Assignment No.04

Architectural and Networking Concepts

-Vaishnavi Jadhav

Q1. A Food based Startup wants to setup its internal network. Answer the following.

A food-based startup needs a well-planned network to ensure secure internal communication, internet access, and proper control over resources.

(a). Difference between Public IP and Private IP Address (with example)

A Food-based startup needs a network to connect its computers, billing systems, kitchen devices, and website. For this, two types of IP addresses are used — **Public IP** and **Private IP**

Parameter	**Public IP Address**	**Private IP Address**
Definition	An IP address that is accessible over the internet	An IP address used within a local or private network
Accessibility	Accessible globally via the internet	Not accessible directly from the internet
Scope	Global	Local (LAN)
Assigned By	Internet Service Provider (ISP)	Network administrator
Uniqueness	Globally unique	Unique within the local network
Security	Less secure, requires firewall protection	More secure due to restricted access
Usage	External communication	Internal communication
Example IP	203.0.113.15	192.168.1.10
Common Examples	Website server, online food ordering application	Office computers, kitchen POS systems, internal database
Common IP Address Range (IPv4)	- 10.0.0.0 – 10.255.255.255 - 172.16.0.0 – 172.31.255.255 - 192.168.0.0 – 192.168.255.255	- 1.0.0.0 – 9.255.255.255 - 11.0.0.0 – 126.255.255.255 - 128.0.0.0 – 172.15.255.255

Public IPs connect the startup to the internet for customer access, while private IPs enable secure internal communication. Using both ensures a safe and efficient network.

(b). What is a CIDR block? If the company has been assigned 192.168.0.0/24, how many usable IP addresses are available?

CIDR Block :-

CIDR (Classless Inter-Domain Routing) is a method of IP address allocation that allows flexible division of IP networks using a **prefix length** (written after /). The prefix length indicates how many bits are used for the **network portion** of the IP address.

Example format :- IP Address / Prefix Length

Given CIDR Block: 192.168.0.0/24

- /24 means **24 bits** are used for the network
- Remaining bits for hosts = **32 − 24 = 8 bits**

Total IP Addresses: 2^8 = 256 IP addresses

Reserved Addresses:

- **1 Network address** → 192.168.0.0
- **1 Broadcast address** → 192.168.0.255

Usable IP Addresses: 256−2=254 usable IP addresses

A CIDR block is a way of representing an IP network using a prefix length for efficient address allocation.For the CIDR block **192.168.0.0/24**, there are **254 usable IP addresses** available for devices in the company's network

---

(c). If a company wants to block a few websites so that employees cannot visit them using the company's internet, where can this configuration be done while setting up the network?

If a food-based startup wants to block certain websites so that employees cannot access them using the company's internet, this configuration can be done while setting up the **network security and access control system**.

The configuration is usually done at the following places:

1. **Firewall / Network Gateway**
   - The firewall acts as the main security control point of the company network.
   - Specific websites can be blocked for all employees through firewall rules.
   - **Example:** The startup blocks social media and streaming websites so that staff in the kitchen and office use the internet only for work-related purposes.
2. **Proxy Server**
   - A proxy server manages and monitors employee internet access.
   - It allows the company to block selected websites and track internet usage.
   - **Example:** Employees are allowed to access supplier portals, but entertainment websites are blocked during working hours.
3. **Router Configuration**
   - In a small food startup, basic website blocking can be done directly on router.
   - This provides simple control over employee browsing.
   - **Example:** The office router blocks gaming and video streaming sites.
4. **DNS Filtering**
   - DNS filtering prevents access to websites by blocking their domain names.
   - It is easy to configure and works for all connected devices.
   - **Example:** When an employee tries to open a blocked website, the page does not load because the domain is restricted.

By configuring **firewalls, proxy servers, routers, or DNS filtering**, a food-based startup can control employee internet usage, improve productivity, and maintain a secure and disciplined network environment.

Q2. Draw a simple diagram showing:

• A VPC with one public subnet and one private subnet.

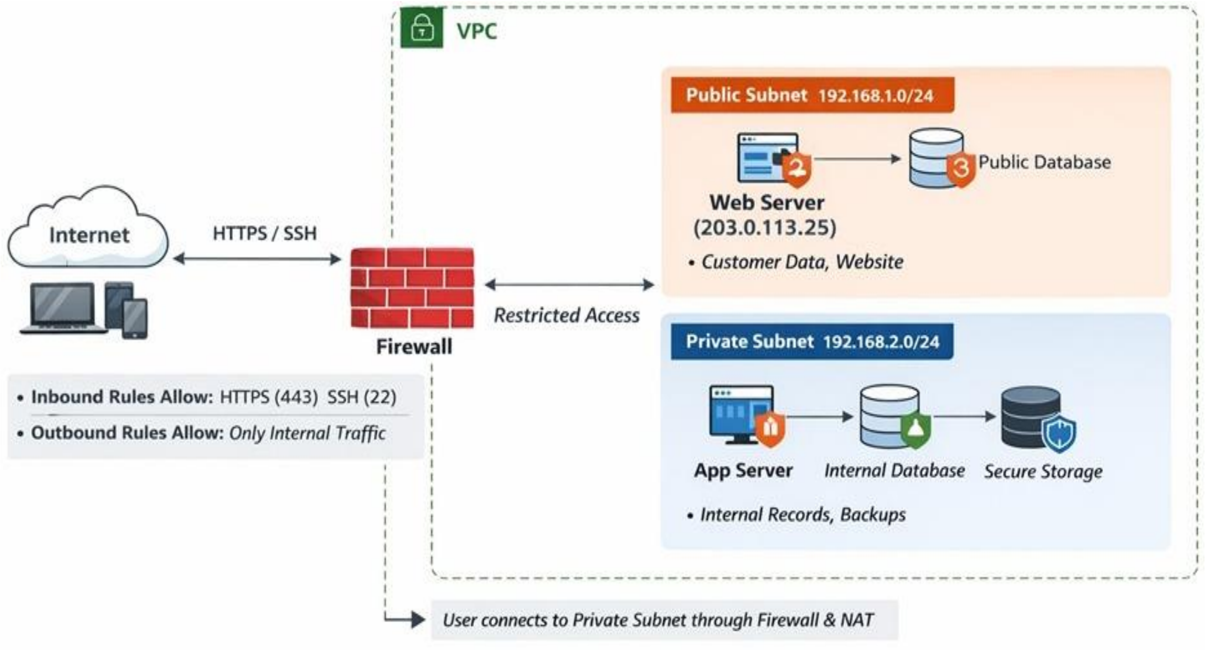
VPC
Public Subnet 192.168.1.0/24
Web Server
(203.0.113.25)
Public Database
• Customer Data, Website
Internet
HTTPS / SSH
Firewall
Restricted Access
Private Subnet 192.168.2.0/24
App Server
Internal Database
Secure Storage
• Internal Records, Backups
• Inbound Rules Allow: HTTPS (443) SSH (22)
• Outbound Rules Allow: Only Internal Traffic
User connects to Private Subnet through Firewall & NAT

Fig: The Architecture VPC with one public subnet and one private subnet

Virtual Private Cloud (VPC) :

A Virtual Private Cloud (VPC**)** is a secure, isolated virtual network in the cloud where a company can host its applications and resources. It allows control over **subnet design, IP addressing , security rules and access.**

For a food-based startup, a VPC can be divided into a **public subnet** (for internet-facing services) and a **private subnet** (for internal systems) to ensure security, performance, and proper resource management.

o Divide the IPs between public and private subnet

Given VPC CIDR: **192.168.0.0/24 → 256 IPs**

Public and Private Subnets with IP Division

- **Public Subnet:** Accessible from the internet, used for customer-facing services.
  - **IP Range:** 192.168.1.0/24
  - Example resources: Web server, public database
- **Private Subnet:** Not directly accessible from the internet, used for internal systems.
  - **IP Range:** 192.168.2.0/24
  - Example resources: Application server, internal database, backups

o Firewall with inbound and outbound rules to configure access

Firewall is used to **control traffic** between the internet, public subnet, and private subnet.

- **Inbound Rules:**
    - Allow HTTP(80) , HTTPS (443) and SSH (22) traffic to the public subnet
    - Only allow necessary traffic from the private subnet to public subnet
    - Block all other ports.
- **Outbound Rules:**
    - Public subnet can access the internet if needed
    - Private subnet communicates internally and restricted outbound internet access
    - Allow servers to access updates
    - Allow database only to respond to app server
    - Block unnecessary external traffic.

Example: Customers connect to the public web server through the firewall; internal servers communicate with the public subnet to process orders securely.

---

o Which data of an organization will reside in public and private subnet.

Data Placement in Subset :-

Subnet	Example Data / Resources
Public Subnet	Web server, online food ordering portal, public database , Load balancer , Reverse Proxy.
Private Subnet **(No Punlic IP)**	Application server, internal database, backups, secure storage,Customer records .

---

o Explain how user can reach from the internet to private subnet.

Users **cannot directly access the private subnet** for security reasons. Access happens **indirectly through the public subnet and firewall**.

Correct Access Flow:

User → Internet → Firewall → Public Web Server → App Server → Private Database

1.User Request: The user sends a request (e.g., placing an order) from the internet.

2.Request Reaches Public Web Server: The request first reaches the **public web server** in the public subnet.

3.Web Server Processes Request: The web server validates and processes the user’s request.

4. Secure Connection to Private Database: The web server connects securely to the private database or application server in the private subnet.

5. Database Sends Response: The private database sends the response back through the web server.

6. User Gets Result: The processed data or confirmation is returned to the user.

The **private subnet is protected** and **cannot be accessed directly** from the internet. All access passes through the **public layer and firewall**, ensuring secure communication and data safety.