Day 5/13

Module 5: Networking

Date
DELTA Pg No.

#1 Introduction

Amazon Virtual Private Cloud (VPC): A logically isolated virtual network within AWS where you can securely launch and manage your cloud resources.

Subnet: A smaller segment of a VPC used to organise resources and control whether they are publicly or privately accessible.

Network Diagram: A diagram is, simply put, a schematic or map of your network in the AWS cloud. It can provide a visual of how users or applications access services, resources or data.

Components:

1. AWS Cloud: The overall global infrastructure where all AWS services run.

2. Region: A physical geographic location (for example Mumbai or Singapore). Each region contains multiple AZ.

3. Availability Zones (AZ): Separate data centers within a region. Deploying resources across multiple AZs improves high availability and

fault tolerance.

4. Amazon VPC: Your own logically isolated virtual network inside AWS where you launch and manage resources.

5. Internet Gateway (IGW): A component that connects your VPC to the public internet, allowing resources in public subnets to send and receive traffic.

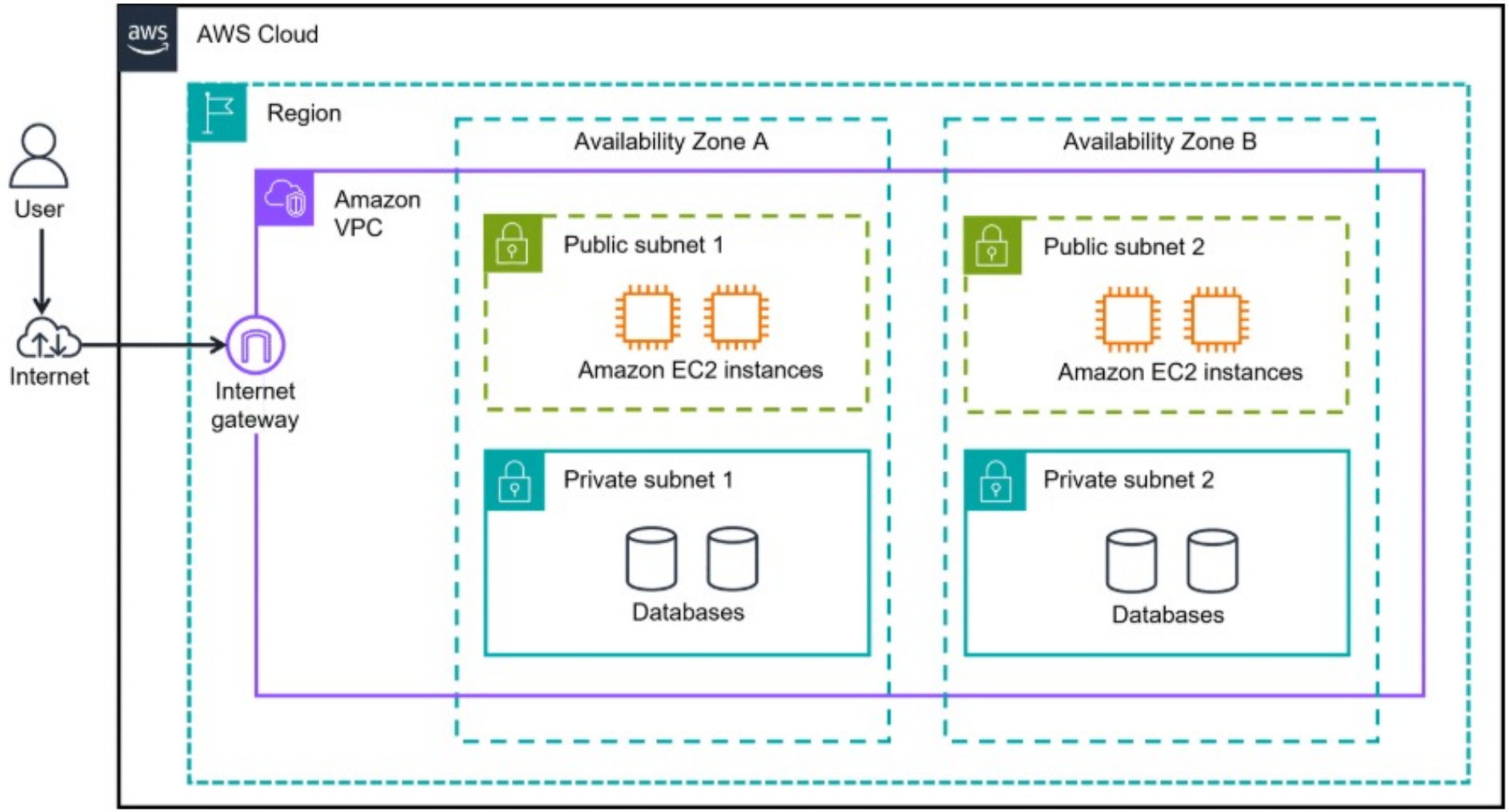
6. Public subnets: Subnets that have a route to the internet gateway. Resources like web servers can communicate directly with the internet.

7. Private subnet: Subnets without direct internet access. Typically used for sensitive resources like databases.

8. Amazon EC2 Instances: Virtual servers that run applications or websites.

9. Databases: Usually placed in private subnets for security, so they are not directly accessible from the internet.

Understanding network diagrams



To learn how network diagrams work, choose START.

Date
DELTA Pg No.

#2 Organising AWS Cloud Resources

VPC - Your own pvt network in VPC
Amazon VPC : It is used to establish boundaries around your AWS resources.

Virtual private Gateway A virtual Private Gateway allows protected internet traffic to enter into the VPC

Virtual Private Network (VPN): A VPN encrypts your internet traffic, helping protect it from anyone who might try to intercept or monitor it.

#3. More ways to connect to AWS Cloud
(i) AWS Direct Connect is a private, dedicated AWS connection to your data center or office.

(ii) AWS Client VPN connects your remote workforce to AWS or on-premises with a VPN.

(iii) AWS Site to Site VPN is an encrypted network connection to your Amazon VPCs

(iv) AWS private Link connects your VPC privately to services and resources as though they were in your VPC.

1️⃣ AWS Direct Connect

👉 Ye ek **private leased line** jaisa hota hai jo aapke office/data center ko directly AWS se connect karta hai.

- Internet use nahi hota
- Fast + stable connection
- Large companies use karti hain

📌 Simple: *Office se AWS tak direct private cable connection.*

2️⃣ AWS Client VPN

👉 Ye remote employees ke liye hota hai.

- Work from home employee VPN se connect karega
- Phir wo AWS ya office network access karega

📌 Simple: *Employee apne laptop se VPN laga ke office/AWS network me ghus jata hai.*

3️⃣ AWS Site-to-Site VPN

👉 Ye **office network aur AWS VPC** ke beech secure tunnel banata hai.

- Internet ke through connection hota hai
- Lekin encrypted hota hai

📌 Simple: *Office router aur AWS ke beech permanent secure tunnel.*

4️⃣ AWS PrivateLink

👉 Isse aap apne VPC se kisi AWS service ko **internet use kiye bina** access kar sakte ho.

- Traffic AWS network ke andar hi rehta hai
- Zyada secure

📌 Simple: *AWS ke andar hi private raasta bana diya jata hai service tak.*

Date
DELTA Pg No.

4 Subnets, security Groups, and Network Access control Lists

(i) Subnet bas Network ka partition hota hai
- Public Subnet → internet access possible
- private subnet → direct internet access nahi

Subnet khud security control nahi karta.
Security control ka kaam aata hi security Group and NACL ka.

(ii) Security Group (Stateful)
Ye EC2 instance ka level par firewall hota hai

Stateful: Agar Incoming traffic allow kiya to uska return automatically allowed hoga.

(iii) Network ACL (Stateless)
Ye subnet ke level pe firewall hota hai
Stateless: Ye kuch yaad nahi rakhta.
Agar Incoming allow kiya to outgoing ke liye alag rule banana padega

5 Amazon VPC Demo

Feature	Security Groups	Network ACLs
Scope	Instance level (attached to EC2 instances)	Subnet level (associated with subnets)
State	Stateful (remembers state)	Stateless (doesn't remember state)
Rule types	Only allow type rules	Both allow and deny type rules
Return traffic	Return traffic is automatically allowed if inbound traffic is allowed	Return traffic must be implicitly allowed in both directions
Uses	Fine-grained control of traffic for individual EC2 instances	Broad control of traffic in and out of subnets

#6 Global Networking

(I) Amazon Route 53
It is a DNS service that helps users find your website by translating your domain name (like example.com) in to an IP Address
→ It connects users to your website.

(II) Amazon Cloudfront
It is a CDN that delivers your websit content (images, videos, files) faster by caching it in locations closer to users.
Simple: It makes your website load faster worldwide.

(III) AWS Global Accelerator
It improves application performance and availabili- by routing traffic through AWS's global network to the nearest healthy endpoint.
→ It sends users to the fastest and the healthiest server.

Route 53 → Find the website.
Cloudfront → Speed up the content
Global Accelerator → Optimise traffic path.