**Cryptography and Network Security**

LAB ASSIGNMENT 12

**Submitted By:**

Name: Himanshu Verma

Roll No: **201210023**

Branch: **CSE**

Semester: **8rd**

****

**NATIONAL INSTITUTE OF TECHNOLOGY, DELHI Department of Computer Science and Engineering (2020)**

**Question 1:**

a)

- Packet Filtering Firewall: Examines packets at the network layer and makes decisions based on information such as source/destination IP addresses, ports, and protocol types.

- Stateful Inspection Firewall: Tracks the state of active connections and makes decisions based on the context of the traffic, such as whether it's part of an established session or a new connection.

- Application Layer Firewall: Operates at the application layer of the OSI model and can inspect and filter traffic based on specific application protocols (e.g., HTTP, FTP, SMTP).

**Question 2:**

For each rule:

1. Allows TCP traffic from specific source IP to specific destination IP on port 80.

- Type of traffic: TCP traffic on port 80

- Potential security risks: If the source IP is spoofed, an attacker could bypass the firewall and access port 80.

2. Denies UDP traffic from any source IP to specific destination IP on port 53.

- Type of traffic: UDP traffic on port 53

- Potential security risks: Denying DNS traffic (port 53) could prevent legitimate DNS resolution.

3. Allows ICMP traffic from any source IP to any destination IP.

- Type of traffic: ICMP traffic

- Potential security risks: ICMP traffic could be used in various attacks like ping flooding or ICMP redirect attacks.

**Question 3:**

Stateful Inspection Firewall:

- Operation: Examines packets at the network and transport layers but also maintains information about the state of active connections.

- Difference: It differs from packet filtering by considering the context of traffic and from application layer firewalls by not inspecting application layer data.

- Advantages: Provides better security as it understands the context of traffic, better performance due to reduced processing overhead, and can handle dynamic protocols.

- Disadvantages: More complex to configure and manage compared to packet filtering, may introduce latency due to maintaining state information.

**Question 4:**

plaintext

1. Allow TCP traffic from any source to 192.168.1.100 on ports 80 and 443

2. Allow TCP traffic from 192.168.1.0/24 to 192.168.1.50 on port 22

3. Deny all incoming traffic

4. Allow all outgoing traffic

**Question 5:**

a)

1. \*\*ALLOW TCP 192.168.1.10 -> 10.0.0.5:80\*\*: Allows TCP traffic from 192.168.1.10 to 10.0.0.5 on port 80.

2. \*\*DENY UDP 192.168.1.20 -> 10.0.0.10:53\*\*: Denies UDP traffic from 192.168.1.20 to 10.0.0.10 on port 53.

3. \*\*ALLOW ICMP 192.168.1.30 -> 8.8.8.8\*\*: Allows ICMP traffic from 192.168.1.30 to 8.8.8.8.

b)

- The denial of UDP traffic to port 53 may prevent DNS resolution for the source IP 192.168.1.20.

- Allowing ICMP traffic to external IP 8.8.8.8 may pose a security risk if it's not necessary for network operations.