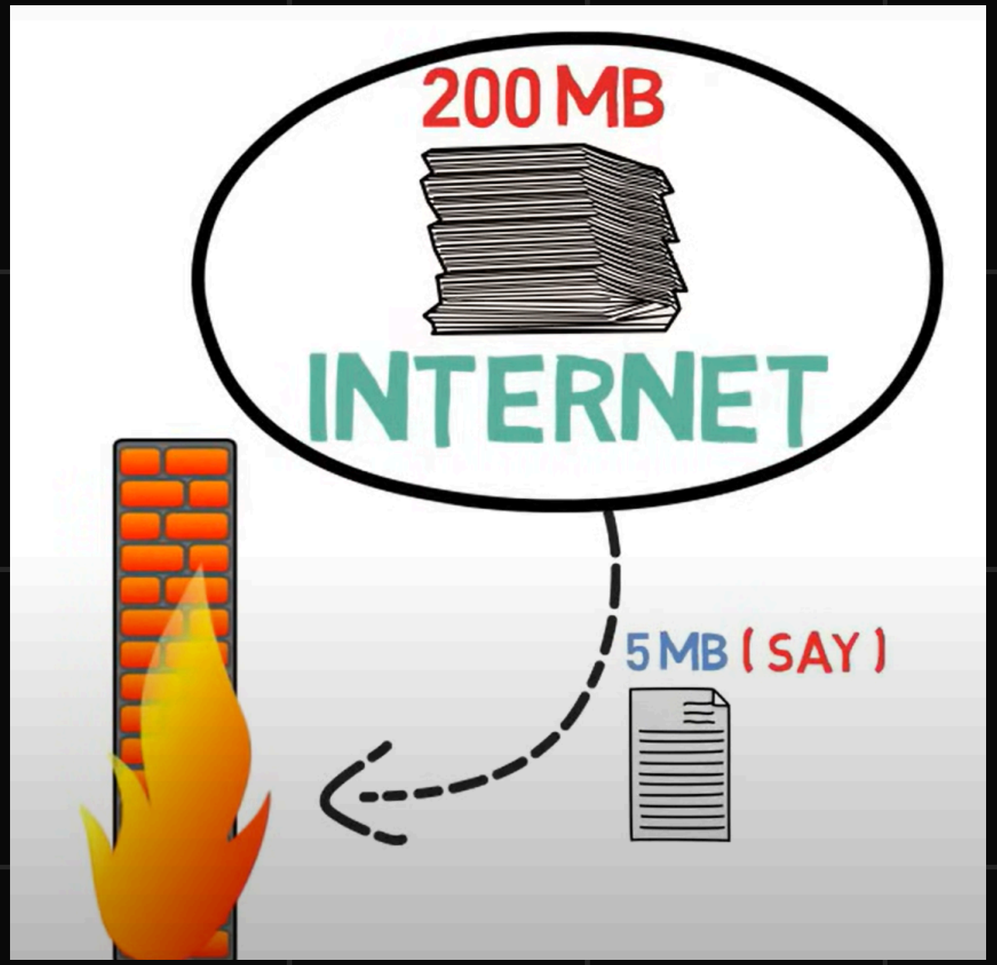
PACKET FILTERING FIREWALL

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

Filtering rules are based on information contained in a network packet.

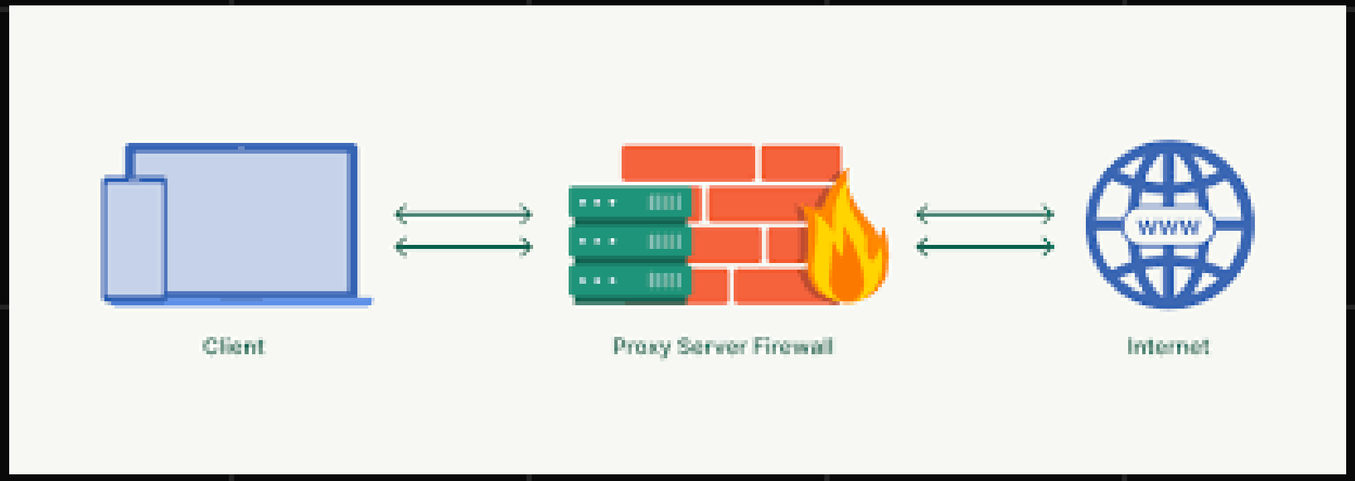
- Source IP address
- Destination IP address
- Source and destination transport level address
- IP protocol field
- Interface

It provides low security since the firewall does not check the payload of the data packet.



APPLICATION OR PROXY FIREWALL

- An application - level gateway, also called an application proxy, acts as a rely of application - level traffic.
- User requests service from proxy. proxy validates request as legal.
- Then actions request and returns result to user.
- Can log / audit traffic at application level.
- It is more secure than packet filter firewall but is also slower since the firewall checks the payload as well

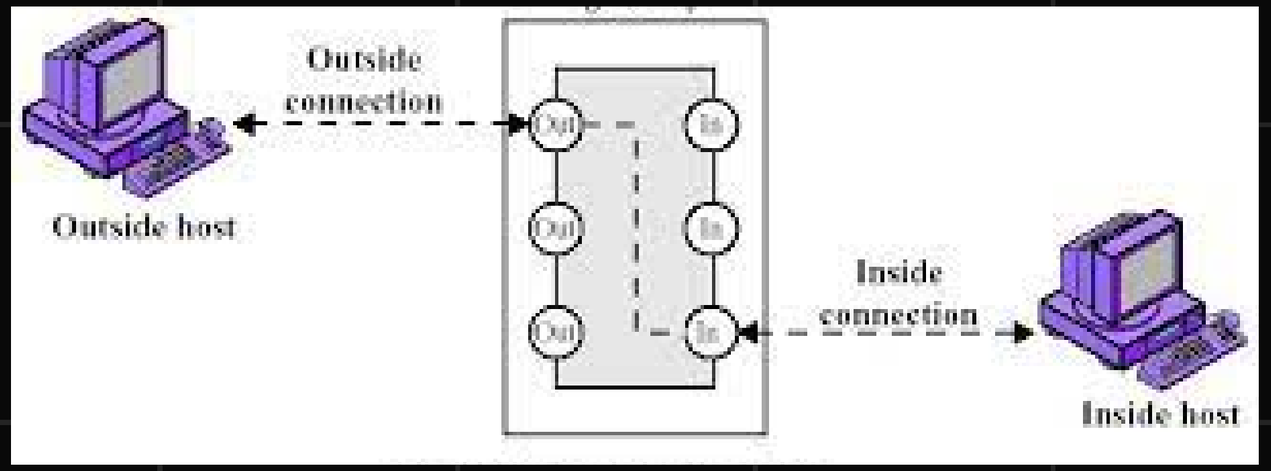


CIRCUIT LEVEL GATEWAY

The gateway sets up two TCP connections

- one between itself and a TCP user on an inner host
- and one between itself and a TCP user on an outside host

They are typically used in combination with packet filtering and application-layer proxy.



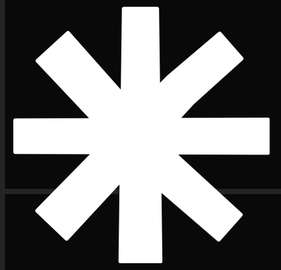
Security check are done before setting up a connection. Once a connection is established, all the data will be passed.

Circuit level gateways are host-based and reside on individual clients & servers inside the network, rather than on dedicated machine as they do with the other types of firewall.

FIREWALL DESIGN PRINCIPLE

SECURITY POLICY

Security policy is a very essential part of firewall design. Security policy is designed according to the requirement of the company or client to know which kind of traffic is allowed to pass. Without a proper security policy, it is impossible to restrict or allow a specific user or worker in a company network or anywhere else. A properly developed security policy also knows what to do in case of a security breach. Without it, there is an increase in risk as there will not be a proper implementation of security solutions.



SIMPLE SOLUTION DESIGN

If the design of the solution is complex. then it will be difficult to implement it. If the solution is easy. then it will be easier to implement it. A simple design is easier to maintain. we can make upgrades in the simple design according to the new possible threats leaving it with an efficient but more simple structure. The problem that comes with complex designs is a configuration error that opens a path for external attacks.

FIREWALL DESIGN PRINCIPLE

CHOOSING THE RIGHT DEVICE

Every network security device has its purpose and its way of implementation. if we use the wrong device for the wrong problem, the network becomes vulnerable. if the outdated device is used for a designing firewall, it exposes the network to risk and is almost useless. Firstly the designing part must be done then the product requirements must be found out, if the product is already available then it is tried to fit in a design that makes security weak.

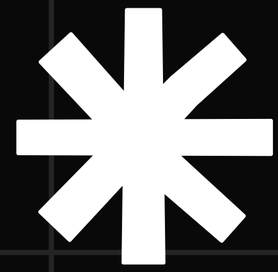
LAYERED DEFENSE

A network defense must be multiple-layered in the modern world because if the security is broken, the network will be exposed to external attacks. Multilayer security design can be set to deal with different levels of threat. It gives an edge to the security design and finally neutralizes the attack on the system.

FIREWALL DESIGN PRINCIPLE

CONSIDER INTERNAL THREATS

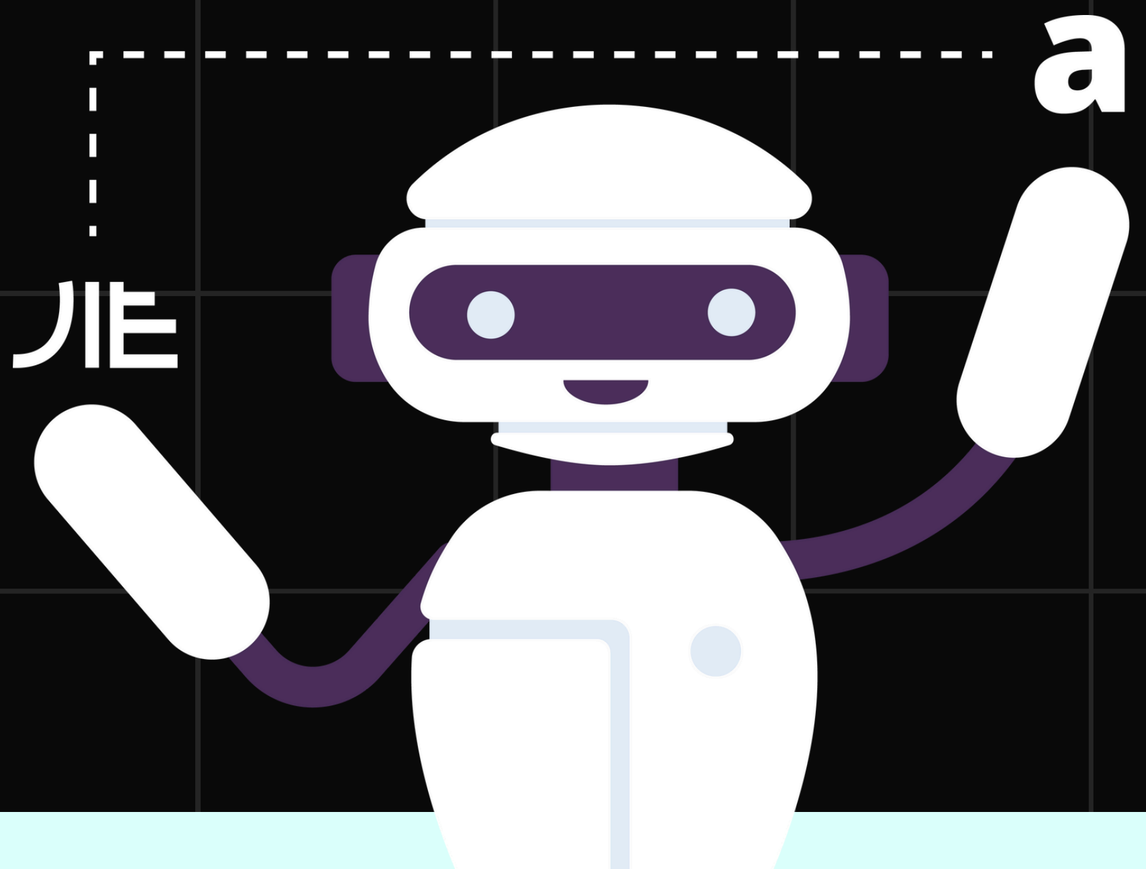
While giving a lot of attention to safeguarding the network or device from external attacks. The security becomes weak in case of internal attacks and most of the attacks are done internally as it is easy to access and designed weakly. Different levels can be set in network security while designing internal security. Filtering can be added to keep track of the traffic moving from lower-level security to higher level.



FUTURE ADVANCEMENTS

INCREASED USE OF ARTIFICIAL INTELLIGENCE (AI) IN FIREWALL TECHNOLOGY

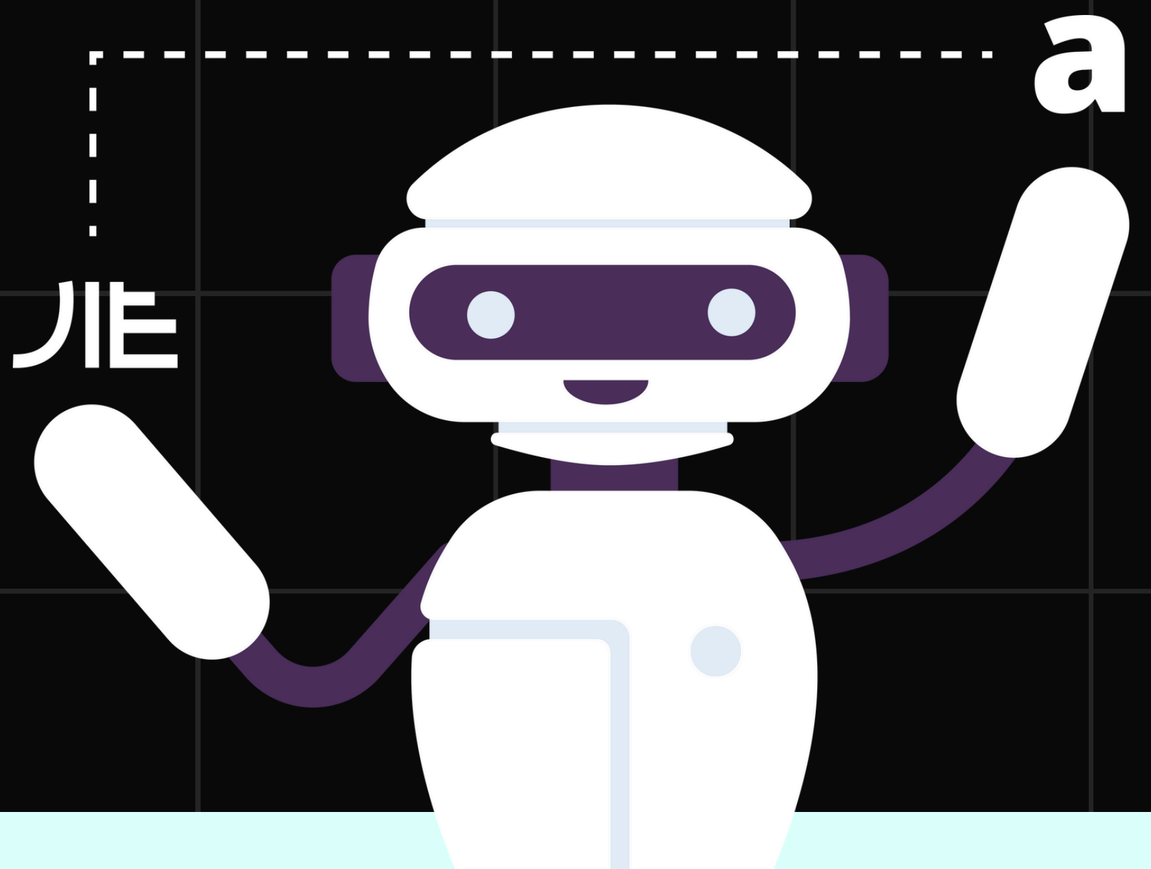
One of the major future trends in firewall technology is the increased utilization of artificial intelligence (AI) algorithms. AI-powered firewalls have the capability to analyze network traffic in real-time, detect anomalies, and respond to threats more effectively.



FUTURE ADVANCEMENTS

INTEGRATION OF CLOUD BASED FIREWALL SOLUTIONS

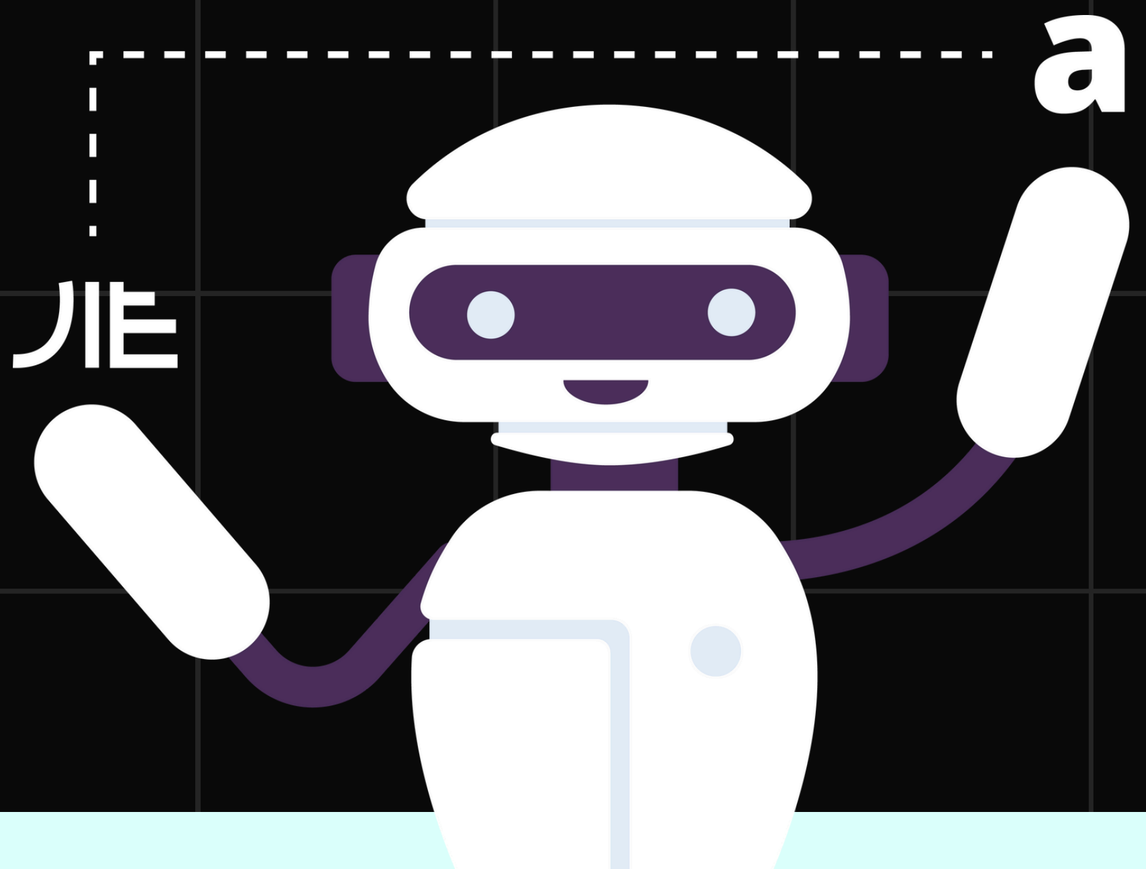
As organizations increasingly migrate their infrastructure to the cloud, the integration of cloud-based firewall solutions is becoming a prominent trend. Cloud-based firewalls offer several advantages, including scalability, flexibility, and centralized management.



FUTURE ADVANCEMENTS

ENHANCED VISIBILITY AND ANALYTICS

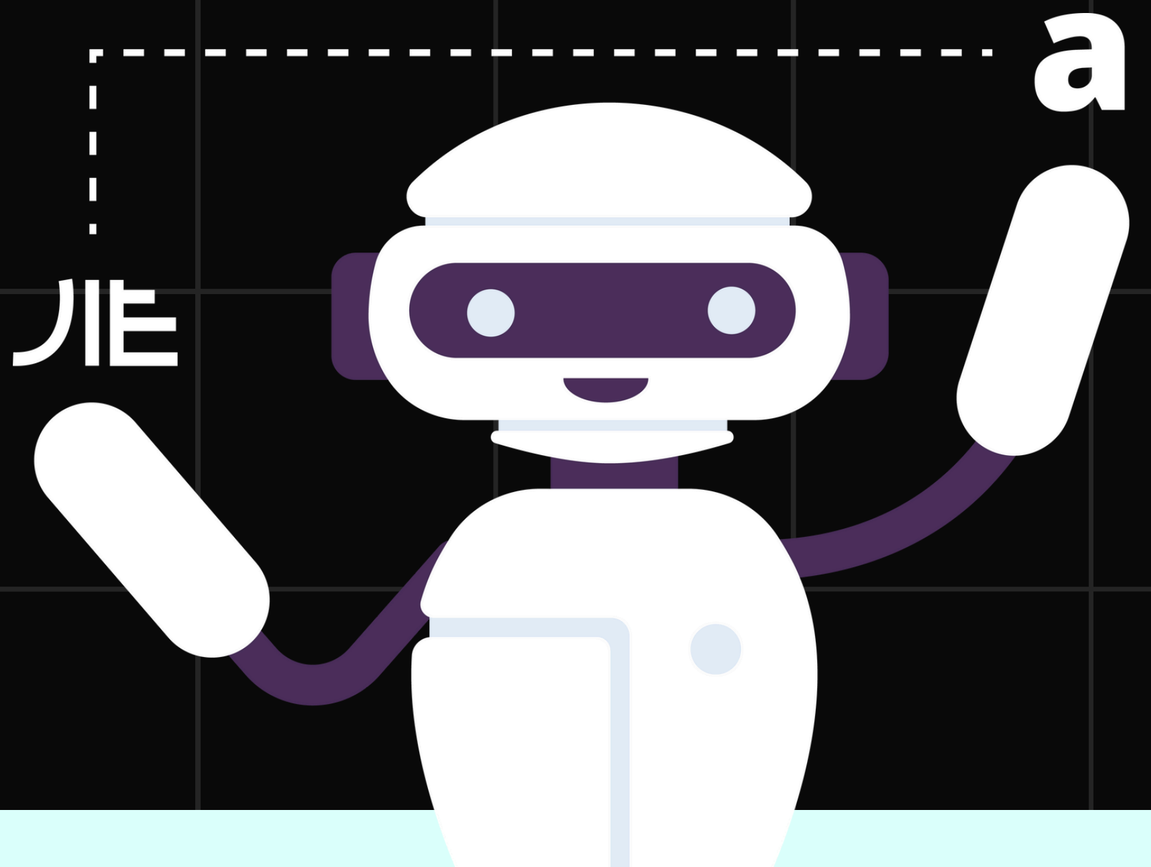
Firewalls of the future will provide enhanced visibility and analytics capabilities to enable organizations to gain deeper insights into their network traffic and security posture.

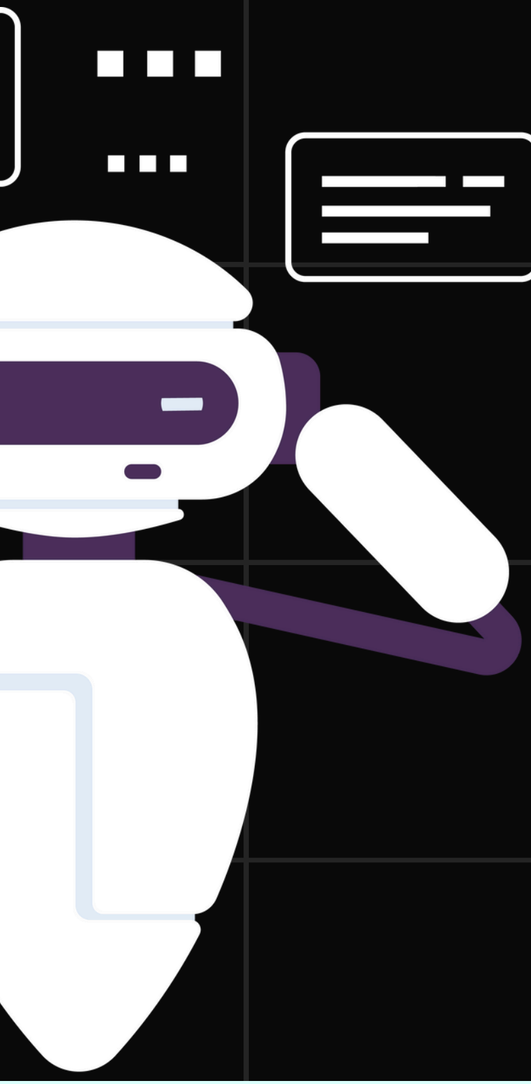


FUTURE ADVANCEMENTS

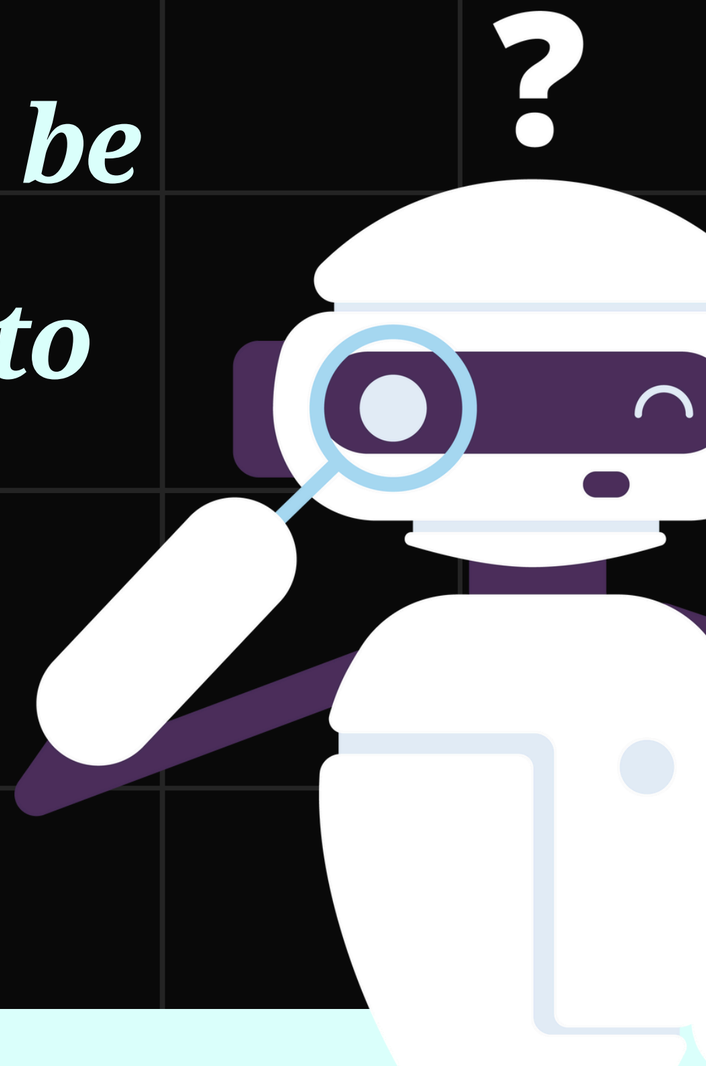
THREAT INTELLIGENCE SHARING AND COLLABORATION

In the future, firewall technology is expected to focus more on threat intelligence sharing and collaboration. By exchanging information about emerging threats and attack patterns, organizations can collectively enhance their defense mechanisms and respond to threats more effectively.

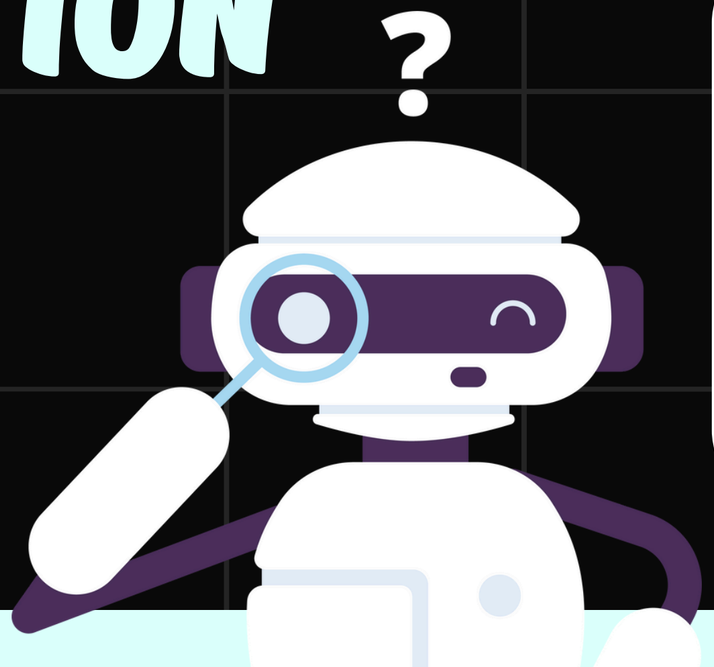




Firewalls will continue to be a cornerstone of cybersecurity, adapting to new technologies and threats.



MULTIPLE CHOICE QUESTION



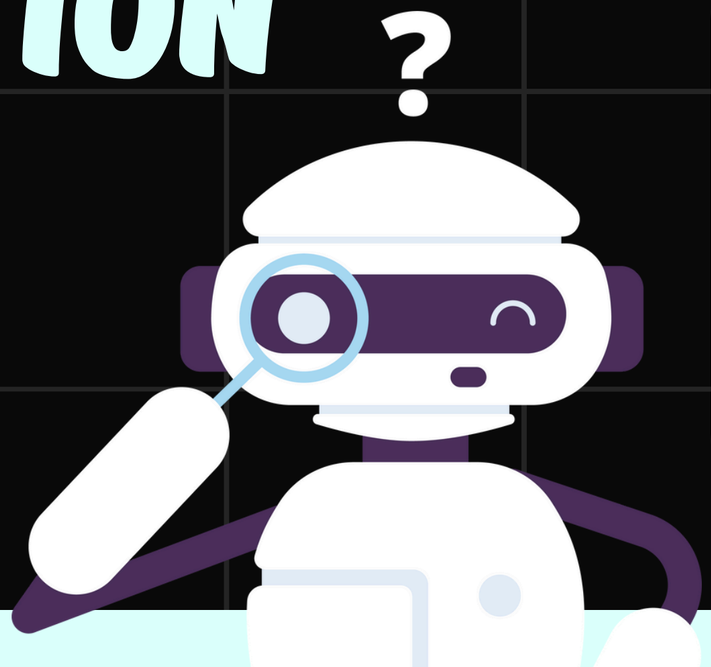
What is the primary function of a firewall?

A) To store data
B) To provide an interface for users
C) To monitor and control network traffic
D) To manage user credentials

What does packet filtering in a firewall involve?

A) Monitoring user behavior
B) Inspecting and allowing/blocking packets based on rules
C) Encrypting network traffic
D) Managing data storage

MULTIPLE CHOICE QUESTION



Which feature allows firewalls to control network access based on user roles?

A) Content filtering
B) Access control
C) Bandwidth management
D) Logging and reporting

What are the two main types of firewalls based on their design?

A) Physical and logical
B) Hardware and software
C) Wired and wireless
D) Static and dynamic

THANK YOU