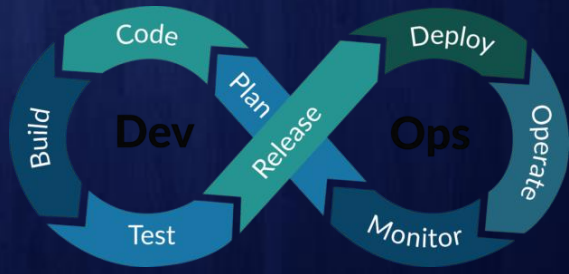
AWS SAA + SysOps + Developer + DevOps Course #Day-21

We will start at 8 AM,
Stay tuned



RAKESH TANINKI
LEARN TO UNLEARN

Recap:

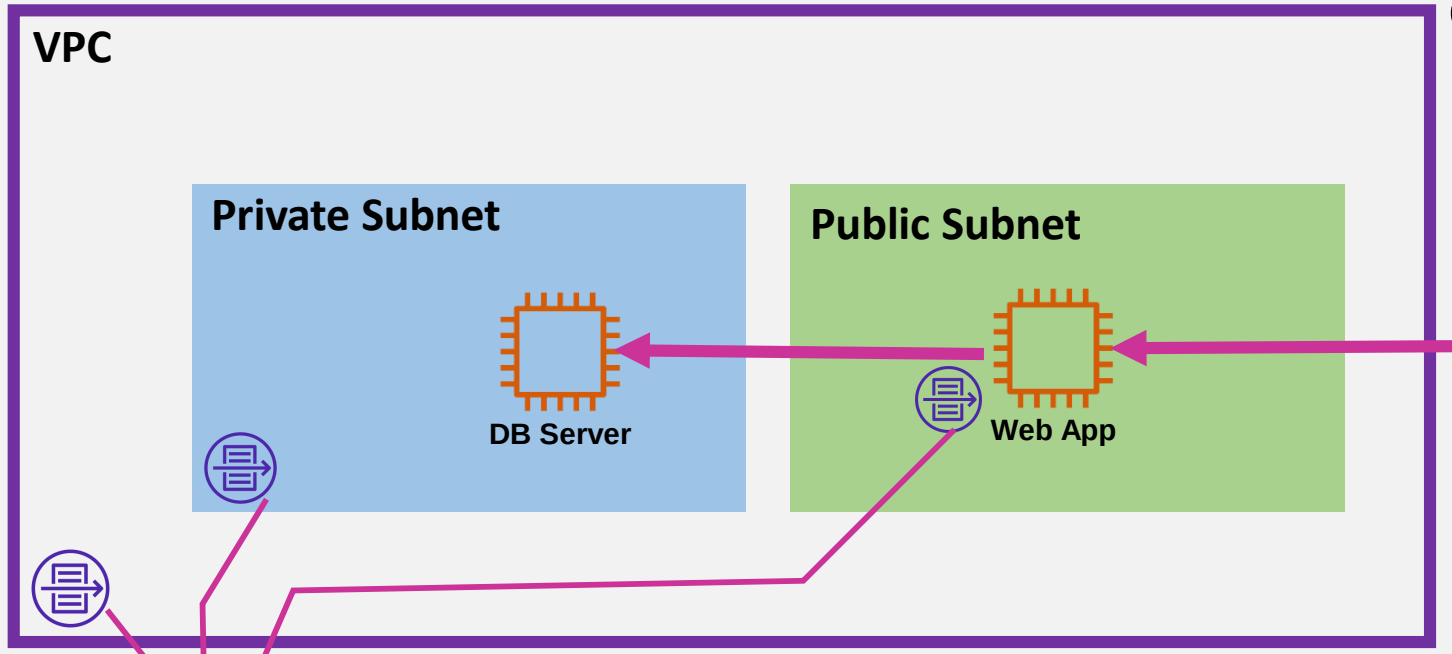
- Hybrid Networking
  - S/w VPN
  - Hardware VPN – S2S
  - Direct Connect
- Demo
  - S/w VPN
  - S2S - project

Today's topics:

- VPC
  - Flow Logs
  - Private Endpoints
    - Gateway
    - Interface
  - Peering
- Demos

VPC Flow Logs

VPC Flow Logs



Flow logs can capture ACCEPTED, REJECTED or ALL metadata

VPC

Subnets

ENIs

S3 Bucket

Flow log record

Cloud Watch logs

2 ACC-ID eni-ID 109.18.34.78 10.0.0.6 1337 443 6 4 336 1425364578 1245356852 ACCEPT OK

VPC Flow Logs

- Capture **metadata** (**Not contents**)
- Source IP, Dest IP, Packet size, Source port, Dest port
- Attached to a **VPC** – **All ENIs** in that **VPC**
- .. **Subnet** – All ENIs in that **subnet**
- .. **ENIs directly**
- Flow logs are not real time
- Log destinations .. **S3** or **cloud watch logs**
- .. Athena for querying the data

VPC Flow Logs

<version>
<account-id>
<interface-id>
<srcaddr>
<dstaddr>
<srcport>
<dstport>
<protocol>
<packets>
<bytes>
<start>
<end>
<action>
<log-status>

2 ACC-ID eni-ID 109.18.34.78 10.0.0.6 1337 443 6 4 336 1425364578 1245356852 ACCEPT OK

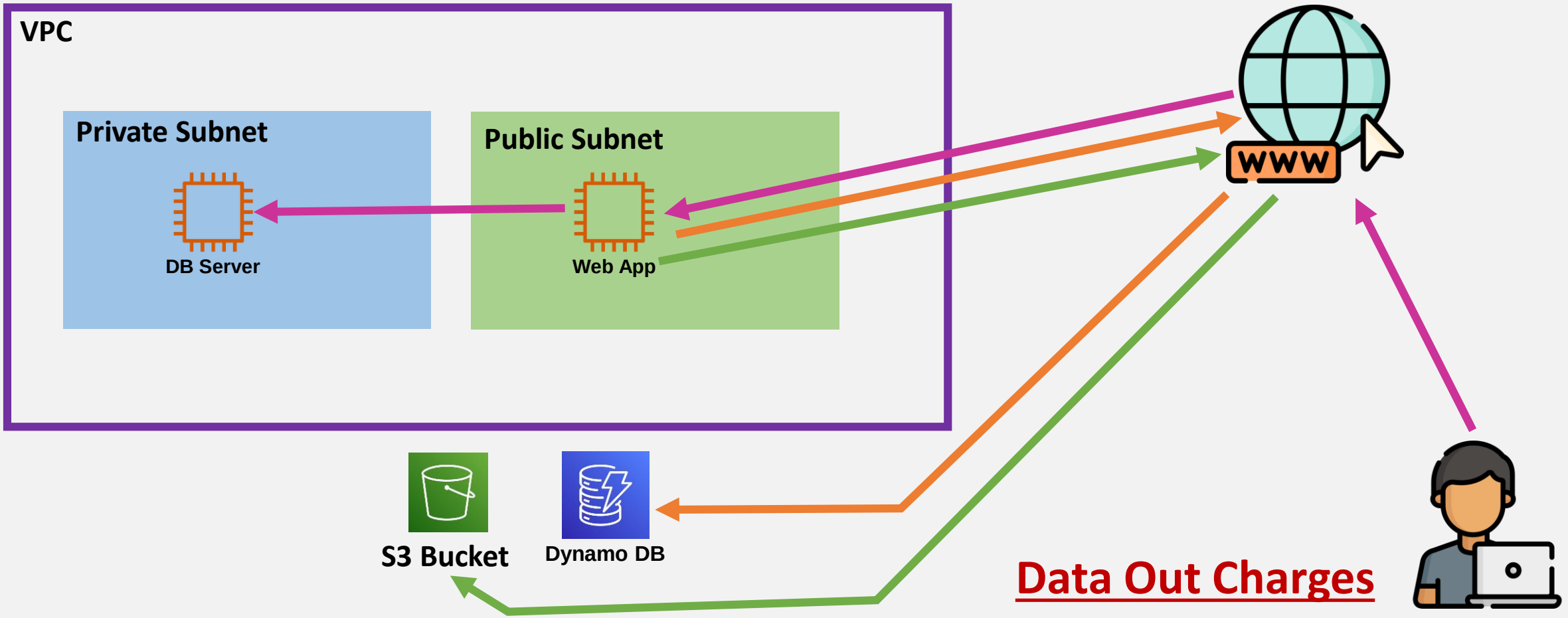
2 ACC-ID eni-ID 109.18.34.78 10.0.0.6 1337 3306 6 4 336 1425364578 1245356852 REJECT OK

VPC Flow Logs - Demo

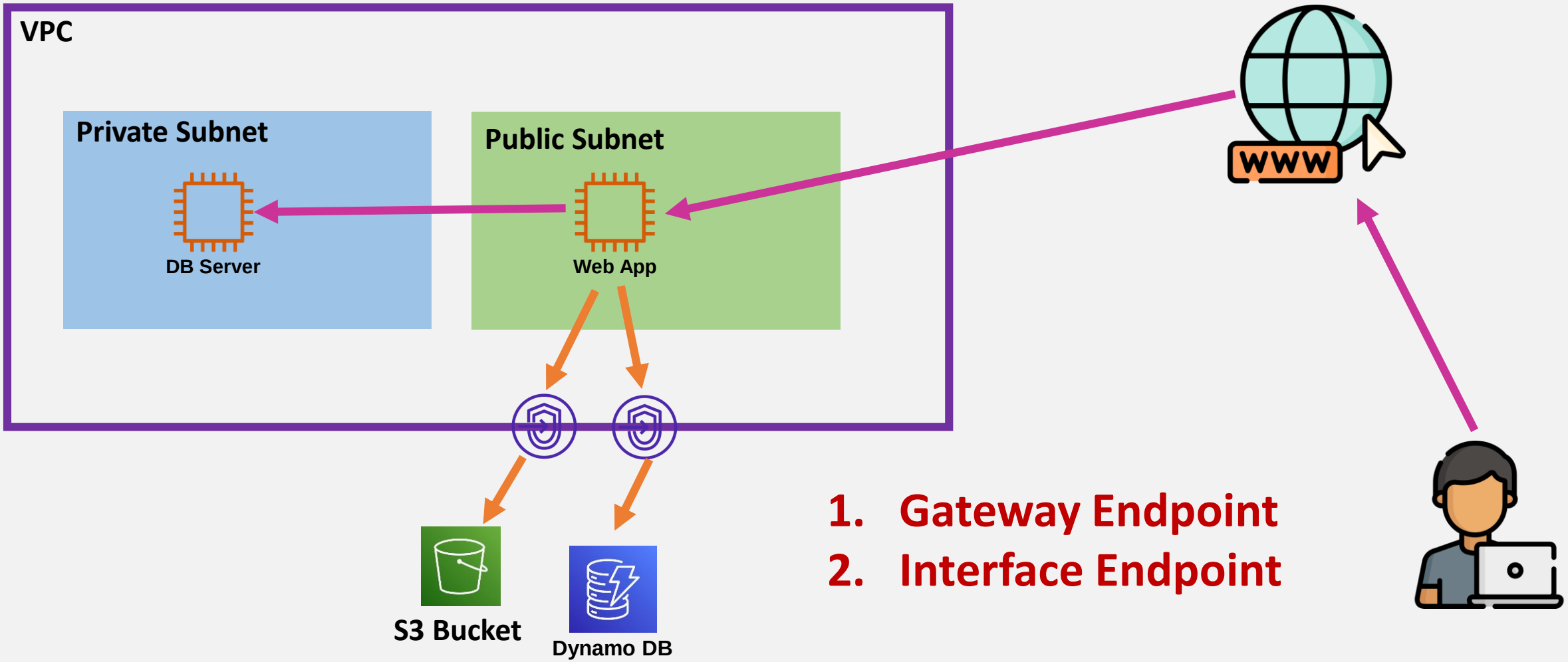
- Enable Flow logs
- Connect to EC2
- Review
- Disable

VPC Endpoints

VPC Private Endpoints



VPC Private Endpoints



VPC Private Endpoints (Gateway)

- Provide **private access** to **S3** and **Dynamo DB**
- Added to VPC, Highly available (**HA**) across all AZs in a region by default
- **Endpoint policy** is used to control what it can access
- Regional .. **Can’t access cross regional** services

VPC Private Endpoints (Interface)

- Provide **private access** to all AWS Public services
- Added to **specific subnet** – an **ENI** – **not HA**
- For HA .. add **one endpoint**, to **one subnet**, **per AZ** used in the VPC
- Network access controlled via **Security Groups**
- **Endpoint policies** – restrict what can be done with endpoint
- Only **TCP** and **IPv4**

VPC Private Endpoints (Interface)

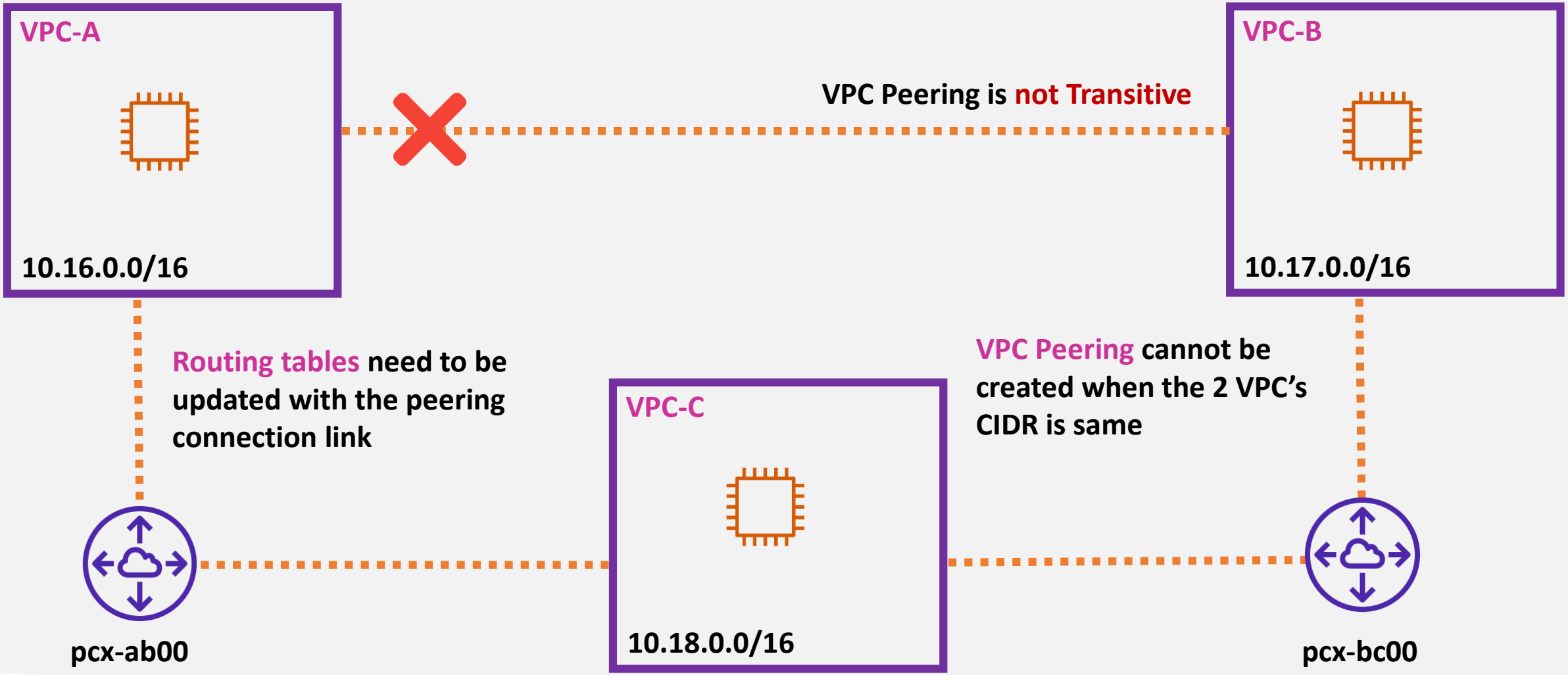
- Endpoint provides a new service endpoint DNS
- Eg: **vpce-123-xyz.s3.ap-south-1.vpce.amazonaws.com**
- Endpoint **Regional DNS**
- Endpoint **Zonal DNS**

VPC Endpoints - Demo

- Gateway Endpoints
- Interface endpoints

VPC Peering

VPC Peering



VPC Peering

- Direct encrypted network link between **two VPCs**
- Works **same**/**cross region**, and **same**/**cross account**
- VPC peering doesn’t support **transitive peering**
- **Routing** configuration needed, **SGs** & **NACLs** can filter

VPC Peering - Demo

- 3 VPCs
- Peering b/w 3 VPCs
- 1 EC2 in each VPC
- Connect from one EC2 to another

Thank you, will meet in tomorrow's session