



[NextWork.org](https://NextWork.org)

# Build a Virtual Private Cloud



Anitta Philip

A large, dark blue cloud shape centered on a solid blue background. Inside the cloud, the letters 'VPC' are written in a large, white, sans-serif font.

VPC



Anitta Philip

<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

# Introducing Amazon VPC!

## What it does & how it's useful

Amazon Virtual Private Cloud (VPC) is a customizable network space in AWS that allows you to launch AWS resources in a virtual network. Developers and teams use Amazon VPC because it offers isolation, security, and control over network configurations.

## How I'm using it in today's project

I'm using Amazon VPC in this project to demonstrate how to create a customizable network space in AWS, set up subnets, and attach an internet gateway. This tutorial aims to provide a step-by-step guide for enabling auto-assign public IPs and configuring network settings.

## This project took me...

The project took me less than an hour to complete. Documentation took me less than an hour to write as well.



Anitta Philip

<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

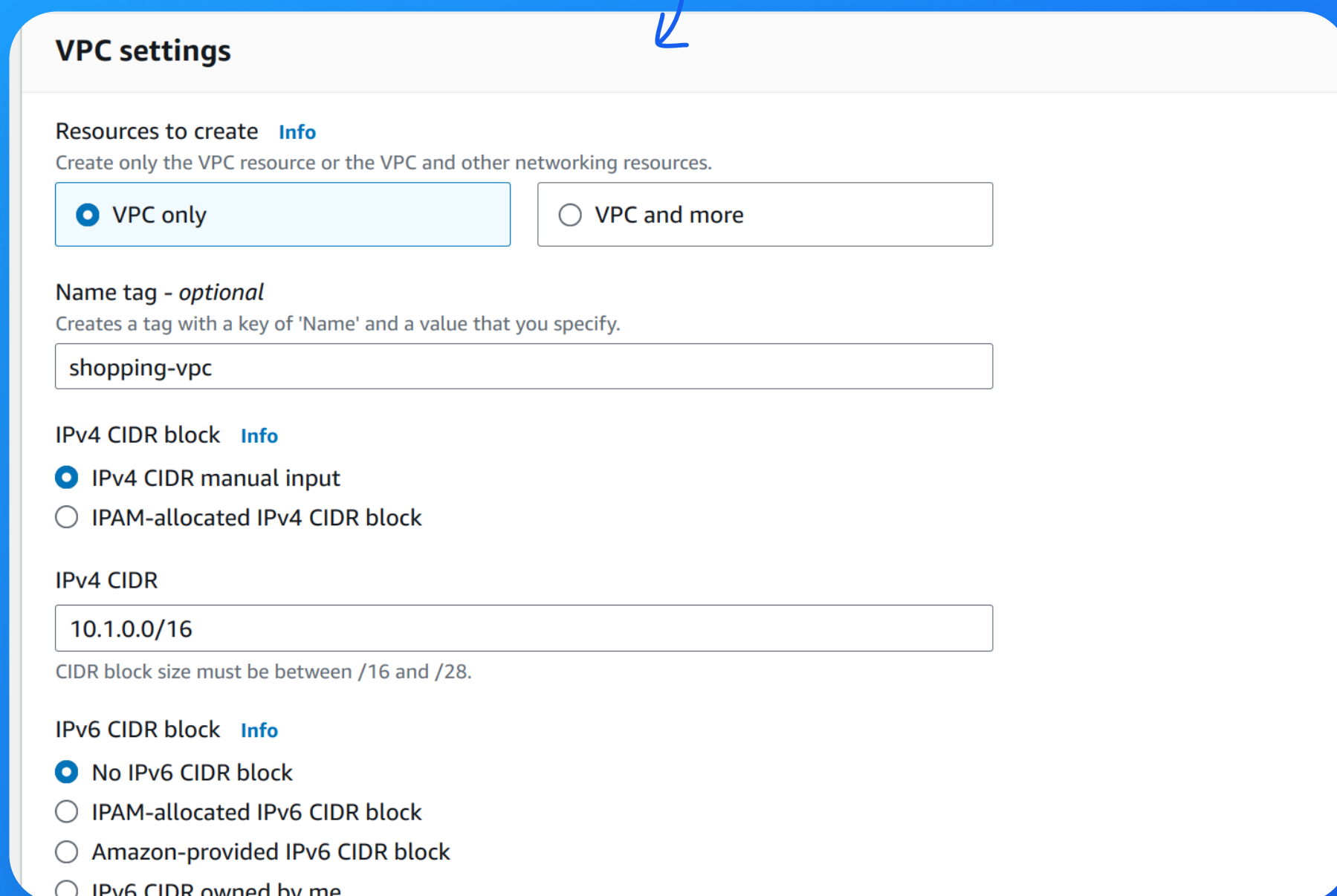
# My first VPC

VPCs are customizable network spaces in AWS that allow you to launch and manage AWS resources within a virtual network.

There was already a default VPC in my account ever since my AWS account was created. This is because AWS automatically provides a default VPC in each region to simplify networking setup for new users.

To set up my VPC, I had to define an IPv4 CIDR, which means specifying an IP address range for the network, such as 10.1.0.0/16, to segment and organize the network space efficiently.

My VPC setup page



**VPC settings**

Resources to create [Info](#)  
Create only the VPC resource 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.

shopping-vpc

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.1.0.0/16

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



Anitta Philip

<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

# Subnets

- Subnets are subdivisions of a VPC's IP address range, used to segment the network for better management and security.
- There are already subnets existing in my account, one for every availability zone in the region. AWS provides multiple subnets to enhance redundancy and availability of resources.
- For a subnet to be considered public, it has to be associated with a route table that has a route to an internet gateway. Conversely, subnets without such a route are private subnets.

My created subnet!



Subnet name

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

shopping-subnet1-ap-south-1a

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.

Asia Pacific (Mumbai) / ap-south-1a

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.

10.1.0.0/16

IPv4 subnet CIDR block

10.1.0.0/1816,384 IPs

< > ^ v

Tags - optional

Key

Value - optional

Q Name X

Q shopping-subnet1-ap-south-1a X

Remove

Add new tag

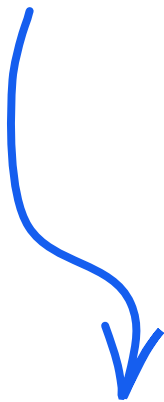


I created four subnets in total: two in ap-south-1a, one in ap-south-1b, and one in ap-south-1c, leveraging all three availability zones in the Mumbai region. The subnets are as follows:

- ap-south-1a: 10.1.0.0/18 and 10.1.192.0/18
- ap-south-1b: 10.1.64.0/18
- ap-south-1c: 10.1.128.0/18

I chose these IP ranges to ensure even distribution and to maximize the available IP addresses within the VPC. Using a Class A IP range (10.1.0.0/16) offers the benefit of a larger address space, which is advantageous for scalability and flexibility in a growing network.

Multiple subnets can be attached to the same availability zone, as I did with ap-south-1a. However, this can lead to potential resource contention and less fault tolerance within that zone. It's important to balance subnets across availability zones to avoid single points of failure.



Subnets (4) Info

Last updated 1 minute ago

Actions

Create subnet

Find resources by attribute or tag

Subnet ID : subnet-08f1d56e6668058d4 Subnet ID : subnet-00890d42e5d022448 Subnet ID : subnet-0e9f6a52a8095c495 Show more (+1)

Clear filters

	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	shopping-subnet4-ap-south-1a	subnet-0700e2844279443ce	Available	vpc-0c16ba27abf589abd   shop...	10.1.192.0/18
<input type="checkbox"/>	shopping-subnet2-ap-south-1b	subnet-00890d42e5d022448	Available	vpc-0c16ba27abf589abd   shop...	10.1.64.0/18
<input type="checkbox"/>	shopping-subnet1-ap-south-1a	subnet-08f1d56e6668058d4	Available	vpc-0c16ba27abf589abd   shop...	10.1.0.0/18
<input type="checkbox"/>	shopping-subnet3-ap-south-1c	subnet-0e9f6a52a8095c495	Available	vpc-0c16ba27abf589abd   shop...	10.1.128.0/18



Anitta Philip

<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

# Internet gateways

- Internet gateways are AWS-managed resources that allow instances within a VPC to connect to the Internet.
- Attaching an internet gateway to a VPC means enabling internet connectivity for instances within the VPC that have public IP addresses assigned.
- While I've set up an internet gateway and attached it to a VPC, I still have to set up route tables. Route tables will need to be configured to direct internet-bound traffic (`0.0.0.0/0`) to the attached internet gateway, enabling instances to communicate with the internet

My created 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.

### 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*



Remove

Add new tag

You can add 49 more tags.





Anitta Philip

<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

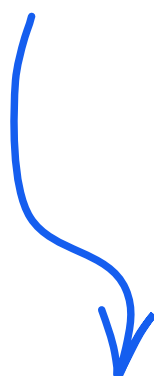
# Attach to vpc

Now we need to attach the newly created internet gateway to our vpc.

To attach an internet gateway to a vpc :

- Right-click on the Internet gateway
- Select attach to VPC
- Select the VPC > Attach internet gateway

By following these steps, you enable internet connectivity for your VPC instances, allowing them to access the internet and be accessed from the internet if they have public IP addresses assigned.



[VPC](#) > [Internet gateways](#) > [Attach to VPC \(igw-00a7b0a3a9ed5311a\)](#)

## Attach to VPC (igw-00a7b0a3a9ed5311a) [Info](#)

**VPC**

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

▶ AWS Command Line Interface command

Cancel

Attach internet gateway



Anitta Philip

<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

# Enable auto-assign public IPv4 address

When you enable auto-assign public IPv4 address for a subnet, any EC2 instance launched in that subnet will automatically receive a public IP address. This makes the instance accessible from the internet without needing to manually assign a public IP.

To attach Enable auto-assign public IPv4 address:

- Right-click the subnet
- Select edit subnet settings
- Enable auto-assign public IPv4 address




[VPC](#) > [Subnets](#) > [subnet-0700e2844279443ce](#) > Edit subnet settings


## Edit subnet settings [Info](#)

### Subnet

Subnet ID

 subnet-0700e2844279443ce

Name

 shopping-subnet4-ap-south-1a

### Auto-assign IP settings [Info](#)

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

☒ Enable auto-assign public IPv4 address [Info](#)





Anitta Philip

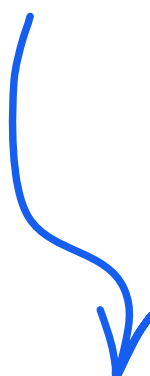
<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

# Update Route Tables

A route table in AWS defines rules that determine where network traffic from instances within a VPC is directed. It maps destination IP addresses to specific destinations, such as other subnets within the VPC, virtual private gateways, or internet gateways. By configuring route tables, you control how network traffic flows between different parts of your VPC and external networks like the internet.

- After attaching the IGW, update the route tables associated with your VPC.
- Edit the route table that your public-facing subnets use.
- Add a route (0.0.0.0/0) pointing to the newly attached IGW. This tells your VPC how to route internet-bound traffic.



Q 0.0.0.0/0 X	Internet Gateway ▼	✓ Active	No	Remove
Q igw [REDACTED] X				
Add route				
				Cancel Preview Save changes



Anitta Philip

<https://www.linkedin.com/in/anittap/>

[NextWork.org](https://NextWork.org)

# My key learnings

1

If AWS didn't have VPCs, the organization and security of resources would be less granular and more challenging to manage. Networks would be less isolated, potentially exposing resources to broader risks and making it harder to control access and traffic flow. Security configurations would likely need to rely more on traditional firewall setups rather than the flexible, policy-driven controls that VPCs provide.

2

A CIDR block is a method for specifying IP addresses and their associated routing prefixes. It allows networks to be divided into smaller, more manageable subnetworks, each identified by a unique CIDR notation that combines an IP address and a prefix length indicating the network's size.

3

The difference between a public and a private subnet lies in their accessibility and routing configuration. A public subnet has a route to an Internet Gateway (IGW) and typically allows instances to have public IP addresses, enabling direct internet access. In contrast, a private subnet does not have a route to an IGW and uses a NAT gateway or NAT instance for outbound internet access, keeping instances within it isolated from direct internet communication.

4

One One thing I didn't expect was how quickly I could set up and configure a VPC with subnets and an internet gateway on AWS. It was faster and more straightforward than I initially anticipated, especially with the automated features like auto-assigning public IPs and the intuitive AWS Management Console interface.