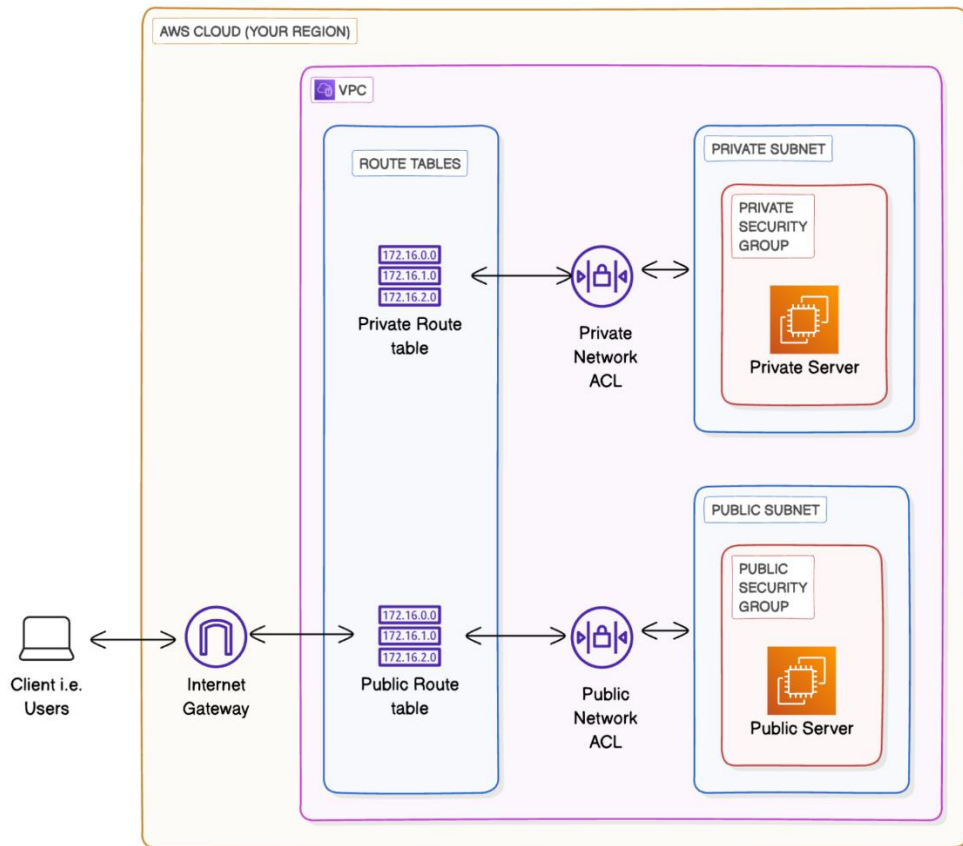


Launching VPC Resources



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create a private network within AWS, offering control over IP ranges, subnets, and security settings. It's useful for securely managing resources and controlling connectivity and network isolation.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a secure, isolated network. I set up public and private subnets, configured route tables for traffic flow, and applied network ACLs to control access, ensuring secure and efficient communication.

One thing I didn't expect in this project was...

One thing I didn't expect in this project was how crucial it is to plan subnet CIDR blocks carefully. Overlapping or misconfigured IP ranges can lead to connectivity issues later, requiring adjustments that can disrupt the network setup.

This project took me...

This project took me an hour to complete. I set up the VPC, created subnets, configured security groups, and set up NAT gateways. I also tested connectivity to ensure proper communication and security before finalizing the network setup.

Setting Up Direct VM Access

Directly accessing a virtual machine means connecting to the instance without intermediaries, typically using protocols like SSH or RDP. This allows you to interact with the EC2 instance's operating system and perform administrative tasks directly.

SSH is a key method for directly accessing a VM

SSH traffic means data transferred over the Secure Shell protocol, which is used to securely access and manage remote systems. It encrypts communication to protect sensitive information, typically used for remote server management or file transfers.

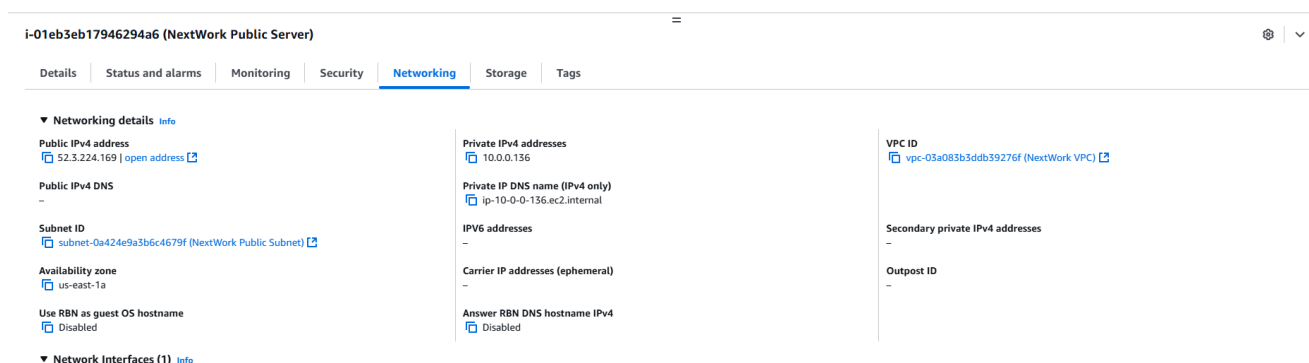
To enable direct access, I set up key pairs

In AWS, key pairs consist of a public key, which is stored on EC2 instances, and a private key, which the user keeps. The private key is used to securely authenticate and establish SSH connections to EC2 instances, ensuring encrypted communication.

A private key's file format means the specific way the key data is structured and stored, typically in formats like PEM or PPK. My private key's file format was PEM, which is a base64 encoded format with a "----BEGIN PRIVATE KEY----" header.

Launching a public server

I updated my EC2 instance's networking settings by modifying security group rules to allow specific traffic like SSH, adjusting network interface settings, and ensuring the proper subnet and route table configurations for seamless connectivity.



The screenshot displays the 'Networking' tab for an EC2 instance named 'i-01eb3eb17946294a6 (NextWork Public Server)'. The 'Networking details' section shows the following information:

- Public IPv4 address:** 52.3.224.169 (with a link to 'open address')
- Public IPv4 DNS:** -
- Subnet ID:** subnet-0a424e9a3b6c4679f (NextWork Public Subnet) (with a link to 'subnet-0a424e9a3b6c4679f')
- Availability zone:** us-east-1a
- Use RBN as guest OS hostname:** Disabled

The 'Network Interfaces (1)' section shows one interface with the following details:

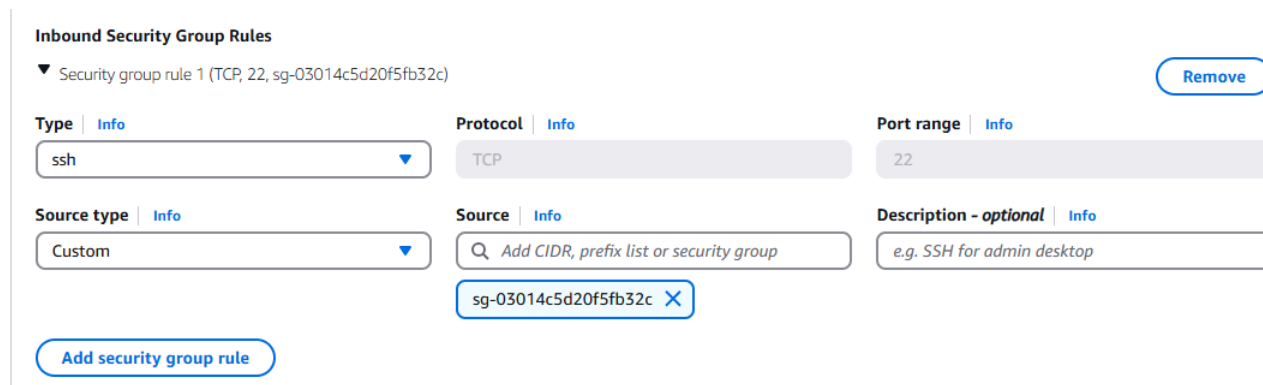
- Private IPv4 addresses:** 10.0.0.136
- Private IP DNS name (IPv4 only):** ip-10-0-0-136.ec2.internal
- IPv6 addresses:** -
- Carrier IP addresses (ephemeral):** -
- Answer RBN DNS hostname IPv4:** Disabled

The 'VPC ID' is vpc-03a083b3ddb39276f (NextWork VPC) (with a link to 'vpc-03a083b3ddb39276f'). The 'Secondary private IPv4 addresses' and 'Outpost ID' are both listed as '-'.

Launching a private server

My private server has its own dedicated security group because it needs to have more restricted access for security purposes. This ensures that only authorized internal resources can communicate with it, minimizing exposure to external threats.

My private server's security group's source is an internal IP range or security group ID, meaning only authorized internal resources can access it. This reduces external exposure and helps maintain tighter security and control for the private server.



The screenshot shows the 'Inbound Security Group Rules' configuration page. A rule named 'Security group rule 1 (TCP, 22, sg-03014c5d20f5fb32c)' is being edited. The configuration is as follows:

- Type:** ssh
- Protocol:** TCP
- Port range:** 22
- Source type:** Custom
- Source:** sg-03014c5d20f5fb32c (with a dropdown arrow)
- Description - optional:** e.g. SSH for admin desktop

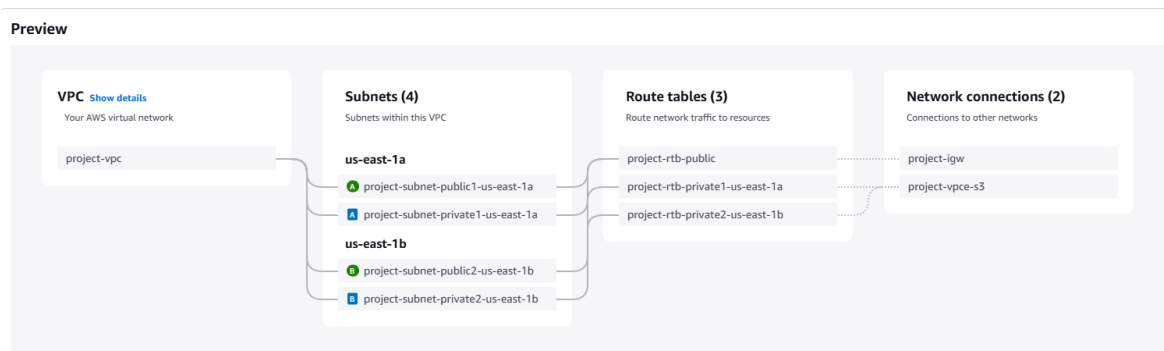
Buttons for 'Remove', 'Add security group rule', and 'Add CIDR, prefix list or security group' are visible.

Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I employed the VPC wizard in the AWS Management Console, selecting predefined configurations for subnets, route tables, and security settings, ensuring a smooth and customized setup.

A VPC resource map is a visual representation of components in a Virtual Private Cloud, like subnets, route tables, security groups, and network interfaces. It helps you understand their relationships, making management and troubleshooting easier.

My new VPC has a CIDR block of 10.0.0.0/16. It is possible for my new VPC to have the same IPv4 CIDR block as my existing VPC because they are in separate, isolated networks, and each VPC can have its own IP range even within the same region.

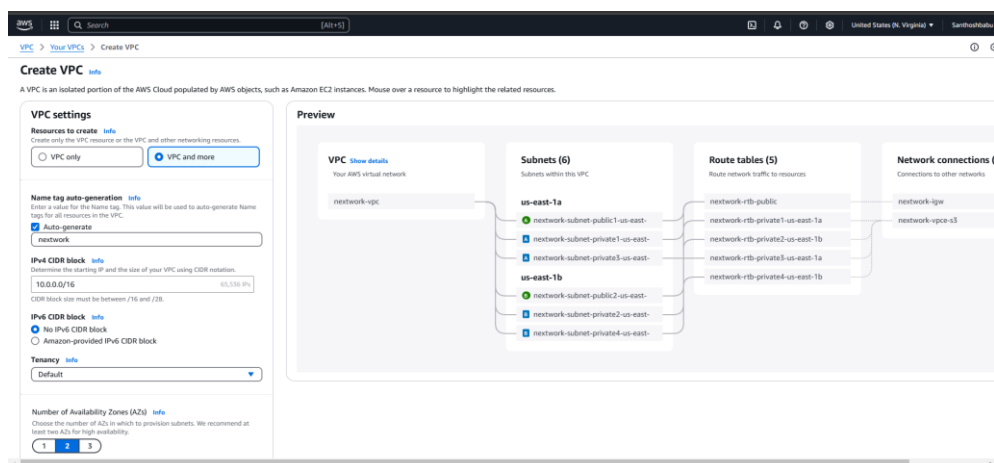


Speeding up VPC creation

Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I had two options: one subnet per Availability Zone or a single subnet. This is because AWS recommends distributing resources across zones for better availability and fault tolerance.

The setup page also offered to create NAT gateways, which are managed services that allow instances in private subnets to access the internet while keeping them secure by blocking inbound traffic, ensuring isolated yet functional resources.



Today you've learnt how to:

- 🖥️ **Launch a public EC2 instance** You launched an EC2 instance in your public subnet, set up the appropriate AMI and instance type, and configured key pairs for secure access.
- 😊 **Launch a private EC2 instance** You launched an EC2 instance in your private subnet, created a security group within the same flow, and used the same key pair for access.
- ⚡ **Launch your VPC setup in minutes:** You explored a new way to create VPCs and used the VPC's resource map to visualize how different components like subnets and route tables are connected.