TYPES OF FIREWALLS

By: Darshan Patel
Senselearner Technologies Pvt Ltd

1. PACKET FILTERING FIREWALL

- Packet Filtering firewall serves as inline security checkpoint attached to a router or switch.
- As the name suggests, it monitors network traffic by filtering incoming packets according to the information they carry.
- Pros: Efficient and fast, Inexpensive
- Cons: Limited Insight, Vulnerable to IP Spoofing

2. STATEFUL INSPECTION FIREWALL

- Stateful Inspection monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.
- It keeps track of the state of connection by monitoring the TCP 3 way handshake.
- Pros: Context awareness, Improved Security
- Cons: Limited application layer inspection, Vulnerable to advanced attack

3. PROXY FIREWALL

- A proxy firewall serves as an intermediate device between internal & external systems communicating over the internet.
- It protects the network by forwarding requests from the original client and masking as it as its own.
- Pros: Enhanced Security, Content filtering
- Cons: Performance overhead, Compatibility Issues

4. NEXT-GEN FIREWALL

- A next generation firewall is a security device that combines a number of functions of other firewalls.
- It incorporates packet, stateful and deep packet inspection.
- Pros: Advanced Security, Integrated Capabilities
- Cons: Very Expensive, More Complex

5. NETWORK ADDRESS TRANSLATION FIREWALL

- NAT firewalls are similar to Proxy firewalls, acting as intermediaries between a group of computers and outside traffic.
- They act as private networks, allowing multiple devices with independent network addresses to connect to the Internet with a single IP address.
- Pros: Easy to implement and Configure, Prevents unsolicited inbound connections
- Cons: No true end-to-end connectivity, Limited protection against advanced threats

6. CIRCUIT LEVEL GATEWAY

- Circuit level gateways are a type of firewall that work at the session layer of the OSI model, observing TCP connections and sessions.
- It monitors TCP handshaking between packets to determine whether a requested session is legitimate.
- Pros: Session State tracking, better performance
- Cons: Lack of user authentication, Difficulty in handling encrypted traffic

7. CLOUD FIREWALL

- A cloud firewall or firewall as a service(FaaS) is a cloud solution for network protection.
- Like other cloud solutions, it is maintained and run on the internet by other third party cloud vendors.
- Pros: Scalability, Cost-effective, Flexibility
- Cons: Network Latency, Limited visibility and controls

8. APPLICATION GATEWAY FIREWALL

- Application gateway firewalls has the capability to inspect packets and ensure the packets are conforming to application specifications.
- It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered.
- Pros: Simplified deployment, Granular access control
- Cons: Incomplete protection, False positives