3 Firewall ,IPS ,IDS

Firewall

A firewall is one of the network equipment running at **layer 4** according to the OSI reference model.
monitor and control network traffic based on configured rules.

> can be placed "inside" the network or "outside" the network.

are known as "Next-generation firewalls" when they include more modern and advanced filtering capabilities.

your payload block by firewall because it their is a signature of payload is present.

Firewalls are crucial network security devices that monitor and control incoming and outgoing traffic based on predefined security rules. They can be hardware, software, or cloud-based, functioning as barriers between trusted internal networks and untrusted external ones, such as the Internet.

Firewalls filter traffic to allow safe data while blocking potentially harmful connections, thus protecting networks from unauthorized access and cyber threats.

Types of Firewalls

Different types of firewalls in networking are:

1. Packet Filtering Firewalls: These examine packets and allow or block them based on source and destination IP addresses and protocols. Basic levels of protection that filter packets based on IP addresses, protocols, or port numbers.

2. Stateful Inspection Firewalls: These track active connections and make filtering decisions based on the state of the connection.

3. Proxy Firewalls: Acting as intermediaries, they prevent direct connections between networks and can provide additional security features. Operate at the application layer, intercepting and inspecting traffic based on applications or functions.

4. Next-Generation Firewalls (NGFW): These combine traditional firewall capabilities with advanced features like intrusion prevention and application awareness to combat

modern threats. - Integrate advanced security technologies like intrusion prevention systems (IPS) and application control for enhanced protection.

5. Web application firewalls (WAFS): Specialize in protecting web applications from specific threats like SQL injection and cross-site scripting (XSS).

Configure Firewalls

Firewall configuration involves setting up rules to allow or block specific types of traffic. Accessing firewall settings, creating new rules, configuring them, saving, applying, and testing the rules to ensure they work as intended.

Firewall Placement in Network

- **Perimeter firewall:** Located at the network edge, they control traffic entering and leaving the network.
- **Internal Firewalls:** Protect specific segments within the network, adding an extra layer of security.
- **Personal Firewalls:** Installed on individual devices such as laptops or smartphones to monitor and control incoming and outgoing traffic. are also called **host based firewall**
- **Cloud Firewalls:** Safeguard cloud-based resources, providing scalable and distributed protection.

Hardware and Software Firewalls

- **Hardware firewalls:** Physical devices offering robust protection but can be expensive and complex to set up.
- **Software firewalls:** Installed on computers or servers, providing more granular control but may consume system resources.

IPS

Intrusion Prevention System (IPS)

- IPS technologies can **detect the Thread and send alert and take action to prevent network** security attacks such as brute force attacks, Denial of Service (DoS) attacks and vulnerability exploits.
  preventing intrusions using methods like signature-based detection, anomaly-based detection, and policy-based detection.

Thread Detection Method used by IPS

1. **Signature-based :**
   Explanation: Think of this like having a "most wanted" list for cyber threats.

How it works: The system looks for known patterns or signatures of threats that are already on the list.
Pros: Effective against known threats that have identifiable patterns.
Cons: Can miss new or modified threats that don't match the known signatures.

2. **Anomaly-based:**
   Explanation: This is like teaching a system what "normal" behavior looks like, so it can spot anything unusual or abnormal.
   How it works: The system learns what is regular on the network or devices.
   Pros: Can detect new or unknown threats by looking for deviations from normal behavior.
   Cons: May generate false positives if legitimate activity is slightly different from the learned normal behavior.

3. **Policy-based Detection:**
   Explanation: You set the rules (policies) for what is allowed and what is not allowed on your network.
   How it works: The system enforces these rules and takes actions based on them.
   Pros: Gives you direct control over what should be allowed and what should be blocked.
   Cons: Needs constant updating and management to stay effective as threats evolve.

> IPS can be Host-based , wireless-based , Network based , Network-based.

> IPS don't need separate device it can be **integrate with NGFW**(Next generation fire wall) OR UTM.

IDS (Intrusion Detection System)

Intrusion Detection System (IDS)

- IDS is similar like IPS but IDS only detect the thread and send the alert to Admin and not take action to prevent network from thread.

IPS don't need separate device it can be **integrate with NGFW**(Next generation fire wall) OR UTM.

The beauty of an IDS is that it's like having a security camera that never blinks, ensuring nothing slips past unnoticed. However, it's important to note that an IDS doesn't take direct action; it's there to detect and alert you, leaving the response up to you.

Firewall and VPNs

Firewalls and virtual private networks (VPNs) work together to secure network traffic. Firewalls control access based on rules, while VPNs encrypt data for secure transmission, making them a powerful combination in network security.

differences between Firewall, IDS, and IPS:

Feature	Firewall	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Function	Controls traffic based on rules	Monitors for malicious activities	Monitors and actively blocks threats
Purpose	Prevents unauthorized access	Detects and alerts on security incidents	Prevents unauthorized access and attacks
Action Taken	Blocks or allows traffic	Logs and reports incidents	Blocks threats in real-time
Response Type	Passive (based on rules)	Passive (alerting only)	Active (automatically intervenes)
Types	Packet-filtering, stateful, proxy	Network-based (NIDS), host-based (HIDS)	Network-based (NIPS), host-based (HIPS)
Deployment Location	Between trusted and untrusted networks	On network or host	On network or host