National University Of Technology

Name : Ayesha Imran

Class : CS (A)-2024

Id : F24605019

Assignment : 04th

Course : Information Security

Submitted To : Ma'am Attiya Ashraf

QUESTION : 01

Explain Firewall and different types of firewalls along with their benefits and limitations?

A Firewall is a security system either hardware, software, or a combination that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Types Of Firewalls:

1- Packet Filtering Firewall

- Works at network layer by examining source and destination IP addresses, ports, and protocols.
- Simple, fast and requires minimal resources.
- Cannot inspect packet payloads, making it vulnerable to spoofing and advanced attacks.

2- Stateful Inspection Firewall

- Tracks the state of active connections and makes decisions based on traffic context.
- More secure than traffic filtering, as it understands ongoing sessions.
- Consumes more resources and may slow down under heavy traffic

3 - Proxy Firewall (Application-Level Gateway)

- Acts as an intermediary between users and services, inspecting traffic at the application layer.
- Provides deep inspections and hides internal network details.
- Slower performance and may not support all applications or protocols.

4- Next Generation Firewall (NGFW):

- Combines traditional firewall features with advanced capabilities like intrusion prevention, deep packet inspection, and application awareness.
- Strong protection against modern threats, granular control over applications.
- Expensive and complex to configure/manage.

5- Hardware Firewall

- A dedicated physical device placed between the network and the internet.
- High performance, protects entire networks, independent of host systems.
- Costly and requires ongoing maintenance

6- Software Firewall

- Installed on individual devices to protect them from threats.
- Flexible, easy to deploy, customizable rules per host.
- Consumes system resources and only protects the device it runs on

7- Cloud Firewall:

- Delivered as a service to protect cloud-based infrastructure.
- Scalable, easy to update, suitable for modern cloud workloads.
- Dependant on provider reliability and may introduce Latency.

8- Hybrid Firewall:

- Combines multiple firewall approaches for layered defense.
- Comprehensive protection covering multiple attack vectors.
- Complex to manage and requires skilled administrators.

Question 2 : Explain Common characteristics of Intrusion Prevention and detection System along with advantage and disadvantage.

- characteristics:

Monitor network traffic continuously

Use signatures (known attack patterns) and anomaly detection (unusual behavior)

IDS → alerts admins; IPS → blocks threats in real time

Often integrated with firewalls for Layered defense

- **Advantages:**

Detects attacks quickly

Provides visibility into network activity

IPS can stop threats automatically

- **Disadvantages:**

False positives can overwhelm admins.

Performance overhead on busy networks.

Needs frequent updates to stay effective

QUESTION 3 : Explain VPNs and different types of VPNs?

A VPN creates a secure, encrypted tunnel between a user/device and a network, ensuring privacy, data protection, and safe communication over the internet.

Remote Access VPN → Used by individuals to connect surely to a Private network (e.g., remote workers).

Site-to-Site VPN → Connects entire office networks across different locations.

Personal VPN → used by everyday users for privacy, hiding IP, bypassing geo-blocks.

Mobile VPN → Maintains secure connection even when switching networks.

Corporate VPN → Enterprise-Level solution with centralized control for employees.