

# Production-Grade Cloud Networking Project

## AWS VPC Design with Multi-Size Subnets & Controlled Internet Access

**STEP 1:** Steps to open **VPC** in AWS Console :

1. Login to **AWS** Console.
2. Make sure the region is **Asia Pacific (Mumbai)**.
3. In the search bar, type **VPC**.
4. Click on **VPC – Isolated Cloud Resources**.
5. You will be redirected to the **VPC Dashboard**.
6. From left menu you can create:
  - VPC
  - Subnets
  - Route Tables
  - Internet Gateway
  - NAT Gateway
  - Security Groups
  - NACLs



**STEP 2:** create a VPC, next steps:

1. Click **Create VPC**.
2. Select **VPC only**.
3. Enter CIDR (example: 10.0.0.0/16).
4. Click **Create VPC**.

**Resources to create** [info](#)  
 Decide only the VPC resources or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

**Name tag - optional**  
 Creates a tag with a key of 'Name' and a value that you specify.

my-vpc-01

**IPv4 CIDR block** [info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

**IPv4 CIDR**  
 10.0.0.0/16  
CIDR block size must be between /16 and /28.

**IPv6 CIDR block** [info](#)  
☒ No IPv6 CIDR block  
☐ IPAM-allocated IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block  
☐ IPv6 CIDR owned by me

**Tenancy** [info](#)  
 Default

**VPC encryption control (S)** [info](#)  
 Monitor mode provides visibility into encryption status without blocking traffic. Enforce mode prevents unencrypted traffic. [Additional changes apply](#)

☒ None ☐ Monitor mode ☐ Enforce mode

**Tags**  
 A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

**Key** **Value - optional**

Q Code X Q Aja Vpc X Remove tag

Add tag

You can add 40 more tags.

Cancel Preview code Create VPC

### STEP 3: Create and attach an **Internet Gateway (IGW)** in AWS:

Search [All+5] top

Internet gateways > Create internet gateway

**Create internet gateway** [info](#)  
 An internet gateway is a virtual router that connects a VPC to the Internet. To create a new internet gateway specify the name for the gateway below.

**Internet gateway settings**

**Name tag**  
 Creates a tag with a key of 'Name' and a value that you specify.

Aja IGW

**Tags - optional**  
 A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

**Key** **Value - optional**

Q Name X Q Aja IGW X Remove

Add new tag

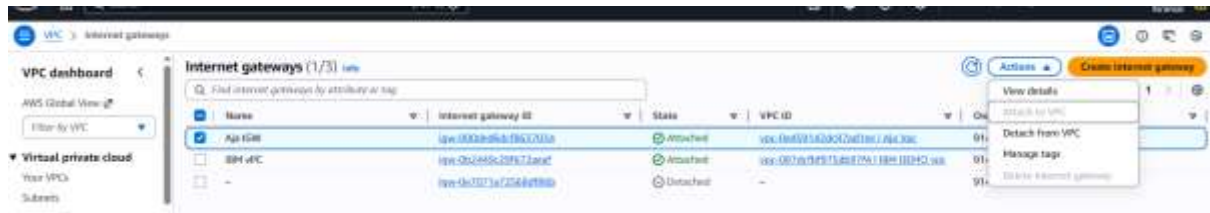
You can add 40 more tags.

Cancel Create internet gateway

#### A. Create Internet Gateway

1. Go to **VPC Dashboard**.
2. Click **Internet Gateways** (left menu).
3. Click **Create internet gateway**.
4. Enter **Name tag** → Aja IGW
5. (Optional) Add tags.
6. Click **Create internet gateway**.

## B. Attach Internet Gateway to VPC



7. Select the created IGW
8. Click **Actions** → **Attach to VPC**.
9. Choose your VPC (example: Aja-VPC or 10.0.0.0/16).
10. Click **Attach internet gateway**.

## C. Add Route to Public Subnet

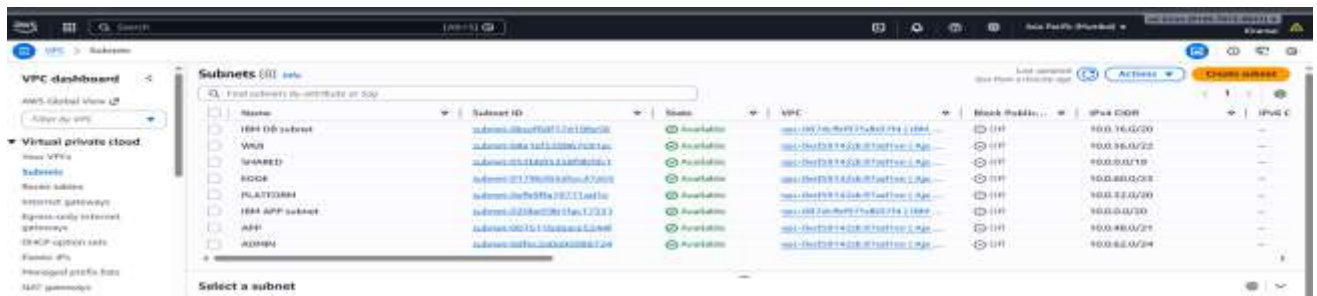
11. Go to **Route Tables**.
12. Select your **Public Route Table**.
13. Click **Edit routes** → **Add route**.
14. Destination: 0.0.0.0/0
15. Target: **Internet Gateway (Aja IGW)**.
16. Click **Save routes**.

Now your **public subnet** has internet access.

### STEP 4: To create the Subnet

1. Go to **VPC Dashboard**.
2. Click **Subnets** → **Create subnet**.
3. Select your **VPC** (example: 10.0.0.0/16).
4. Under **Subnet 1 of 3**:
  - **Subnet name**: SHARED
  - **Availability Zone**: Select **No preference** (or choose ap-south-1a if needed)
  - **IPv4 VPC CIDR block**: 10.0.0.0/16
  - **IPv4 subnet CIDR block**: 10.0.0.0/19  
(This gives 8,192 IPs)
5. Tags (optional):
  - Key: Name
  - Value: SHARED
6. Click **Create subnet**.

If you are creating 6 subnets.



### Subnet 1 of 3

#### Subnet name

Create a tag with a key of 'Name' and a value that you specify.

SHARED

The name can be up to 256 characters long.

#### Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

#### IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

#### IPv4 subnet CIDR block

10.0.0.0/19

8,192 IPs

#### Tags - optional

##### Key

Name

##### Value - optional

SHARED

Remove

Add new tag

You can add 49 more tags.

Remove

10
.
0
.
0
.
0
/
19

0 0 0 0 1 0 1 0

255.255.224.0

**Netmask**

8,192

**Count**

0 0 0 0 0 0 0 0

10.0.0.0

**CIDR Base IP**

10.0.0.1

**First Usable IP**

0 0 0 0 0 0 0 0

10.0.31.255

**Broadcast IP**

10.0.31.254

**Last Usable IP**

Copy CIDR

Copy Share Link

### Subnet 2 of 3

#### Subnet name

Create a tag with a key of 'Name' and a value that you specify.

PLATFORM

The name can be up to 256 characters long.

#### Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

#### IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

#### IPv4 subnet CIDR block

10.0.32.0/20

4,096 IPs

#### ▼ Tags - optional

### STEP 5 : Create Route Table

1. Go to **VPC Dashboard**.
2. Click **Route Tables** (left side).
3. Click **Create route table**.
4. In **Name**: AJA Public RT
5. Select **VPC**: Aja VPC (10.0.0.0/16)
6. Tags:
  - Key: Name
  - Value: AJA Public RT
7. Click **Create route table**.

### B. Add Internet Route

8. Select the created route table (AJA Public RT).
9. Go to **Routes** tab → Click **Edit routes**.
10. Click **Add route**:
  - Destination: 0.0.0.0/0
  - Target: **Internet Gateway (Aja IGW)**
11. Click **Save routes**.

## Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

### Route table settings

#### Name - optional

Create a tag with a key of 'Name' and a value that you specify.

AJA Public RT

#### VPC

The VPC to use for this route table.

vpc-0ed59142dc97ad1ee (AJA Vpc)

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

#### Key

Q Name

X

#### Value - optional

Q AJA Public RT

X

Remove

Add new tag

You can add 40 more tags.

Cancel

Create route table

<input checked="" type="checkbox"/>	AJA Private RT	<a href="#">rtb-0a59d51d894d8a38</a>	...	...	Yes	<a href="#">vpc-0ed59142dc97ad1ee   AJA ...</a>	914970130631
<input type="checkbox"/>	...	<a href="#">rtb-09a9d56bb406ad67</a>	...	...	Yes	<a href="#">vpc-0870c7b975db97f4   IBN ...</a>	914970130631
<input type="checkbox"/>	...	<a href="#">rtb-0f65f149bba4fcda</a>	...	...	Yes	<a href="#">vpc-07cec576949c8663</a>	914970130631
<input checked="" type="checkbox"/>	AJA Public RT	<a href="#">rtb-0c7d708fca3088713</a>	...	...	No	<a href="#">vpc-0ed59142dc97ad1ee   AJA ...</a>	914970130631

## C. Associate with Public Subnet

12. Go to **Subnet associations** tab.
13. Click **Edit subnet associations**.
14. Select your **Public subnet**.
15. Click **Save associations**.

Now your public subnet can access the internet.

VPC

Route tables

VPC dashboard

Virtual private cloud

Security

PrivateLink and Lattice

Find route tables by attribute or tag

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC	Owner ID
IBM Route APP	rtb-02964c793a655339	subnet-0286a09615ae17...	-	No	vpc-087a6b975da97f94...	914970130631
IBM Route City	rtb-0a07a186a33c5a5c5d	subnet-0bce989f17d199a...	-	No	vpc-087a6b975da97f94...	914970130631
AJA Private RT	rtb-0a07a186a33c5a5c5d	-	-	Yes	vpc-0e59142a97aef1ee...	914970130631
-	rtb-0a07a186a33c5a5c5d	-	-	Yes	vpc-087a6b975da97f94...	914970130631
-	rtb-0a07a186a33c5a5c5d	-	-	No	vpc-07ac1576948c8655	914970130631
AJA Public RT	rtb-0c7d708fca3088723	-	-	No	vpc-0e59142a97aef1ee...	914970130631

rtb-0c7d708fca3088723 / AJA Public RT

DetailsRoutesSubnet associationsEdge associationsRoute propagationTags

Explicit subnet associations (0)

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
------	-----------	-----------	-----------

## Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/5)

Filter subnet associations

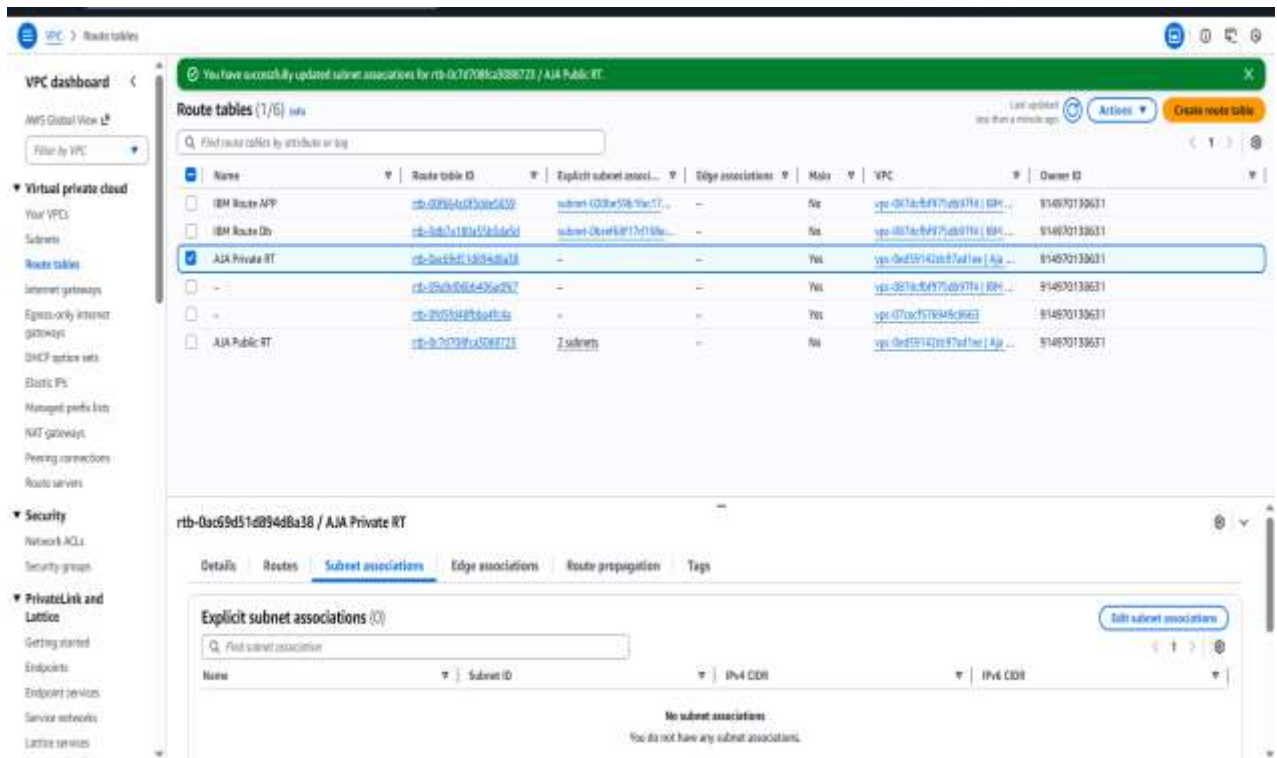
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
WEB	subnet-08e1ef539867a91ae	10.0.56.0/22	-	Main (rtb-0a07a186a33c5a5c5d)
SHARED	subnet-053b605258f8b4d1	10.0.0.0/19	-	Main (rtb-0a07a186a33c5a5c5d)
EDGE	subnet-01796265d5cc47a55	10.0.60.0/23	-	Main (rtb-0a07a186a33c5a5c5d)
PLATFORM	subnet-0e1f9b915771aef1e	10.0.32.0/20	-	Main (rtb-0a07a186a33c5a5c5d)
APP	subnet-007511bdacac5244f	10.0.48.0/21	-	Main (rtb-0a07a186a33c5a5c5d)
ADMIN	subnet-0d9ec2a0a95088724	10.0.62.0/24	-	Main (rtb-0a07a186a33c5a5c5d)

Selected subnets

subnet-0d9ec2a0a95088724 / ADMIN X

subnet-01796265d5cc47a55 / EDGE X

Cancel Save associations



**STEP 6:** To add Internet Gateway route:

1. Go to **VPC Dashboard**
2. Click **Route Tables**
3. Select your route table
4. Click **Routes** tab
5. Click **Edit routes**

Now add this:

6. Click **Add route**
7. In **Destination** → enter 0.0.0.0/0
8. In **Target** → select **Internet Gateway (igw-xxxxxx)**

You will see:

- 10.0.0.0/16 → local (already there, don't change)
- 0.0.0.0/0 → igw-xxxxxx

9. Click **Save changes**

Now this subnet becomes **Public Subnet** (it has internet access).



**Edit routes**

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>			
	Internet Gateway		No	CreateRoute
	<input type="text" value="igw-000de6dc18637034"/>			
	Use: "igw-000de6dc18637034"			
	igw-000de6dc18637034 (Aja VPC)			

**STEP 7:** You are in **Route Table** → **Edit routes**.

Right now it has only one rule:

**10.0.0.0/16 → local**

This means:

- All computers (EC2) inside your VPC can talk to each other.
- They **cannot go to the internet yet**.

**Edit routes**

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>			

**STEP 8:** Instance creation for Validation and Testing

Simple steps to launch EC2 in your VPC:

1. Go to **EC2** → **Instances** → **Launch instance**
2. Select **AMI**: Ubuntu 24.04
3. Select **Instance type**: t3.micro
4. In **Network settings**:
  - VPC: **Aja VPC (10.0.0.0/16)**
  - Subnet: **WEB (Public Subnet)**
  - Auto-assign Public IP: **Enable**

5. Create **Security Group**:
  - Allow **SSH (22)** from **0.0.0.0/0**
6. Select or create **Key Pair**
7. Click **Launch instance**

**Network settings**

VPC - required  
vpc-0ed59142dc97aaf1ee (Ap-Northeast-1)

Subnet  
subnet-08a1ef539867c01as (Ap-Northeast-1) Create new subnet

Auto-assign public IP  
Enable

Firewall (security group)  
Create security group Select existing security group

Security group name - required  
launch-wizard-5

Description - required  
launch-wizard-5 created 2026-01-28T11:40:57-06:00

Inbound Security Group Rules  
Security group rule 1 TCP: 22, 0.0.0.0/0

**Summary**

Number of instances: 1

Software image (AMI)  
Amazon Linux 2 AMI, 2023.09.0, x86\_64, read more

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GB

Cancel Launch instance Preview code

## Private Subnet Validation

- EC2 instances in Web/App/Platform/Shared:
  - Cannot reach the internet
  - Can communicate internally

**Why:** No route to IGW exists



**Network settings**

VPC - required  
vpc-0ed59142dc97aaf1ee (Ap-Northeast-1)

Subnet  
subnet-08a1ef539867c01as (Ap-Northeast-1) Create new subnet

Auto-assign public IP  
Enable

Firewall (security group)  
Create security group Select existing security group

Security group name - required  
launch-wizard-5

Description - required  
launch-wizard-5 created 2026-01-28T11:40:57-06:00

**Summary**

Number of instances: 1

Software image (AMI)  
Amazon Linux 2 AMI, 2023.09.0, x86\_64, read more

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GB

Cancel Launch instance Preview code

## Public Subnet Validation

- **EC2 instances in Admin/Edge can:**
  - Resolve DNS
  - Reach external IPs
  - Access the internet

**Why:** Route table contains 0.0.0.0/0 → IGW

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
```

```
To run a command as administrator (user "root"), use "sudo <command>". See "man sudo_root" for details.
```

```
ubuntu@ip-10-0-62-248:~$
```