

## Week 5: Network Security in the Cloud

**Name-** Saish Dhiwar

**PRN-** 2124UCSM2011

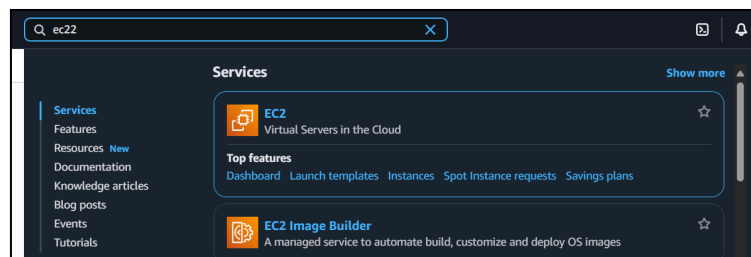
**Email-** [saish.dhiwar\\_24ucs@sanjivani.edu.in](mailto:saish.dhiwar_24ucs@sanjivani.edu.in)

**Task-** 1) Configure security groups and firewall rules.

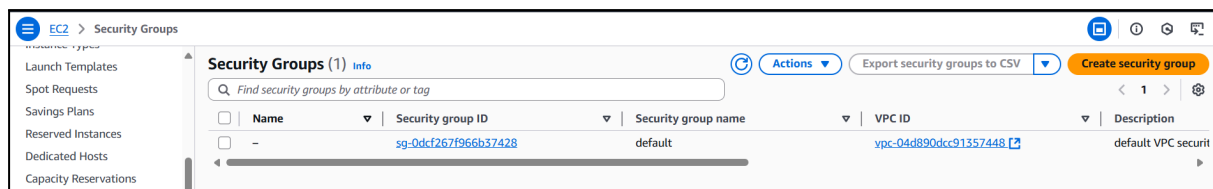
- 2) Block unnecessary ports.
- 3) Document security ruleset.

### Task 1- Configure security groups and firewall Rules.

- 1) Log in to AWS Console. Go to <https://aws.amazon.com>, sign in to the AWS Management Console.
- 2) Open the EC2 Dashboard in the AWS Console, search for EC2 in the services.



- 3) Click on Security Groups in the left sidebar under “Network & Security”



- 4) Create a Security Group, fill in the details of the Security Group.

A screenshot of the AWS Management Console 'Create security group' form. The breadcrumb trail at the top shows 'EC2 > Security Groups > Create security group'. The form title is 'Create security group' with an 'Info' link. Below the title is a descriptive paragraph: 'A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.' The form is divided into three sections: 'Basic details', 'Description', and 'VPC Info'. The 'Basic details' section has a 'Security group name' field with the value 'security\_group' and a note 'Name cannot be edited after creation.' The 'Description' section has a 'Description' field with the value 'first security group'. The 'VPC Info' section has a 'VPC' dropdown menu with the value 'vpc-04d890dcc91357448' selected.

5) Then enter Inbound and Outbound Rules and click the Create Group button.

The screenshot shows the AWS IAM console interface for configuring a security group. It is divided into two main sections: 'Inbound rules' and 'Outbound rules'.

**Inbound rules:** This section has a header 'Inbound rules' with an 'Info' link. Below it are five input fields: 'Type' (set to 'SSH'), 'Protocol' (set to 'TCP'), 'Port range' (set to '22'), 'Source' (set to 'My IP'), and 'Description - optional'. A search bar is present next to the 'Source' field, and a button 'Add rule' is at the bottom left. A 'Delete' button is at the bottom right.

**Outbound rules:** This section has a header 'Outbound rules' with an 'Info' link. Below it are five input fields: 'Type' (set to 'All traffic'), 'Protocol' (set to 'All'), 'Port range' (set to 'All'), 'Destination' (set to 'Custom'), and 'Description - optional'. A search bar is present next to the 'Destination' field, and a button 'Add rule' is at the bottom left. A 'Delete' button is at the bottom right.

6) Security Group created successfully.



7) Block Unnecessary Ports, Edit Inbound and Outbound Rules.

The screenshot shows the AWS IAM console interface for the security group 'sg-0a2677257fd4d8378 - security\_group'. It has an 'Actions' dropdown menu in the top right corner.

**Details:** This section contains a table with the following information:

Security group name	Security group ID	Description	VPC ID
security_group	sg-0a2677257fd4d8378	first security group	vpc-04d890dcc91357448
Owner	Inbound rules count	Outbound rules count	
240110921708	1 Permission entry	1 Permission entry	

**Inbound rules:** This section has a header 'Inbound rules (1)' with a search bar, a 'Manage tags' button, and an 'Edit inbound rules' button. Below the header is a table with the following information:

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-051492b2c91627d5e	IPv4	SSH	TCP	22

## Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

### Inbound rules Info

Inbound rule 1 Delete

Security group rule ID

sgr-051492b2c91627d5e

Type Info

SSH

Protocol Info

TCP

Port range Info

22

Source type Info

Custom

Source Info

103.112.8.222/32

Description - optional Info

Add rule

Cancel
Preview changes
Save rules

8) Unnecessary ports are now blocked, and your instance is more secure.

9)

Direction	Port	Protocol	Source/Destination	Description
Inbound	20	TCP	My IP	SSH for Admin
Inbound	80	TCP	Anywhere	HTTP for Web
Outbound	All	All	0.0.0.0/0	Default Method