a) What is meant by a Spoofing attack?. Describe in brief the types of spoofing attack . Consider the case of the SYN Flood attack and explain briefly what a Denial of Service attack is.

Ans.

Spoofing Attack

A spoofing attack is a type of cyberattack where a malicious actor pretends to be a trusted source to deceive systems, devices, or users. The goal is to bypass security measures, steal sensitive information, or disrupt network services.

Ans.

Types of Spoofing Attacks

1. **IP Spoofing**: The attacker disguises their IP address to impersonate another device on a network, often used in DDoS attacks.
2. **Email Spoofing**: Fake email headers are created to make it look like emails are from a trusted sender, often for phishing.
3. **DNS Spoofing**: The attacker alters DNS records, redirecting users to malicious websites without their knowledge.
4. **MAC Spoofing**: The attacker changes their MAC address to bypass network controls or impersonate another device.

Ans.

SYN Flood Attack

A SYN flood is a Denial of Service (DoS) attack where an attacker repeatedly sends SYN requests to a server, initiating many incomplete connections. The server allocates resources to each request but, due to the lack of response from the attacker, becomes overwhelmed and unable to handle legitimate connections. This creates a **Denial of Service** as valid users are blocked from accessing the server's resources.

b) What is packet filtering firewall? Briefly explain its working principle Differentiate between transport and tunnel modes of operation of IPSec. Explain brute force attack.

Ans.

Packet Filtering Firewall

A packet filtering firewall controls network access by monitoring outgoing and incoming packets, allowing or blocking them based on predefined rules. It examines packet headers, checking IP addresses, protocols, ports, and flags to decide if a packet should be allowed or blocked.

Ans.

Working Principle

The firewall inspects each packet's header information without considering the packet's content or state. Based on rules, it permits or denies the packet's passage, making it effective for simple traffic control.

Ans.

Transport vs. Tunnel Modes of IPSec

- **Transport Mode**: Encrypts only the data (payload) in a packet. Used for end-to-end communication between two devices.
- **Tunnel Mode**: Encrypts the entire packet, including the header. Used for network-to-network communication, such as between gateways in a VPN.

Ans.

Brute Force Attack

A brute force attack is a method where attackers systematically attempt all possible combinations to guess a password or encryption key. This trial-and-error approach is time-consuming but can succeed if password strength is weak or computational resources are high.

c) Explain man-in-the -middle attack with suitable example. What is a worm? How does it differ from a virus? What is VPN? Why VPN is required?

Ans.

Man-in-the-Middle (MITM) Attack

In a MITM attack, an attacker intercepts communication between two parties to secretly listen, alter, or steal data. For example, in an unsecured public Wi-Fi, an attacker could intercept messages between a user and a website, capturing login credentials or sensitive information.

Ans.

Worm: A self-replicating malware that spreads across networks without user interaction.

Ans.

Worm vs. Virus

- **Worm**: A self-replicating malware that spreads across networks without user interaction. It exploits network vulnerabilities to propagate.
- **Virus**: A malware that attaches itself to files and requires user action (like opening a file) to spread. It can't self-replicate without a host file or program.

Ans.

VPN (Virtual Private Network)

A VPN creates a secure, encrypted connection over the internet, allowing users to access networks remotely and privately.

Ans.

Why VPN is Required: It enhances privacy by masking IP addresses, protects data over unsecured networks, and enables secure access to remote resources.

d) Explain DNS spoofing with suitable example How is a circuit gateway different from an application gateway? Explain how NAT works with an example.

Ans.

DNS Spoofing

DNS spoofing (or DNS cache poisoning) is an attack where an attacker corrupts DNS records to redirect users to malicious websites. For example, if a user tries to visit a legitimate website like "bank.com," a spoofed DNS response could redirect them to a phishing site, tricking them into entering sensitive information.

Ans.

Circuit Gateway vs. Application Gateway

- **Circuit Gateway**: Operates at the session layer, managing TCP or UDP connections without inspecting packet contents. It's faster but less secure.
- **Application Gateway (Proxy)**: Works at the application layer, inspecting traffic for specific applications (e.g., HTTP, FTP) to provide fine-grained security control. It's slower due to deep packet inspection but more secure.

Ans.

Network Address Translation (NAT)

NAT translates private IP addresses on a local network to a single public IP address for internet communication. For example, multiple devices in a home network with private IPs (e.g., 192.168.0.x) access the internet through the router's public IP, with NAT translating each device's IP address, helping conserve public IP addresses and providing an extra layer of security.

e) What is a firewall? Explain different types of firewall configurations with neat diagram.. What is the purpose of the SSL alert protocol?

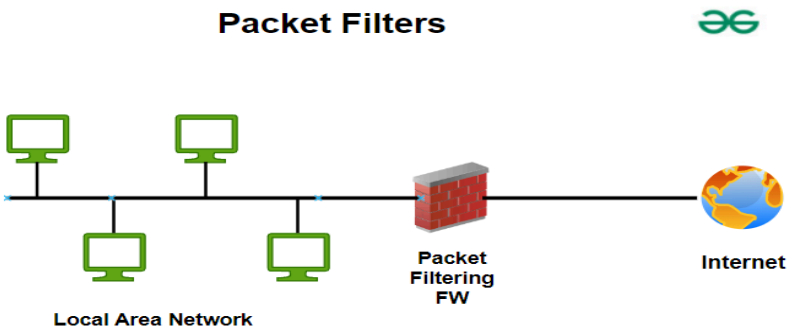
Ans.

Firewall
A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between trusted and untrusted networks.

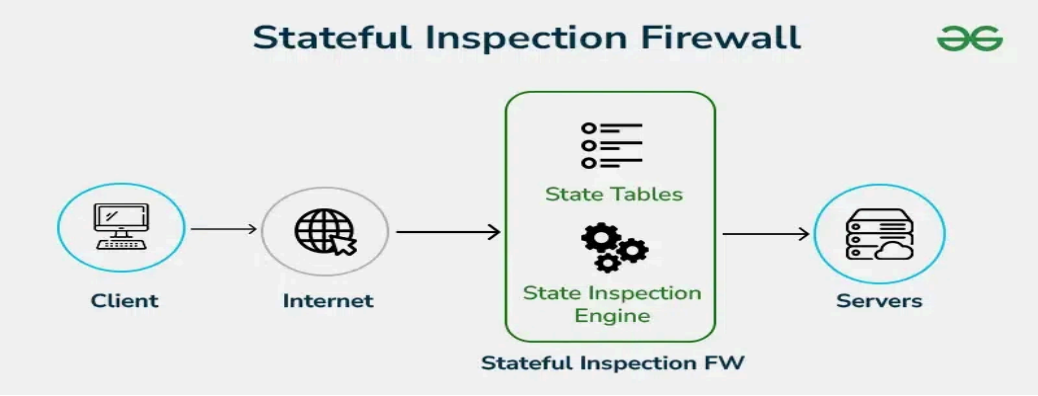
Ans.

Types of Firewall Configurations

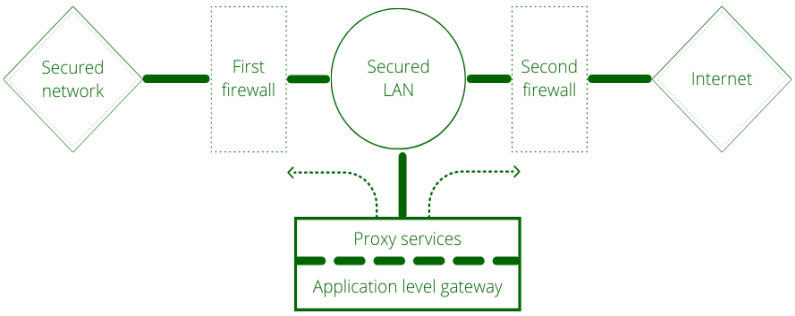
1. **Packet Filtering Firewall**: Filters packets based on IP addresses, protocols, and ports.



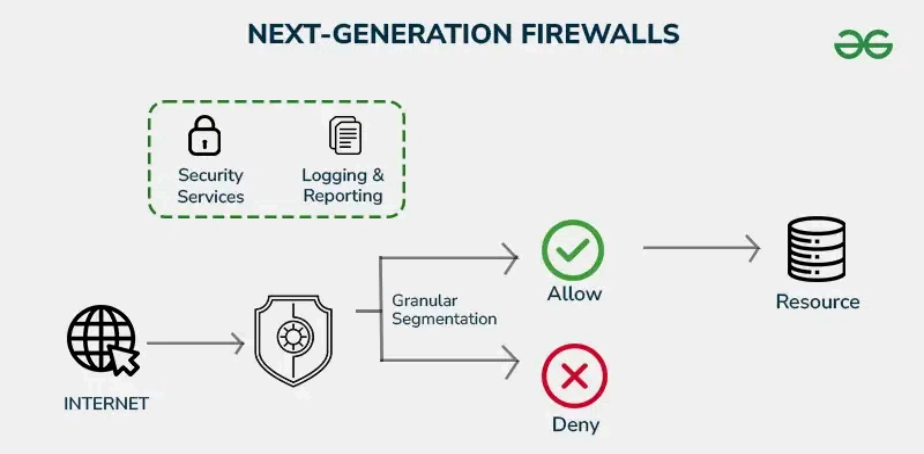
2. **Stateful Inspection Firewall**: Tracks active connections, inspecting packets based on the state of the connection.



3. **Proxy Firewall (Application Gateway)**: Intermediates between user and server, filtering traffic for specific applications.



4. **Next-Generation Firewall (NGFW)**: Combines traditional firewall features with advanced security functions like intrusion prevention and deep packet inspection.



Ans.

Purpose of SSL Alert Protocol
The SSL (Secure Sockets Layer) alert protocol notifies parties of any issues in a secure connection. Alerts can indicate warnings, errors, or connection terminations to maintain secure communication between clients and servers.

f) Explain different attacks possible on packet filtering router. State the suitable countermeasure for each attack . Explain the working of SSL record protocol in detail, with a neat diagram . Define the term non-repudiation

Ans.

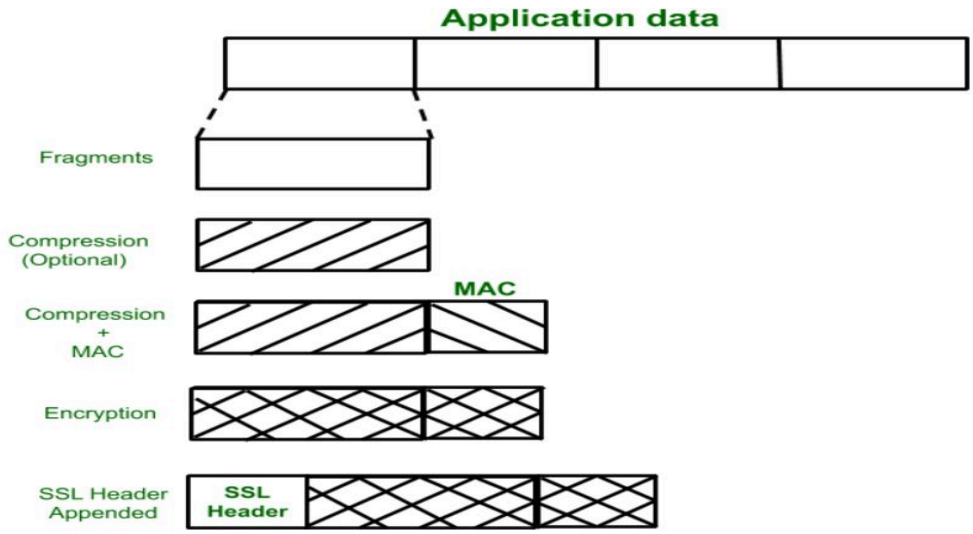
Attacks on Packet Filtering Routers & Countermeasures

1. **IP Spoofing**: Attackers forge IP addresses to bypass filters.
    - **Countermeasure**: Use ingress and egress filtering to block spoofed addresses.
2. **Source Routing Attacks**: Attackers specify packet routes, avoiding security filters.

    - **Countermeasure**: Disable source routing to prevent attackers from dictating packet paths.
3. **Tiny Fragment Attack**: Splits headers across multiple packets to bypass filtering rules.
    - **Countermeasure**: Block tiny fragments or reassemble packets for inspection.
4. **Denial of Service (DoS)**: Floods the router with traffic, overwhelming it.
    - **Countermeasure**: Implement rate limiting and intrusion detection systems (IDS).

Ans.

SSL Record Protocol
The SSL Record Protocol provides data confidentiality and integrity over SSL connections. It divides application data into manageable blocks, compresses, and optionally encrypts them before adding a Message Authentication Code (MAC). The encrypted data is sent to the receiver, where it's decrypted, verified, and reassembled.



Ans.

Non-Repudiation
Non-repudiation ensures that a party cannot deny the authenticity of their actions, like sending a message or making a transaction, providing proof of origin and integrity.

g) Why SSL is placed between application layer and transport layer of OSI model . State at least two advantages and drawbacks of application-level gateway . Explain with neat sketch, the working of handshake protocol in SSL.

Ans.

Why SSL is Placed Between Application and Transport Layers
SSL is positioned between the application and transport layers to provide end-to-end encryption and secure data transmission without altering application or transport layer protocols. It ensures

secure communication over the transport layer (e.g., TCP) while maintaining application compatibility.

Ans.

Advantages of Application-Level Gateway

1. **Enhanced Security**: Inspects application data and blocks specific threats, providing granular control.
2. **User Authentication**: Allows user authentication for each session, adding an extra security layer.

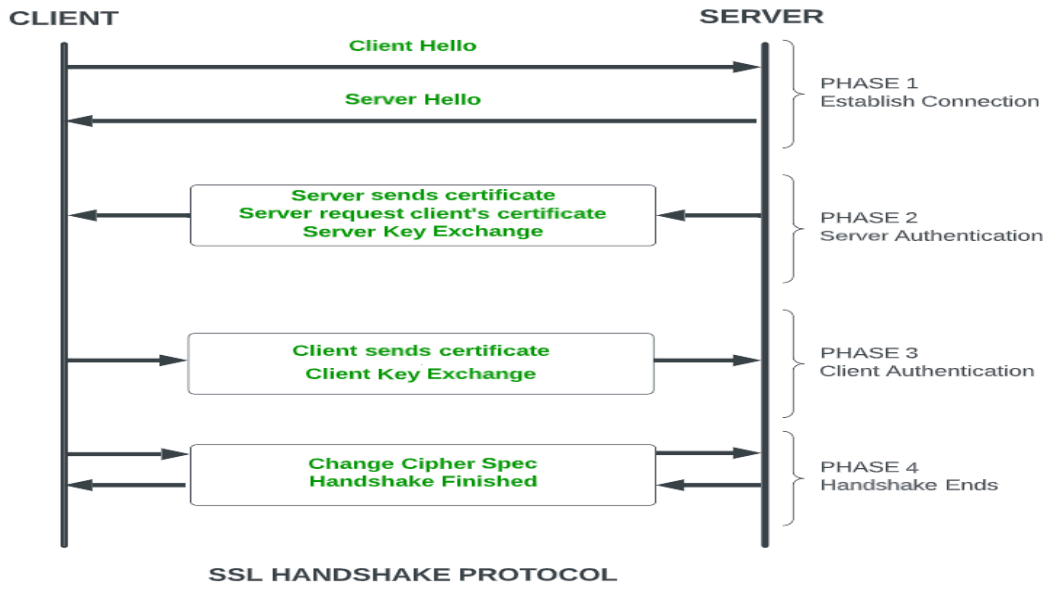
Drawbacks of Application-Level Gateway

1. **Performance Overhead**: Slower due to deep packet inspection at the application layer.
2. **Complex Configuration**: Requires more setup and may limit application compatibility.

Ans.

SSL Handshake Protocol
The SSL handshake establishes a secure connection through these steps:

1. **Client Hello**: Client sends supported SSL versions, cipher suites, and a random number.
2. **Server Hello**: Server chooses SSL version and cipher, sends certificate, and a random number.
3. **Key Exchange**: Both parties generate session keys using exchanged data.
4. **Finished Messages**: Both confirm the handshake, and secure data transfer begins.



h) Write short notes on (i) Phishing (ii) Trojan Horse (iii) Pharming (iv) Active attacks.

Ans.

(i) Phishing
Phishing is a social engineering attack where attackers impersonate trusted entities (e.g., banks, email providers) to deceive users into revealing sensitive information like login credentials or financial details, often through fake emails or websites.

(ii) Trojan Horse
A Trojan Horse is malicious software disguised as legitimate software. When users download and run it, the Trojan performs hidden harmful activities, such as stealing data or allowing unauthorized access to the infected system.

(iii) Pharming
Pharming redirects users from legitimate websites to fake ones by corrupting DNS settings. It's often used to steal sensitive information by tricking users into thinking they're on a trusted website.

(iv) Active Attacks
Active attacks involve altering or disrupting data in transit, such as message modification, replay attacks, or Denial of Service (DoS). Attackers actively manipulate communication channels to compromise data integrity and availability.