Architectural and Networking Concepts

- *Vighnesh Brahme*

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

a) Explain the difference between public IP and private IP addresses. Give an example of when each is used.

Answer:

Feature	**Public IP Address**	**Private IP Address**
Definition	A public IP address is an address that is assigned to a device directly connected to the Internet. It is globally unique and routable across the Internet.	A private IP address is used within a local/internal network (LAN) and is not routable on the public Internet. It identifies devices internally.
Visibility	Visible to external networks and the Internet.	Visible only within the organization's internal network.
Assigned By	Assigned by Internet Service Providers (ISPs) or regional Internet registries.	Assigned manually by network administrators or dynamically via DHCP within the LAN.
Example Ranges (RFS 1918)	Examples: 8.8.8.8 (Google DNS), 13.107.42.14 (Microsoft).	Examples: 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, 192.168.0.0–192.168.255.255.
Use Case	Used for web servers, routers connected to the Internet, or cloud-hosted services that must be accessible globally.	Used for computers, printers, and internal servers inside a company's LAN.
Example cases	The startup's main Internet gateway or hosted website (e.g., www.foodstartup.com) would use a public IP address to be accessible globally.	Employees' computers and internal servers (e.g., 192.168.0.10) would use private IP addresses for communication inside the office 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?

Answer:

CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses and routing that replaces the old class-based system. It represents an IP address along with a prefix length indicating how many bits are used for the network portion.

Example:

192.168.0.0/24

/24 means 24 bits are reserved for the network, and the remaining 8 bits are available for hosts.

IP range: 192.168.0.0 → 192.168.0.255

Total IP addresses = 2^(32 - 24) = 2^8 = 256

However:

- 1 address is reserved for the network address (192.168.0.0)
- 1 address is reserved for the broadcast address (192.168.0.255)

Thus, Usable IP addresses = 256 − 2 = 254

So, the startup has 254 usable IPs available for assigning to devices within the internal 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?

Answer:

To prevent employees from accessing specific websites, filtering or blocking can be configured at various network layers. The most common and effective location is at the network gateway or firewall.

Where and How It Can Be Configured:

1. Firewall / Router Level

Configure URL filtering or domain-based blocking. The firewall inspects outbound requests (HTTP/HTTPS) and blocks connections to disallowed domains or IPs.

Example: Block facebook.com, youtube.com at the firewall's web filtering policy.

2. DNS Server Configuration

Configure the company's DNS server or use a DNS filtering service (like Cisco Umbrella or OpenDNS). When users try to resolve a blocked domain, the DNS server refuses the resolution or redirects it to a null IP.

3. Proxy Server or Web Gateway

If the company uses a proxy server, administrators can apply access control lists (ACLs) or content filtering policies on the proxy to deny traffic to specific URLs or categories.

4. Unified Threat Management (UTM) Appliance

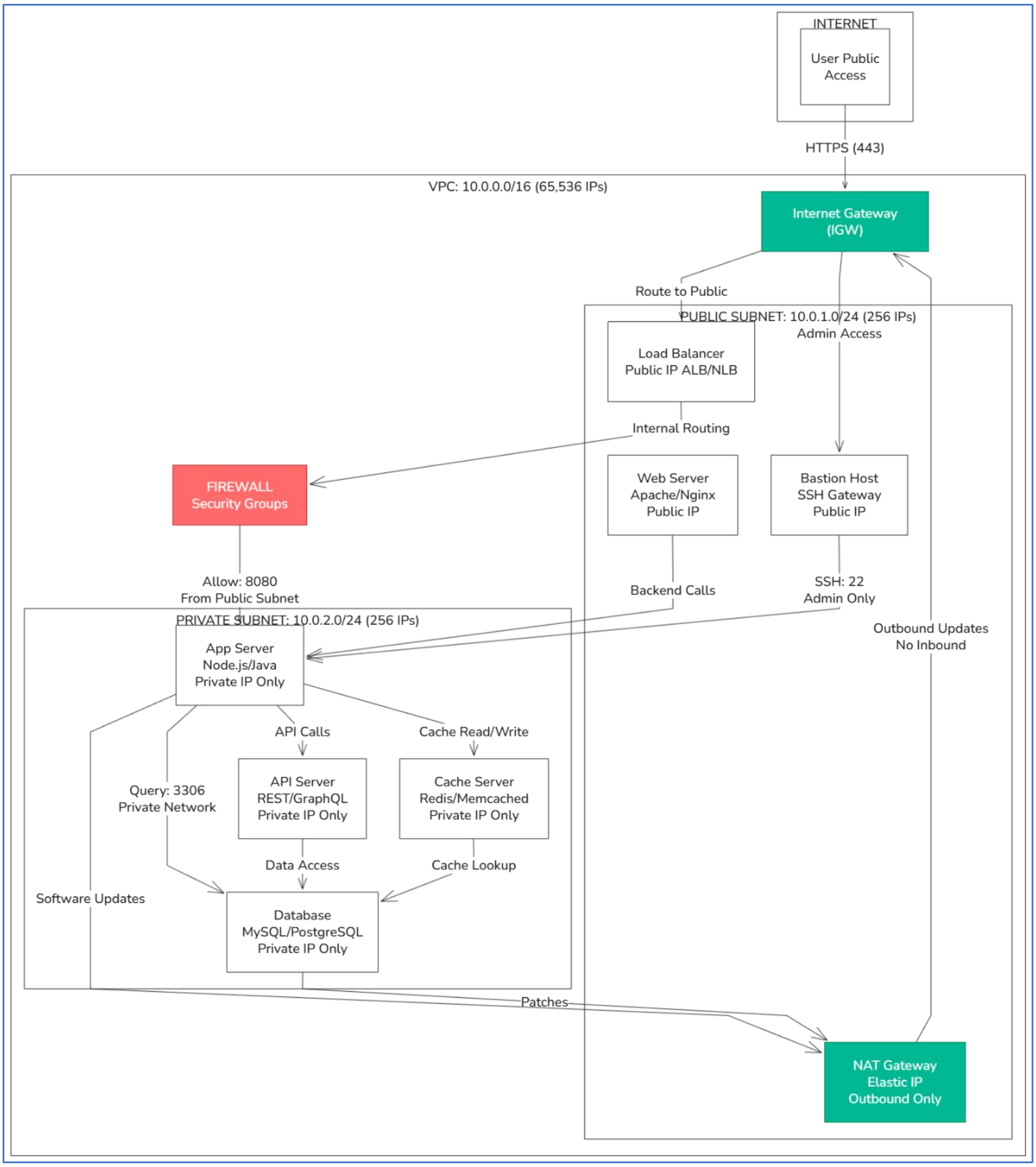
Many enterprises use UTM devices that integrate firewall, web filtering, intrusion prevention, and antivirus in one system.

Thus, my recommended approach is to implement domain blocking via the company's firewall or security gateway — this ensures centralized control, visibility, and enforceability for all users on the internal network.

Q2. Draw a simple diagram showing:

- A VPC with one public subnet and one private subnet.
    - Divide the IPs between public and private subnet
- Firewall with inbound and outbound rules to configure access
- Which data of an organization will reside in public and private subnet.
    - Explain how user can reach from the internet to private subnet.

Answer:



INTERNET
User Public Access
HTTPS (443)
VPC: 10.0.0.0/16 (65,536 IPs)
Internet Gateway (IGW)
Route to Public
PUBLIC SUBNET: 10.0.1.0/24 (256 IPs)
Admin Access
Load Balancer Public IP ALB/NLB
Internal Routing
FIREWALL Security Groups
Web Server Apache/Nginx Public IP
Bastion Host SSH Gateway Public IP
Allow: 8080 From Public Subnet
Backend Calls
SSH: 22 Admin Only
Outbound Updates No Inbound
PRIVATE SUBNET: 10.0.2.0/24 (256 IPs)
App Server Node.js/Java Private IP Only
API Calls
Cache Read/Write
Query: 3306 Private Network
API Server REST/GraphQL Private IP Only
Cache Server Redis/Memcached Private IP Only
Data Access
Cache Lookup
Software Updates
Database MySQL/PostgreSQL Private IP Only
Patches
NAT Gateway Elastic IP Outbound Only

A Virtual Private Cloud (VPC) is a logically isolated section of a cloud provider's network (e.g., AWS, Azure, GCP) where an organization can launch resources in a secure, controlled environment.

Let’s design:

- One Public Subnet (for resources accessible from the Internet — e.g., web servers)
- One Private Subnet (for internal-only resources — e.g., databases, application servers)
- Firewall / Security Groups to control inbound and outbound access
- NAT Gateway or Bastion Host to allow secure access from public to private subnet

IP Allocation Example

- VPC CIDR Block: 10.0.0.0/16 → 65,536 IPs total
- Public Subnet: 10.0.1.0/24 → for Web/App servers
- Private Subnet: 10.0.2.0/24 → for Database/Backend servers

Firewall (Security Group) Rules

Rule Type	**Direction**	**Protocol/Port**	**Source/Destination**	**Purpose**
Allow HTTP/HTTPS	Inbound	TCP 80, 443	0.0.0.0/0	Allow public access to web servers
Allow SSH	Inbound	TCP 22	Specific IP (e.g., Admin IP)	Secure admin access
Allow DB Access	Inbound	TCP 3306 (MySQL)	Public subnet only	Allow app servers to connect to DB
Allow Outbound Traffic	Outbound	All	0.0.0.0/0	Permit updates and responses

Subnet	**Data/Resource Type**	**Examples**
Public Subnet	Public-facing applications and services	Web servers, Load balancers, Bastion host
Private Subnet	Sensitive internal data and backend services	Databases, APIs, internal microservices

Internet → Private Subnet Access Path

1. User (Internet) → Public Subnet (Web Server / Bastion Host): User accesses the public IP (e.g., a web app or bastion host).

2. Public Subnet → Private Subnet: Internal communication occurs over private IPs within the VPC. Web/app servers in public subnet connect securely to databases or services in the private subnet.

3. No direct Internet access to private subnet — all traffic passes through controlled, secure routes (firewall or NAT gateway).