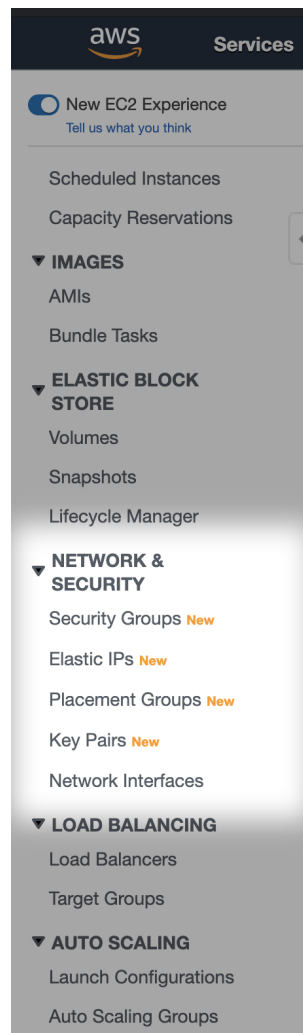


Solution: Security Group Exercise

If you have not done so already, launch an EC2 instance from the EC2 console.

Part 1: Create a Security Group

From the EC2 console, scan the sidebar to find the **Network & Security** section. Within that section click on **Security Groups**.



Click on the **Create security group** button

Fill the information for your security group name and description.

EC2 > Security Groups > Create security group

Create security group [Info](#)

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.

Basic details

Security group name [Info](#)
MySecurityGroup
Name cannot be edited after creation.

Description [Info](#)
Allow SSH and HTTP access

VPC [Info](#)
vpc-036ef207f1f23c608

Click on the **Add Rule** button under the inbound section and add the following rules:

SSH TCP 22 Anywhere

HTTP TCP 80 Anywhere

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info
SSH	TCP	22	Anywhere
HTTP	TCP	80	Anywhere

[Add rule](#)

Click on the **Create security group** button to create the security group.

Part 2: Attach The Security Group To An EC2 Instance

Navigate via the sidebar to EC2 Instances Dashboard. Select the instance to which you want to add the security group.

From the **Actions** dropdown menu select **Networking**, followed by **Change Security Groups**.

Actions ^

- Connect
- Get Windows Password
- Create Template From Instance
- Launch More Like This
- Instance State ▶
- Instance Settings ▶
- Image ▶
- Networking** ▶
- CloudWatch Monitoring ▶

Change Security Groups

- Attach Network Interface
- Detach Network Interface
- Disassociate Elastic IP Address
- Change Source/Dest. Check
- Manage IP Addresses

	Availability Zone	Instance S
	us-east-1b	termina
	us-east-1a	termina
	us-east-1b	running

3c7dfbf47f63bae	t3.medium
b2fb67a88ecb050	t3.medium
b66d41958bf692c	t3.medium

Select the security group you just created in Step 1 and click the **Assign security groups** button.

In the **Description** tab at the bottom of the screen, we can now see the security group.

Private IPs 172.31.39.198

Secondary private IPs

VPC ID [vpc-036ef207f1f23c608](#)

Subnet ID [subnet-0281cefdaa6d0b3b7](#)

Network interfaces [eth0](#)

IAM role -

Key pair name ami

Security groups [MySecurityGroup](#) [view inbound rules](#) [view outbound rules](#)

Security Groups associated with i-01c8c94257b83b5cc

Ports	Protocol	Source	MySecurityGroup
80	tcp	0.0.0.0/0, ::/0	✓
22	tcp	0.0.0.0/0, ::/0	✓

T2/T3 Unlimited Disabled

[_64-gp2 \(ami-](#)