Day 3 – Networking & Security

Introduction

On Day 3, the focus shifts to understanding the networking and security components within AWS, including Virtual Private Cloud (VPC), Subnets, and Security Groups. These elements form the backbone of secure cloud infrastructure by defining how resources communicate and stay protected from unauthorized access.

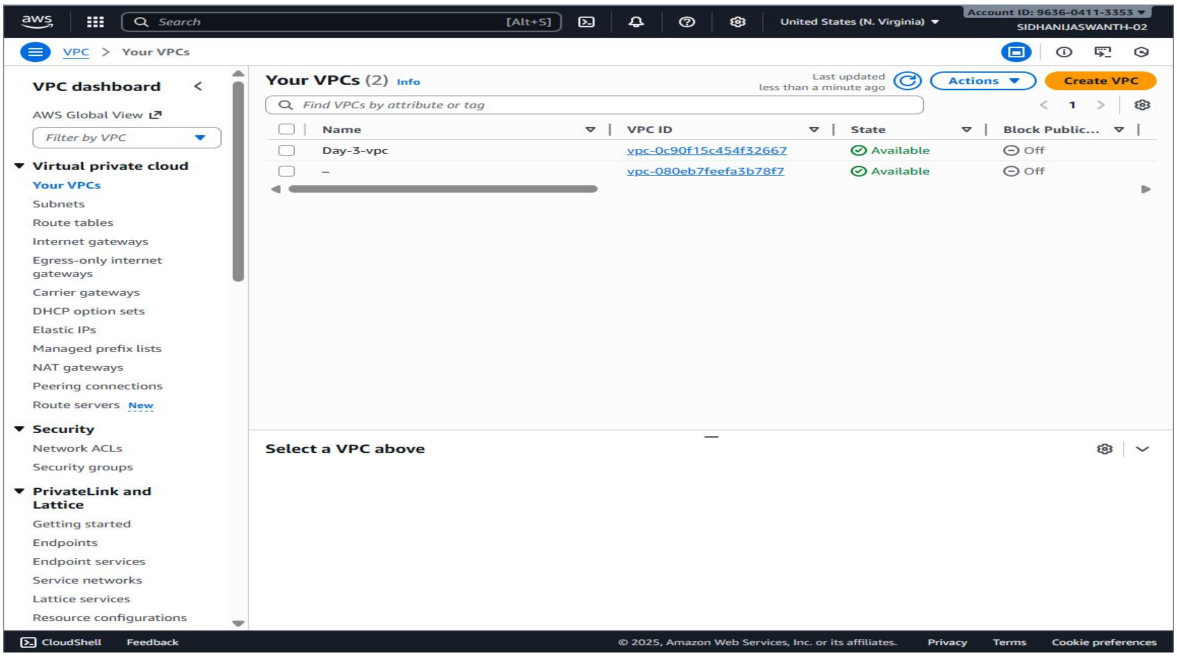
1. Amazon VPC (Virtual Private Cloud)

Amazon VPC allows users to create an isolated section of the AWS cloud where they can define their own IP address ranges, subnets, route tables, and gateways. It provides complete control over the network environment and is fundamental for deploying secure applications.

Hands-On Steps:

- 1. Go to the AWS Management Console and open the VPC dashboard.
- 2. Click on 'Create VPC' and choose 'VPC and more' for guided configuration.
- 3. Provide a name (e.g., MyCustomVPC) and specify an IPv4 CIDR block such as 10.0.0.0/16.
- 4. Keep the default settings for tenancy and DNS options, then create the VPC.
- 5. Verify that your new VPC is listed under 'Your VPCs'.

■ Screenshot



Your VPCs (2) Info

Name	VPC ID	State	Block Public...
Day-3-vpc	vpc-0c90f15c454f32667	Available	Off
–	vpc-080eb7feefa3b78f7	Available	Off

Select a VPC above

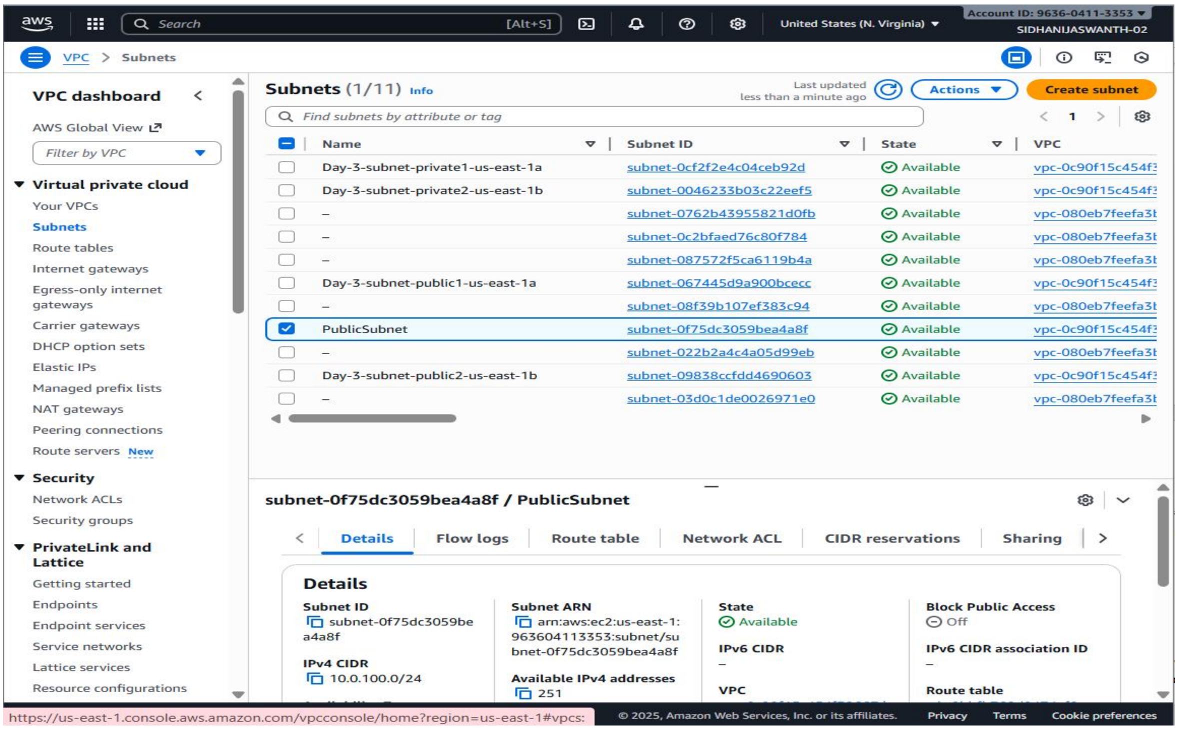
2. Subnets

Subnets divide a VPC's IP address range into smaller sections to organize resources. Public subnets connect to the internet via an Internet Gateway, while private subnets are used for internal resources.

Hands-On Steps:

- 1. In the VPC dashboard, navigate to 'Subnets' and click on 'Create Subnet'.
- 2. Choose your newly created VPC and name the subnet (e.g., PublicSubnet).
- 3. Assign an IPv4 CIDR block, such as 10.0.100.0/24.
- 4. Choose an Availability Zone and create the subnet.
- 5. Attach an Internet Gateway to enable public access.

■ Screenshot



Subnets (1/11)

☐	Name	Subnet ID	State	VPC
☐	Day-3-subnet-private1-us-east-1a	subnet-0cf2f2e4c04ceb92d	✓ Available	vpc-0c90f15c454f3
☐	Day-3-subnet-private2-us-east-1b	subnet-0046233b03c22eef5	✓ Available	vpc-0c90f15c454f3
☐	–	subnet-0762b43955821d0fb	✓ Available	vpc-080eb7feefa3b
☐	–	subnet-0c2bfaed76c80f784	✓ Available	vpc-080eb7feefa3b
☐	–	subnet-087572f5ca6119b4a	✓ Available	vpc-080eb7feefa3b
☐	Day-3-subnet-public1-us-east-1a	subnet-067445d9a900bcecc	✓ Available	vpc-0c90f15c454f3
☐	–	subnet-08f39b107ef383c94	✓ Available	vpc-080eb7feefa3b
☑	PublicSubnet	subnet-0f75dc3059bea4a8f	✓ Available	vpc-0c90f15c454f3
☐	–	subnet-022b2a4c4a05d99eb	✓ Available	vpc-080eb7feefa3b
☐	Day-3-subnet-public2-us-east-1b	subnet-09838ccfdd4690603	✓ Available	vpc-0c90f15c454f3
☐	–	subnet-03d0c1de0026971e0	✓ Available	vpc-080eb7feefa3b

subnet-0f75dc3059bea4a8f / PublicSubnet

Details

Subnet ID: subnet-0f75dc3059bea4a8f

Subnet ARN: arn:aws:ec2:us-east-1:963604113353:subnet/subnet-0f75dc3059bea4a8f

State: ✓ Available

Block Public Access: Off

IPv4 CIDR: 10.0.100.0/24

Available IPv4 addresses: 251

IPv6 CIDR: –

IPv6 CIDR association ID: –

VPC

Route table

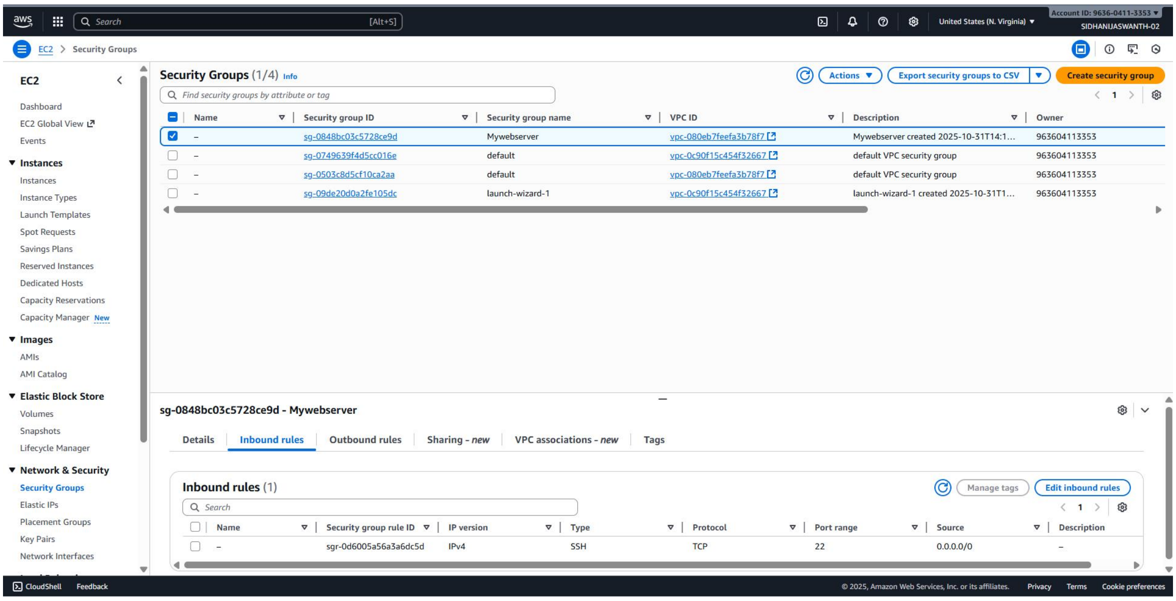
3. Security Groups and Firewall Rule

Security Groups act as virtual firewalls that control inbound and outbound traffic to AWS resources. Each Security Group contains rules that define what type of network traffic is allowed or denied.

Hands-On Steps:

- 1. Navigate to the EC2 dashboard and open 'Security Groups'.
- 2. Click 'Create Security Group' and name it (e.g., WebAccessSG).
- 3. Add inbound rules for HTTP (port 80) and SSH (port 22) access.
- 4. Choose 'Anywhere (0.0.0.0/0)' for testing or restrict it to your IP for security.
- 5. Launch a new EC2 instance within your VPC and assign this Security Group.

■ Screenshot



Security Groups (1/4) Info

	Name	Security group ID	Security group name	VPC ID	Description	Owner
☑	–	sg-0848bc03c5728ce9d	Mywebserver	vpc-080eb7feefa3b78f7	Mywebserver created 2025-10-31T14:1...	963604113353
□	–	sg-0749639f4d5cc016e	default	vpc-0c90f15c454f32667	default VPC security group	963604113353
□	–	sg-0503c8d5cf10ca2aa	default	vpc-080eb7feefa3b78f7	default VPC security group	963604113353
□	–	sg-09de20d0a2fe105dc	launch-wizard-1	vpc-0c90f15c454f32667	launch-wizard-1 created 2025-10-31T1...	963604113353

sg-0848bc03c5728ce9d - Mywebserver

Inbound rules (1)

	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-0d6005a56a3a6dc5d	IPv4	SSH	TCP	22	0.0.0.0/0	–

Short Note on Security Advantages of VPC Setup

A custom VPC setup enhances security by isolating network environments and allowing granular control over traffic. Public and private subnets can be separated to protect internal applications from external exposure. Security Groups and Network ACLs together ensure multiple layers of protection, reducing the risk of unauthorized access.

Reflection

Day 3 deepened my understanding of cloud networking and security. Learning how to design a custom VPC gave me a clear idea of how AWS ensures secure, isolated environments. Setting up subnets and security groups helped me appreciate how cloud systems balance accessibility and protection. Initially, configuring IP ranges and security rules was tricky, but after experimenting, it became intuitive. This hands-on experience taught me the importance of designing networks with both flexibility and security in mind.