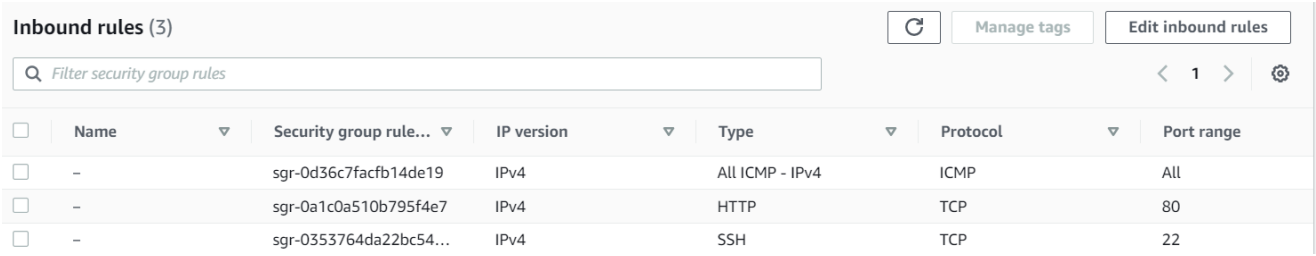
Install Apache Server on EC2 instance

1-Create Security Group



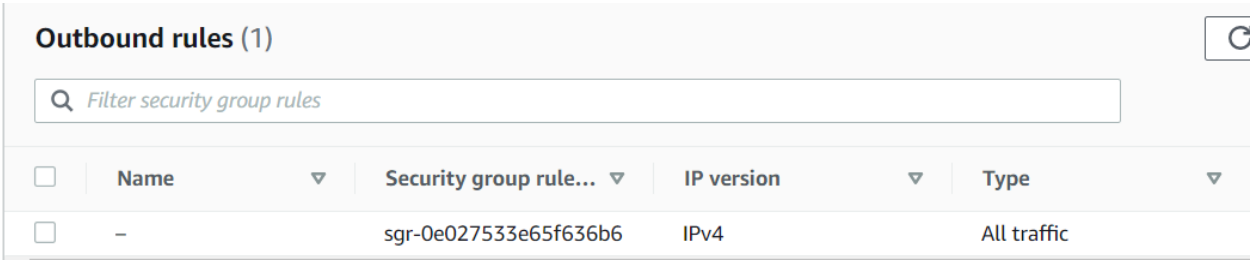
Inbound rules (3)

Manage tags | Edit inbound rules

Filter security group rules

1

Name	Security group rule...	IP version	Type	Protocol	Port range
–	sgr-0d36c7facfb14de19	IPv4	All ICMP - IPv4	ICMP	All
–	sgr-0a1c0a510b795f4e7	IPv4	HTTP	TCP	80
–	sgr-0353764da22bc54...	IPv4	SSH	TCP	22



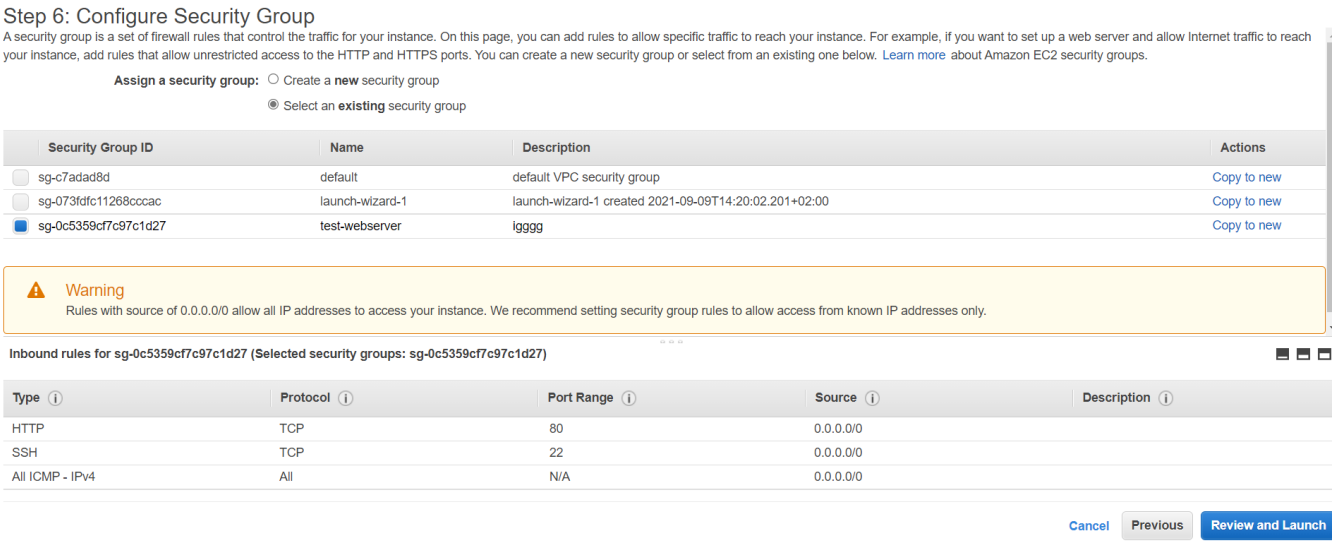
Outbound rules (1)

Filter security group rules

Name	Security group rule...	IP version	Type
–	sgr-0e027533e65f636b6	IPv4	All traffic

2-Create and Launch Instance

-Create instance by default settings then select already created security group then install instance pair keys to access server



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group

◉ Select an **existing** security group

Security Group ID	Name	Description	Actions
sg-c7adad8d	default	default VPC security group	Copy to new
sg-073fdfc11268cccac	launch-wizard-1	launch-wizard-1 created 2021-09-09T14:20:02.201+02:00	Copy to new
sg-0c5359cf7c97c1d27	test-webserver	igggg	Copy to new

Warning

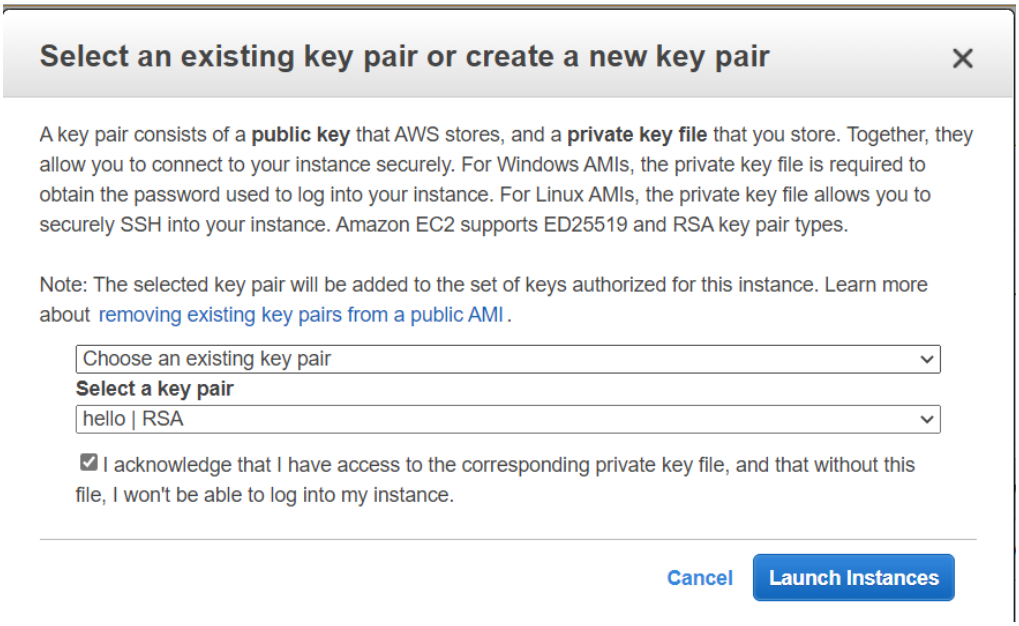
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Inbound rules for sg-0c5359cf7c97c1d27 (Selected security groups: sg-0c5359cf7c97c1d27)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
All ICMP - IPv4	All	N/A	0.0.0.0/0	

Cancel | Previous | Review and Launch

-I already created key pairs so I will use them in this instance



3-Acess Instance and install and Launch Apache Server on it

-Access Instance through pair key using ssh command

```
C:\Programming\Embedded course>ssh -i hello.pem ec2-user@3.21.166.126
The authenticity of host '3.21.166.126 (3.21.166.126)' can't be established.
ECDSA key fingerprint is SHA256:vhSFAG+/aGUWdh8B1UJ/BQnhv5eh/E1Oo8NQvefB+lc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.21.166.126' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-38-36 ~]$ sudo su
```

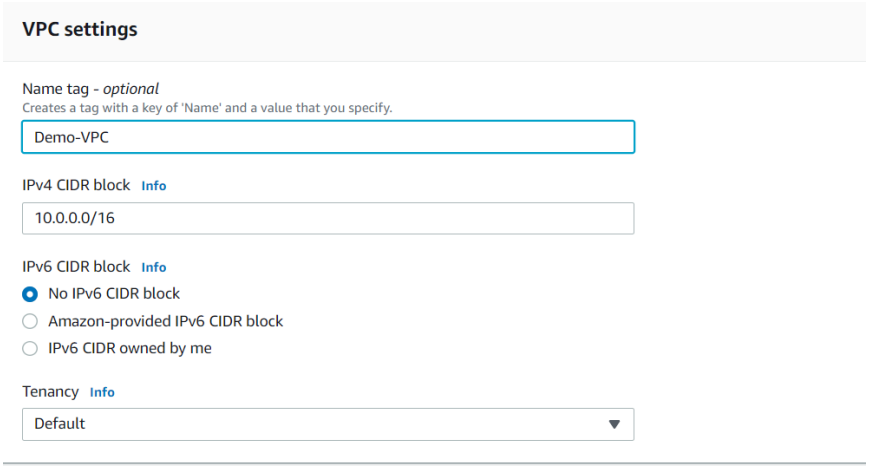
-then give root access then by applying the following commands:

```
yum update -y

yum install -y httpd

systemctl start httpd

systemctl enable httpd

echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html
```

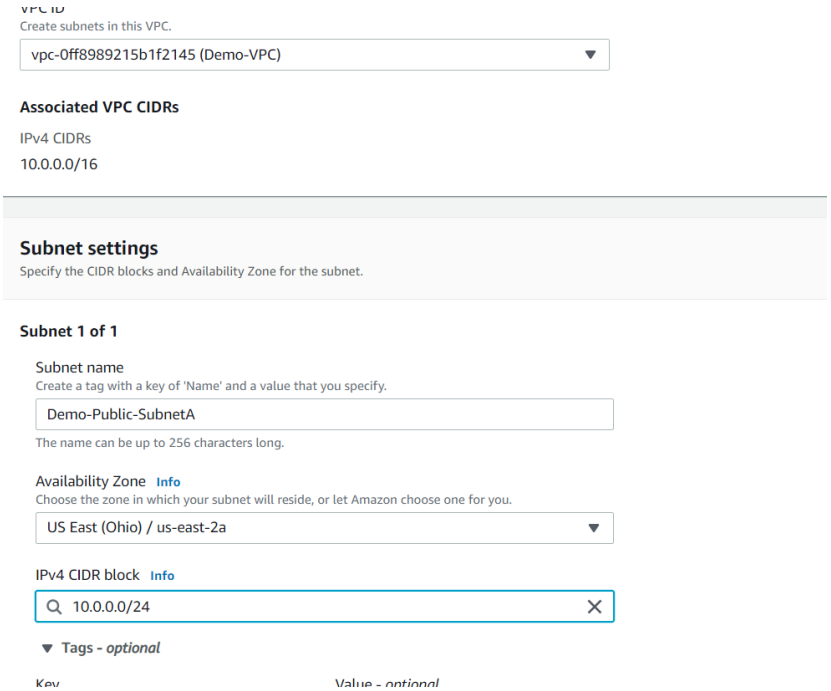
The Result

Create and Configure VPC

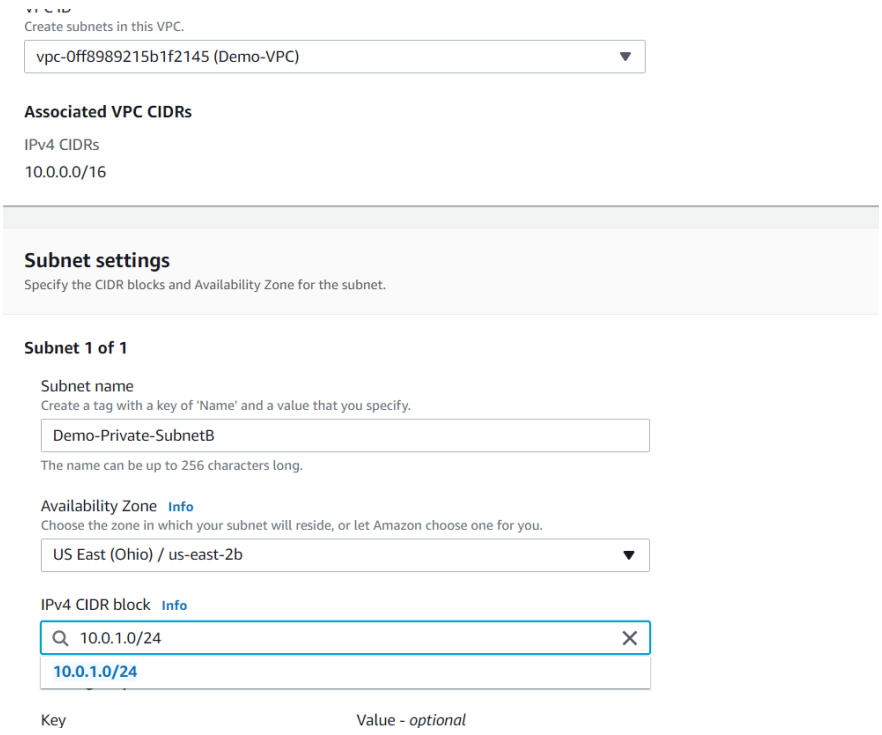
1-Create VPC



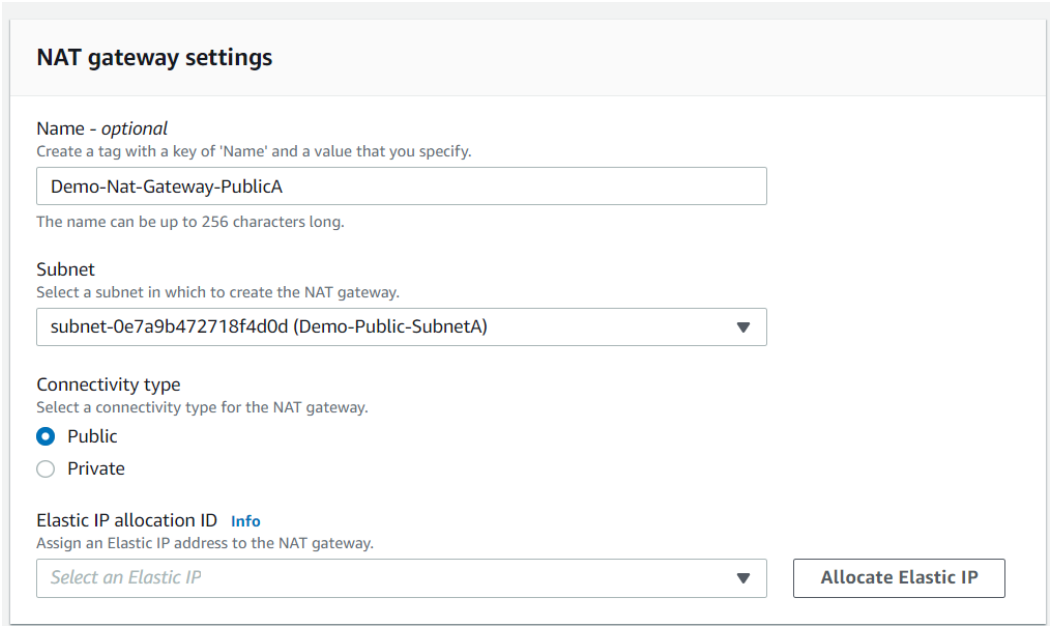
2-Create Public Subnet



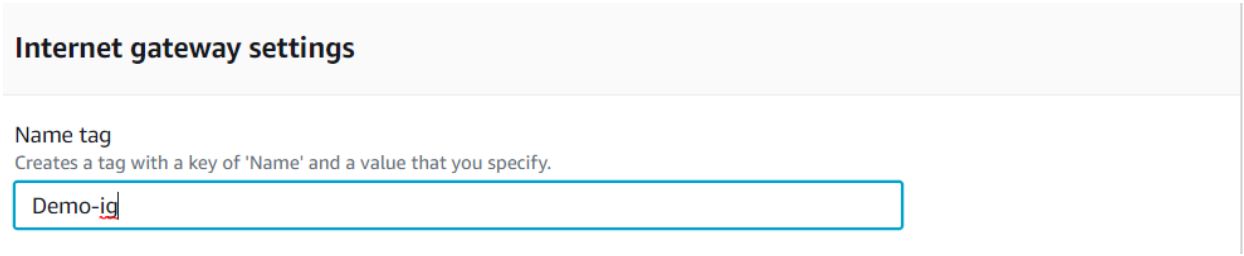
3-Create Private Subnet



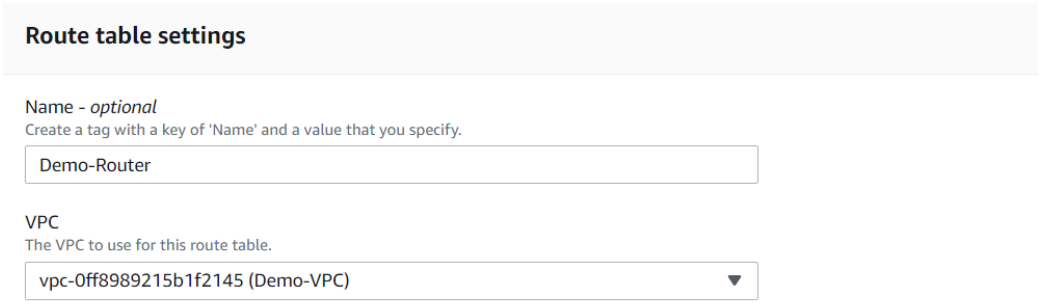
4-Create NAT

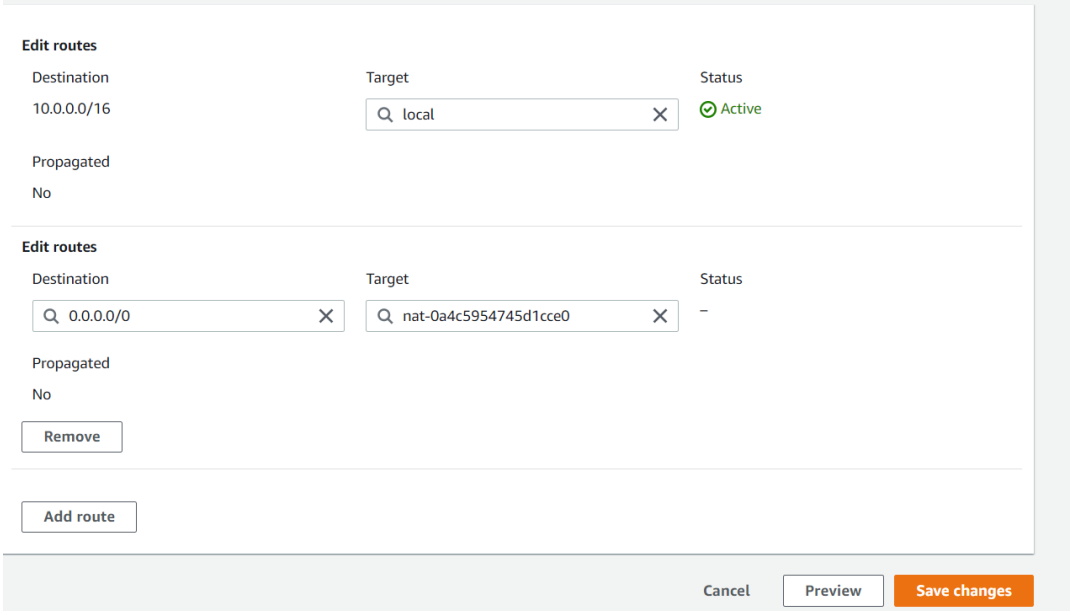


5-Create Internet Gateway

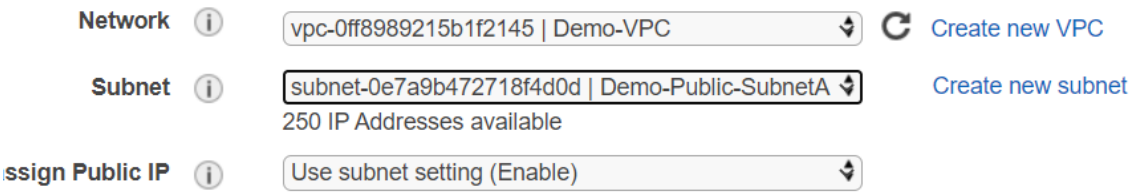


6-Create Router





6-Create EC2 on Public Subnet



7-Create EC2 on Private Subnet