Somaiya Vidyavihar University
K J Somaiya School of Engineering

Course Name:	**Information Security (116U01L602)**	**Semester:**	VI
Date of Performance:	27/ 03 / 2025	**DIV/ Batch No:**	A-4
Student Name:	Hyder Presswala	**Roll No:**	16010122151

Title: Implementation and configuration of Firewall using Iptable. Demo of Palo Alto Next Gen Firewall

Objectives:

To write a program to convert plain text into cipher text using Caesar cipher and Transposition cipher

Expected Outcome of Experiment:

CO4 :- Illustrate and Compare network security mechanisms

Books/ Journals/ Websites referred:

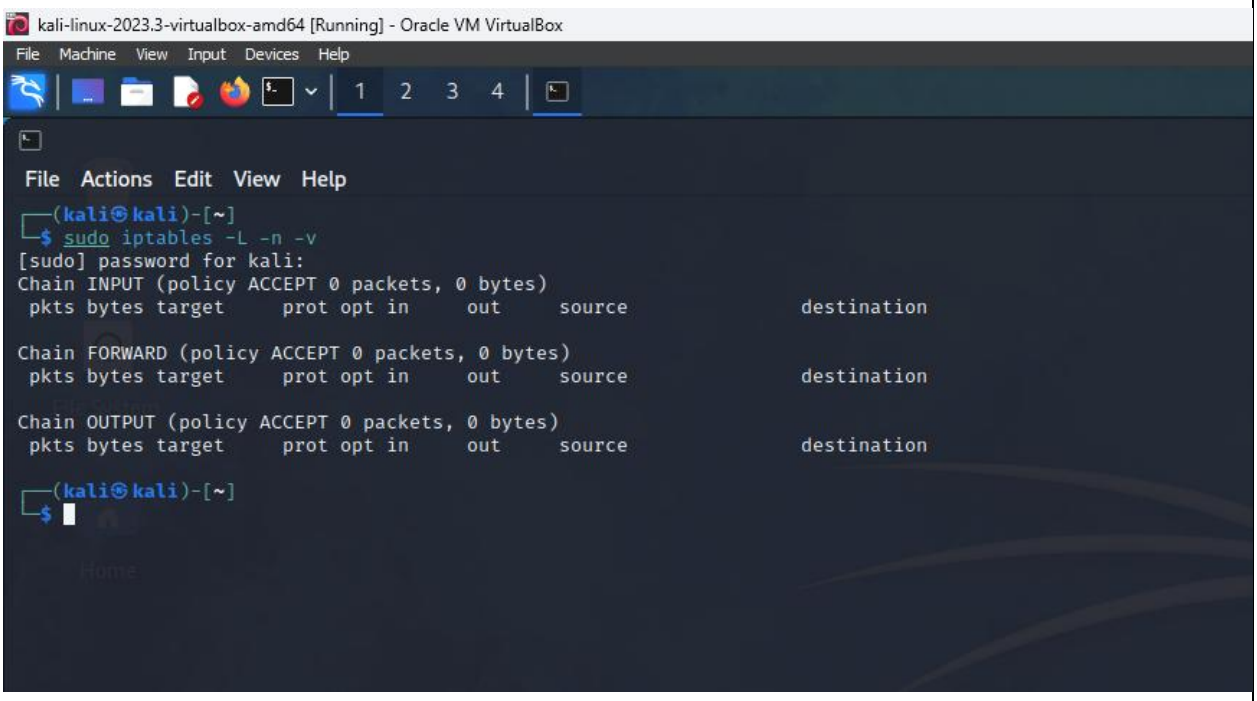
1. Security in Computing
2. Cryptography and Network Security
3. Cryptography and Network Security: Principles and Practice

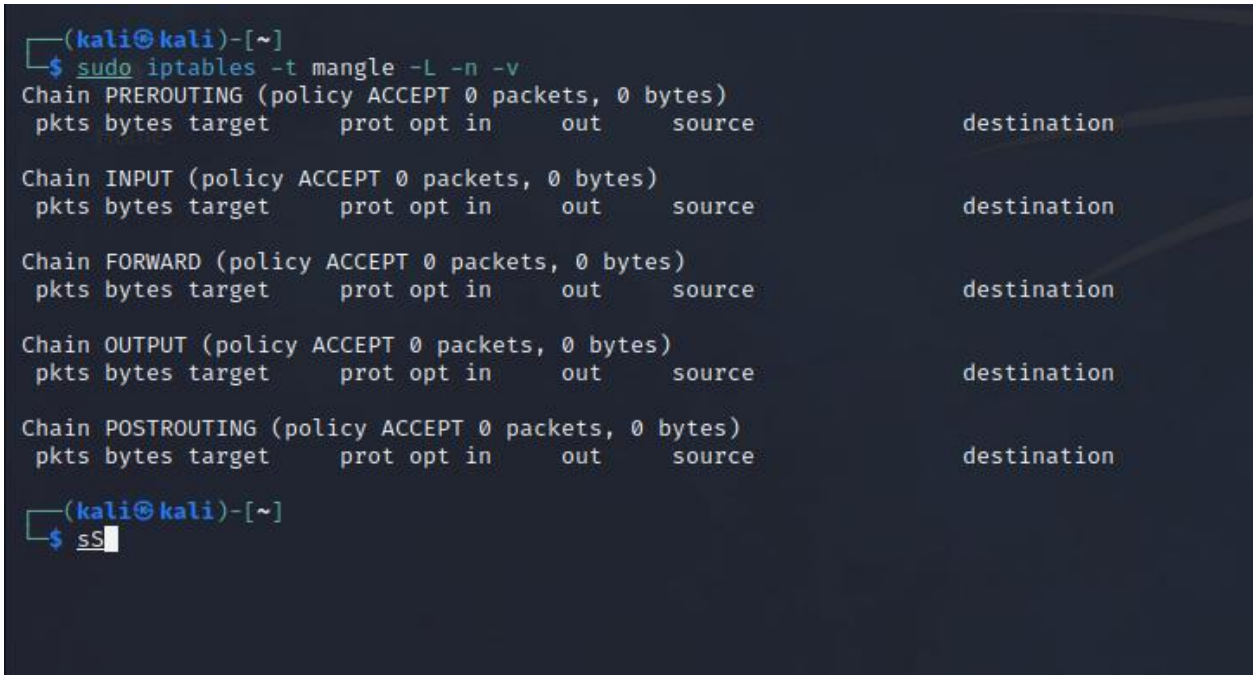
Pre Lab/ Prior Concepts:

New Concepts to be learned:

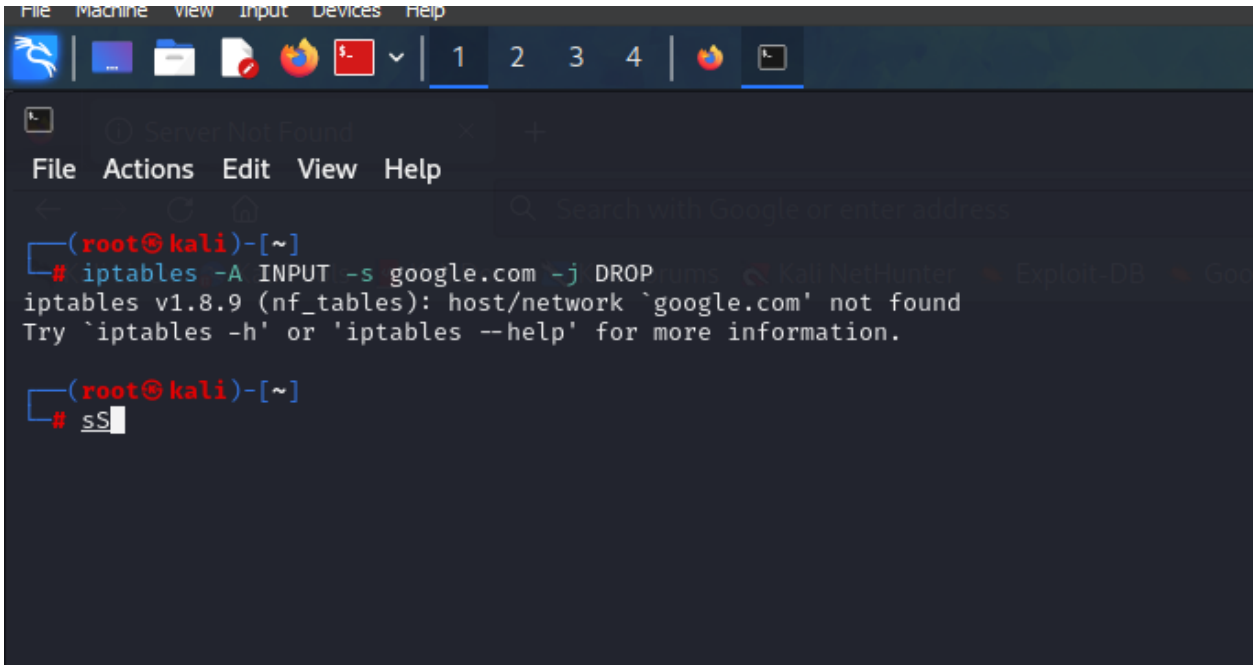
Abstract:

Implementation Details:

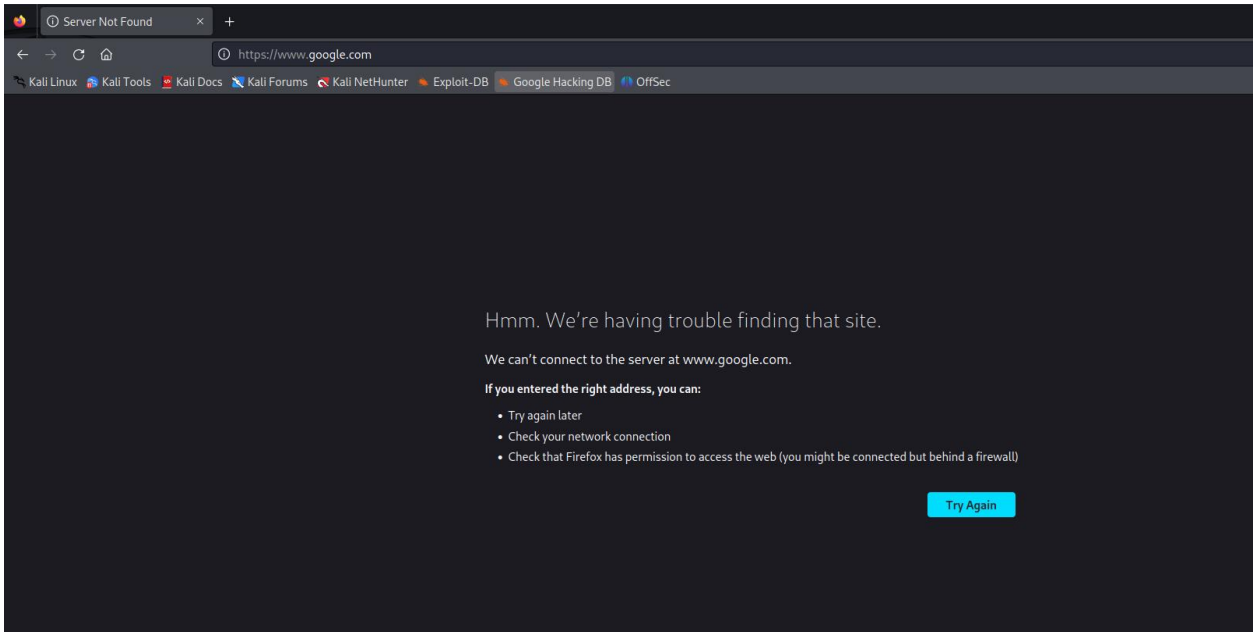




```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

┌──(kali㉿kali)-[~]
└─$
```

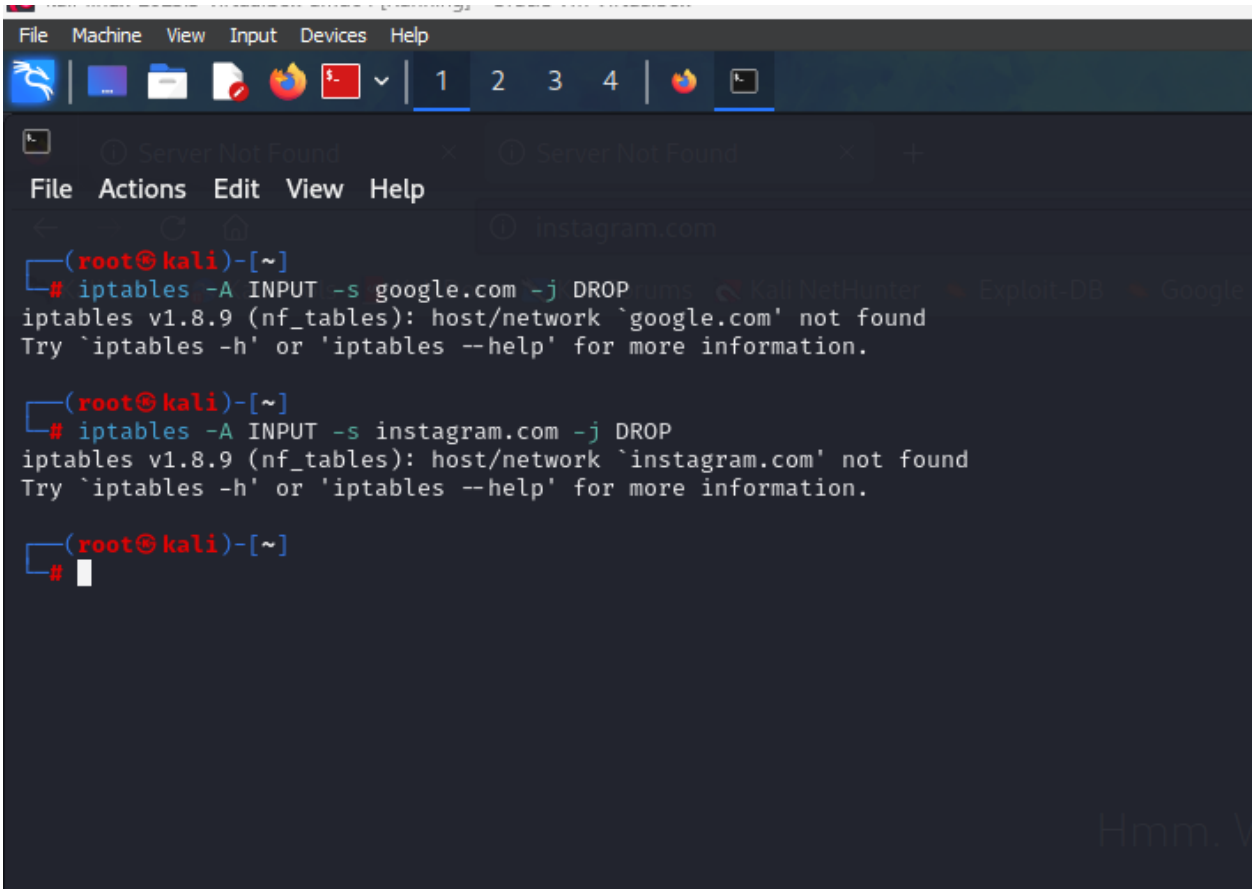


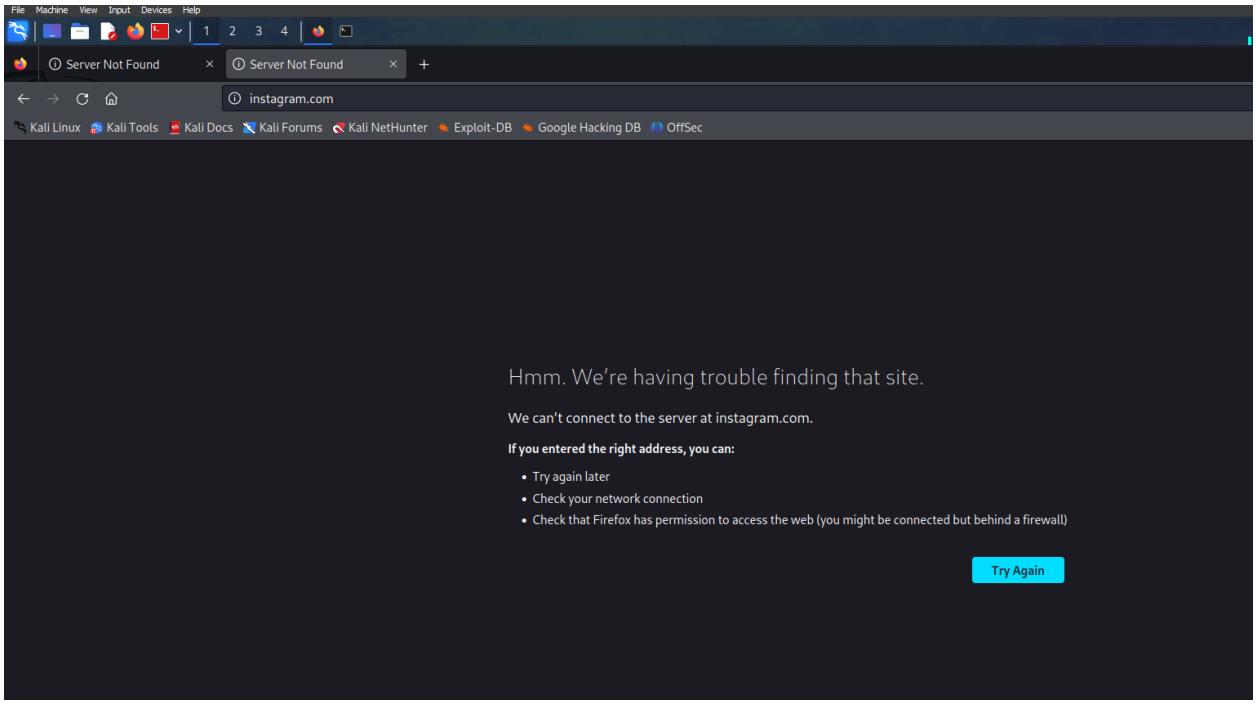
We blocked google



Not able to access google

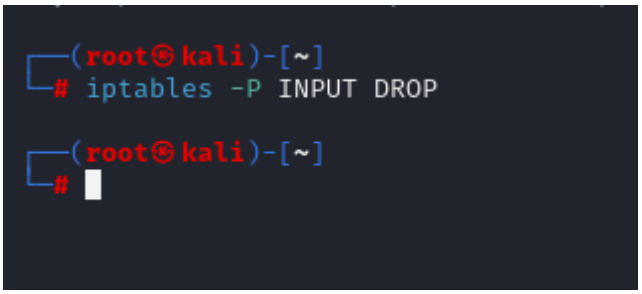
Now lets block instagram

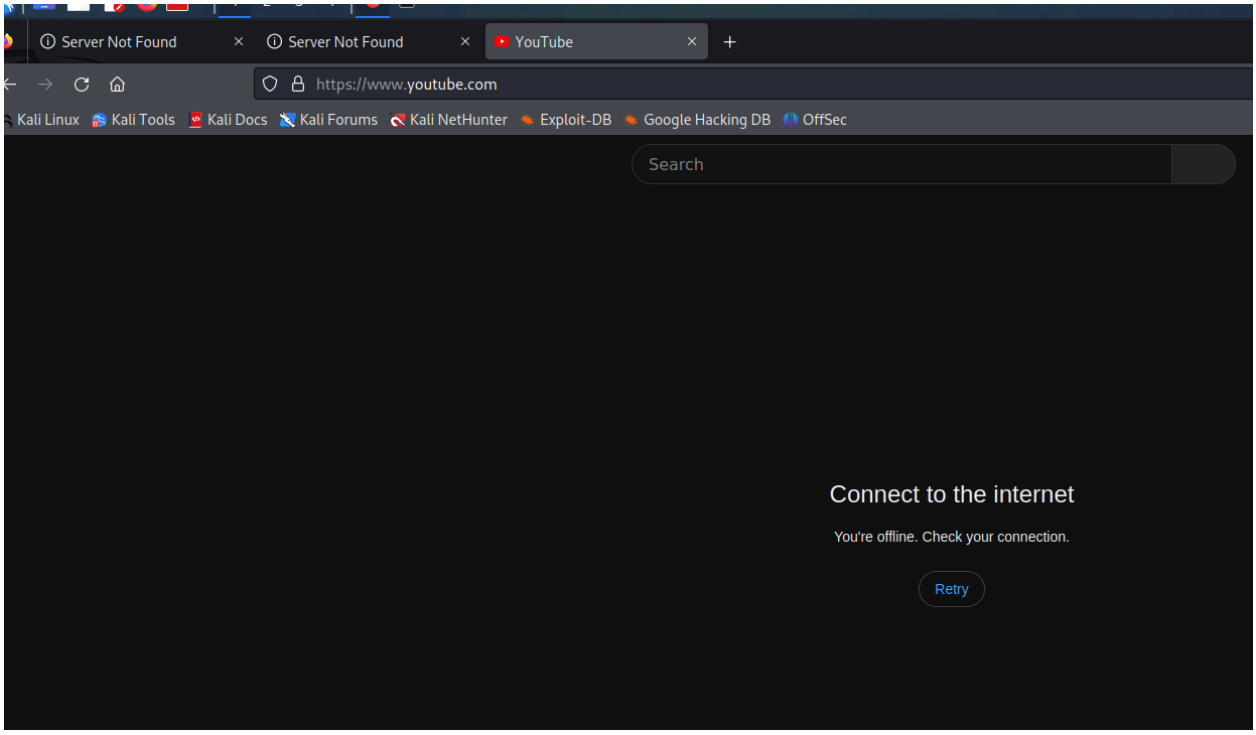




Instagram is blocked now

Now lets block default





Default blocked

Unblocking google

```
┌──(root㉿kali)-[~]
└─# iptables -A INPUT -s google.com -j ACCEPT
iptables v1.8.9 (nf_tables): host/network `google.com' not found
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[~]
└─# iptables -P INPUT ACCEPT

┌──(root㉿kali)-[~]
└─#
```


Conclusion:
Learned how to use iptables to block websites and internet.

Post-Lab Questions:

1 What is the difference between stateful and stateless firewalls?

Ans)

- **Stateful Firewall:**
  A stateful firewall keeps track of the state of active connections and uses this information to decide whether to allow or block network traffic. It understands the context of traffic, such as whether it is part of an established session, and can enforce rules based on that context.
  Example: It allows response packets if a request packet was previously allowed.
- **Stateless Firewall:**
  A stateless firewall evaluates each packet independently of its context. It uses static rules to decide whether to allow or block traffic without considering the state of the connection.
  Example: It blocks or allows packets based only on IP address, port, or protocol, without knowing if they are part of an existing session.

2 How does a firewall protect data?

Ans)

A firewall protects data by:

1. **Traffic Filtering:** It filters incoming and outgoing traffic based on predefined security rules, blocking malicious traffic.
2. **Access Control:** It restricts access to specific resources by allowing or denying traffic based on IP addresses, ports, and protocols.
3. **Preventing Unauthorized Access:** It ensures only authorized users or devices can access a network.
4. **Mitigating Attacks:** It blocks known threats like DDoS attacks, malware, and unauthorized connections.
5. **Packet Inspection:** Stateful firewalls inspect data packets to ensure they are part of legitimate sessions, reducing the risk of data breaches.

3 What can't a firewall protect against?

Ans)

A firewall has limitations and cannot protect against:

1. **Insider Threats:** Malicious activity from within the organization.

2. **Social Engineering Attacks:** Phishing, scams, or manipulation of users to steal credentials.
3. **Zero-Day Exploits:** Attacks exploiting unknown vulnerabilities.
4. **Encrypted Threats:** Malicious traffic hidden in encrypted packets that the firewall cannot inspect.
5. **Non-Network Attacks:** Physical access to systems or attacks that do not use the network, such as USB malware.

4 How is a firewall different from an IDS and an IPS? Explain.
Ans)

- **Firewall:**
  1. Acts as a gatekeeper, blocking or allowing traffic based on predefined rules.
  2. Primary purpose: Prevent unauthorized access.
  3. Operates at the network layer and focuses on filtering traffic.
- **Intrusion Detection System (IDS):**
  1. Monitors network traffic and identifies suspicious or malicious activities.
  2. Primary purpose: Alert administrators of potential threats.
  3. Does not block traffic, only generates alerts.
- **Intrusion Prevention System (IPS):**
  1. Similar to IDS but actively blocks malicious traffic in real-time.
  2. Primary purpose: Prevent attacks by blocking threats automatically.

Key Difference: A firewall controls traffic based on rules, while IDS/IPS detects and responds to threats by analyzing traffic behavior. An IDS is passive (alert only), whereas an IPS is active (blocks threats).