22°

Lab - AWS re/Start

Creación de una VPC y lanzamiento de un servidor web

SWIPE

Tarea 01

Resolviendo el Ticket del cliente

En este laboratorio, deberá utilizar Amazon Virtual Private Cloud (VPC) para **crear su propia VPC** y agregar componentes adicionales con el fin de producir una red personalizada para una gran empresa. Además, creará **grupos de seguridad** para la instancia de EC2. Deberá configurar y personalizar **una instancia de EC2 para ejecutar un servidor web** y lanzarla en la VPC que se parece al siguiente diagrama del cliente:

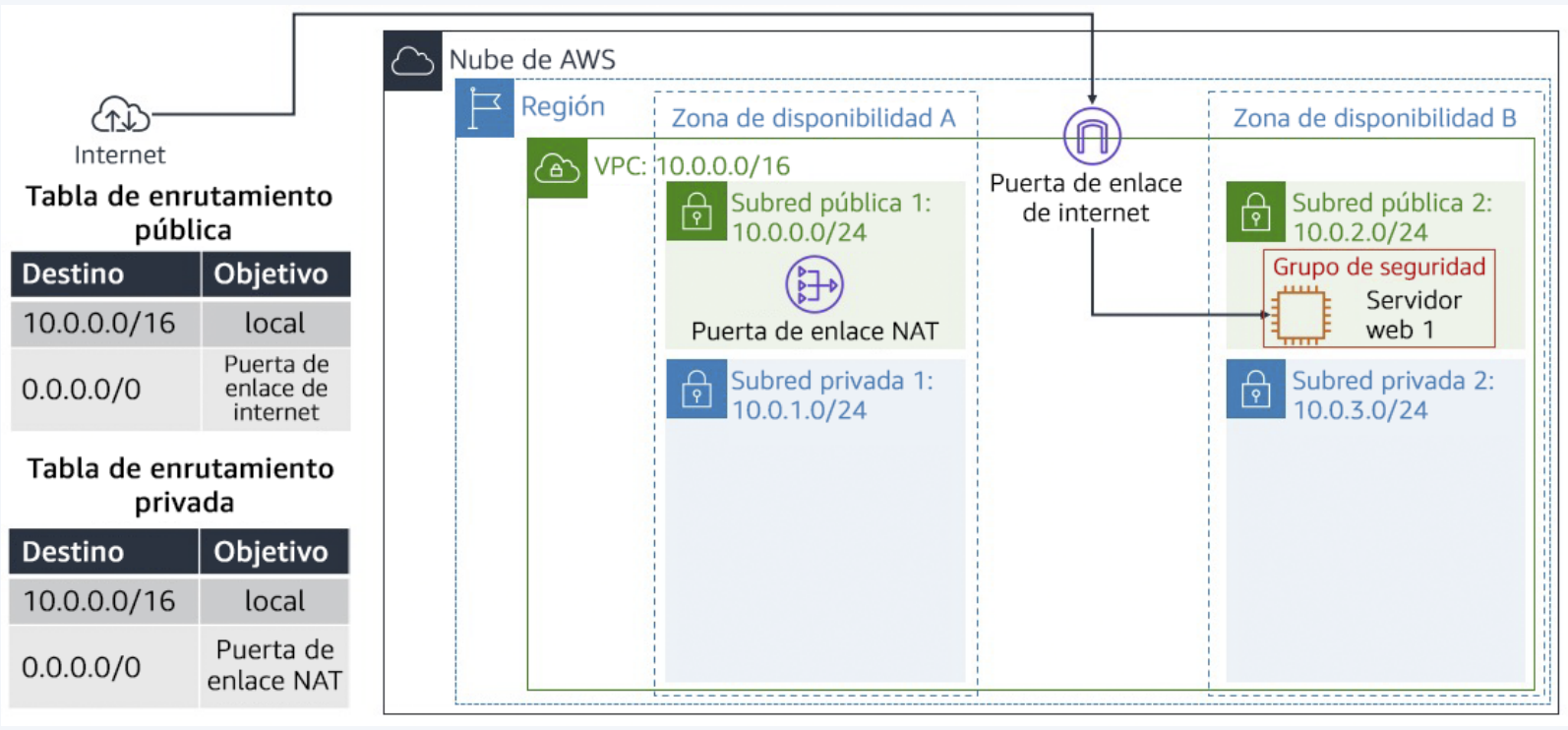


Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	Puerta de enlace de internet

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	Puerta de enlace NAT

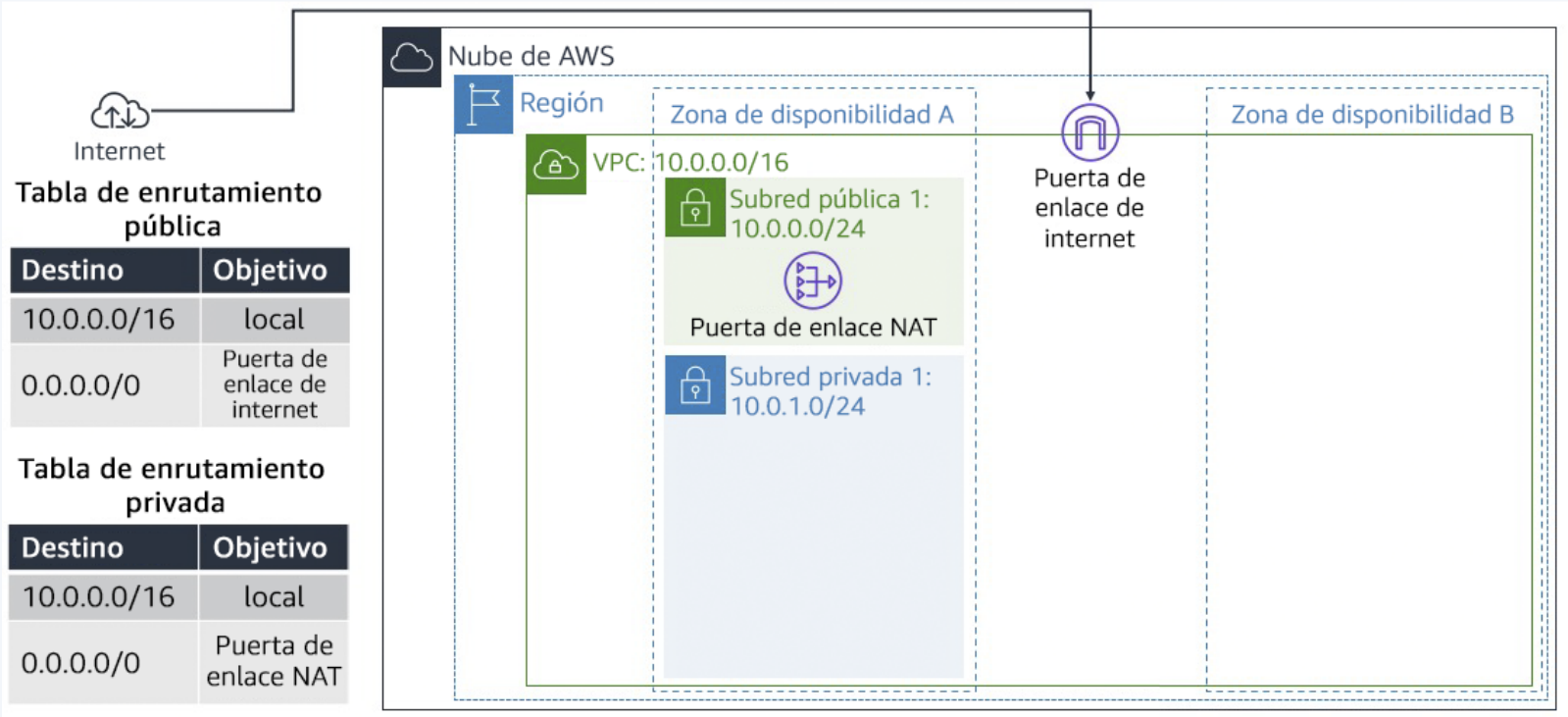
SWIPE

Tarea 01

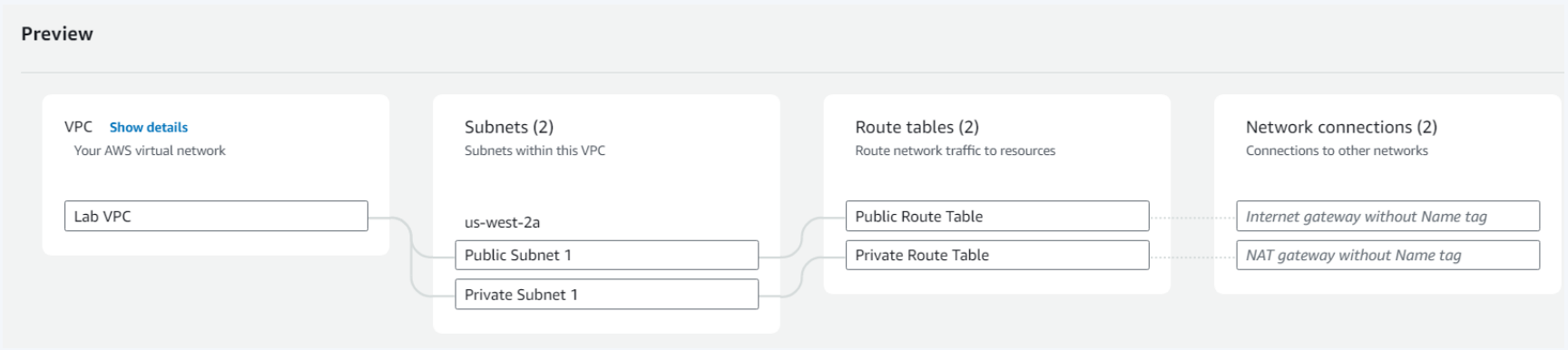
Empezamos por la creación de la VPC, y la subred pública y privada de una AZ. Me refiero al siguiente diagrama, pues adicionalmnte asignaremos las tablas de enrutamiento a cada subred.

OJO:

- Cada subred necesita de una tabla de enrutamiento. Y esta tabla de enrutamiento puede ser común entre subredes.



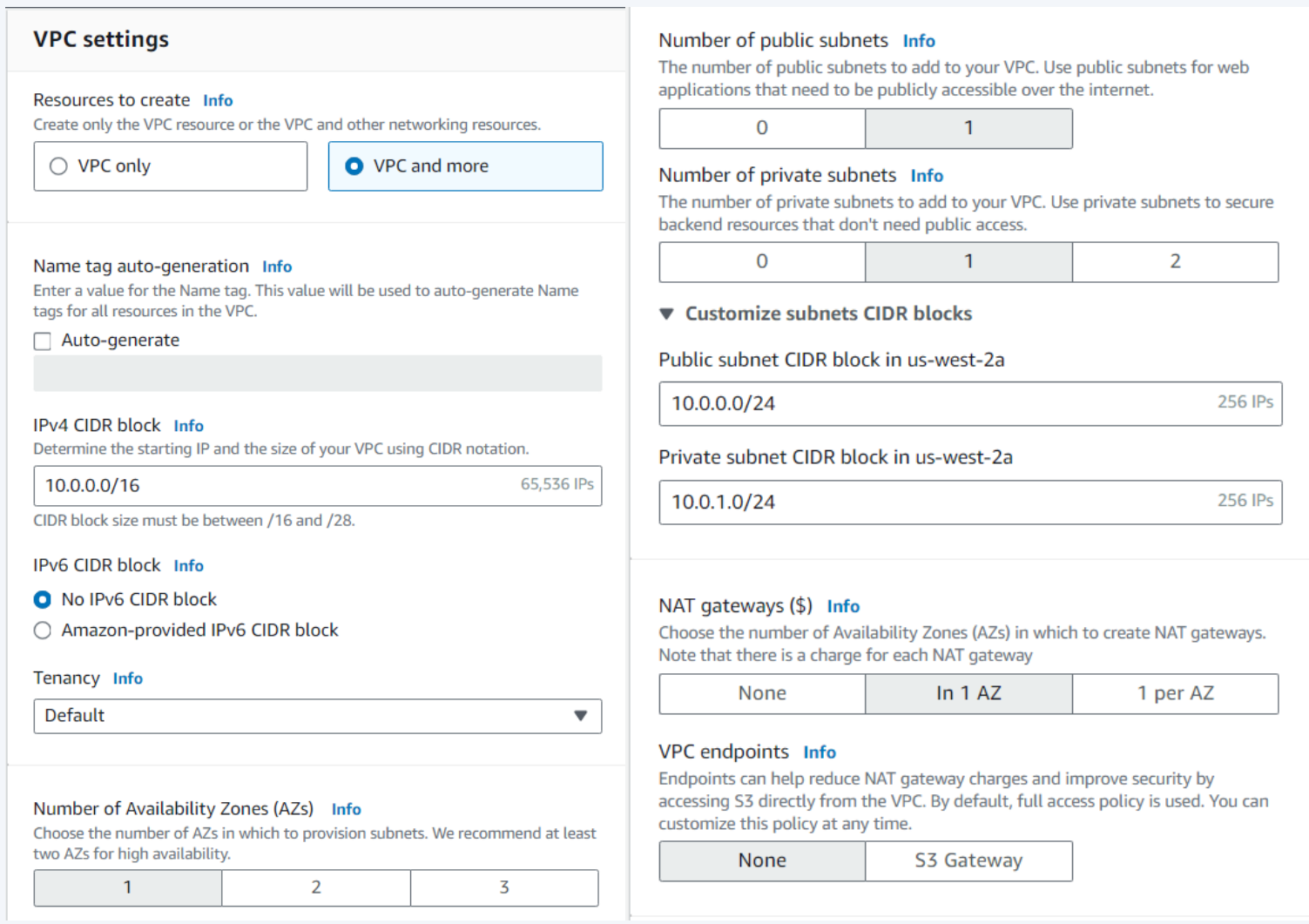
Así la vista previa es:



SWIPE

Tarea 01

Y la configuración de la VPC fue la siguiente, donde también señalamos que **se creará una puerta de enlace NAT en una zona de disponibilidad**. Recuerda que las subredes se crean a nivel de AZs:

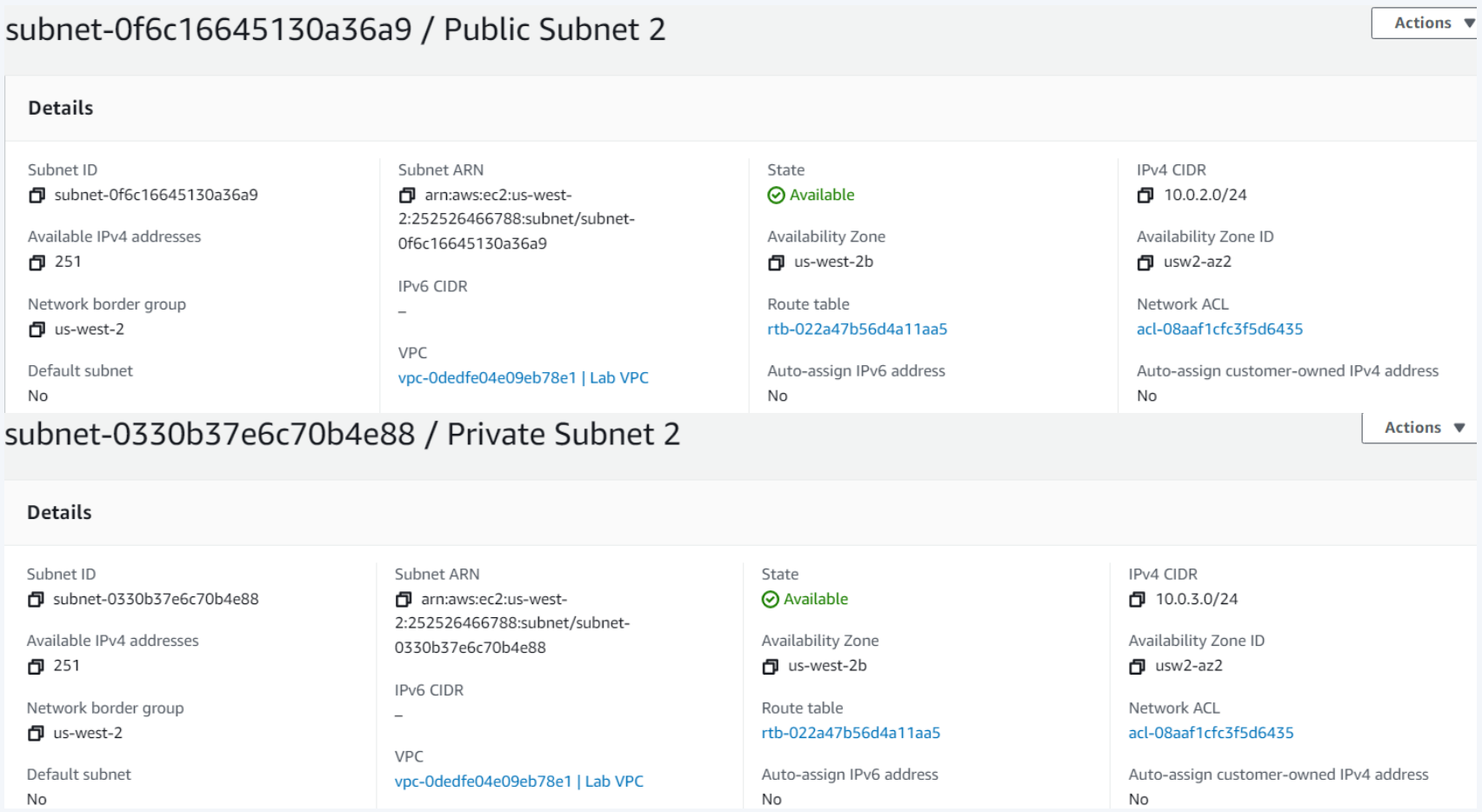


Luego procedemos a crear las subredes restantes del diagrama, estas se encuentran **en otra zona de disponibiladad** (en este caso **usw2-az2**).

SWIPE

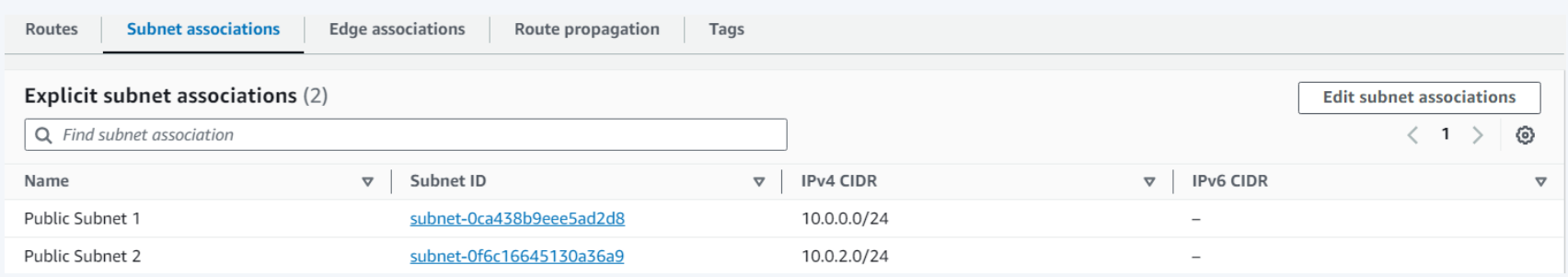
Tarea 01

Así, logramos crear ambas subredes dentro de la otra AZ, estas son sus configuraciones:



Ahora, lo que debemos hacer es asignar una tabla de enrutamiento a cada una de estas subredes.

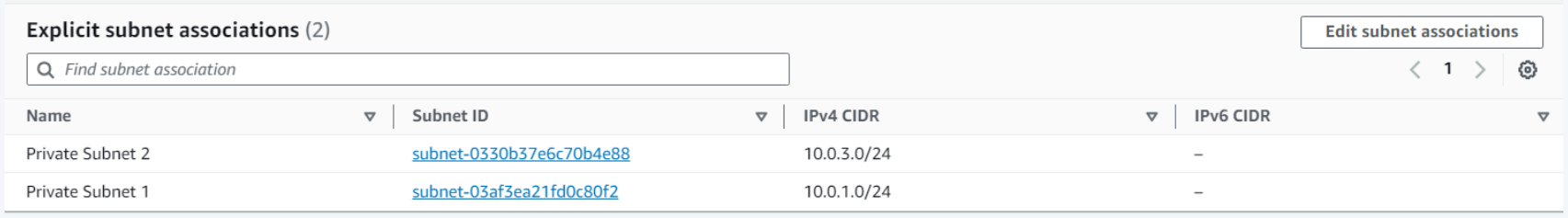
Así, la *Public route table* está asociada a las subredes públicas



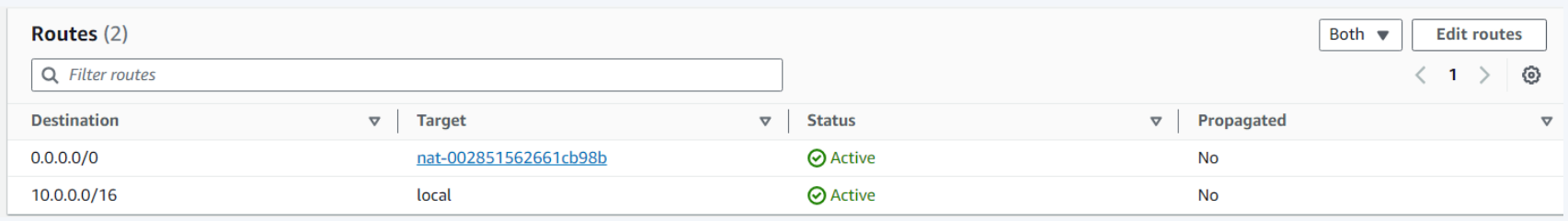
SWIPE

Tarea 01

Y la tabla de enrutamiento privada (*Private route table)* estará asociada a las subredes privadas.



OJO: Notar que el tráfico que quiere **acceder a internet desde algún servicio de la subred privada** tiene como ***target*** **a la puerta de enlace NAT**. La cual es el medio para que los servicios en una subred privada puedan conectarse a internet tras pasar también por la puerta de enlace de internet (IGW)

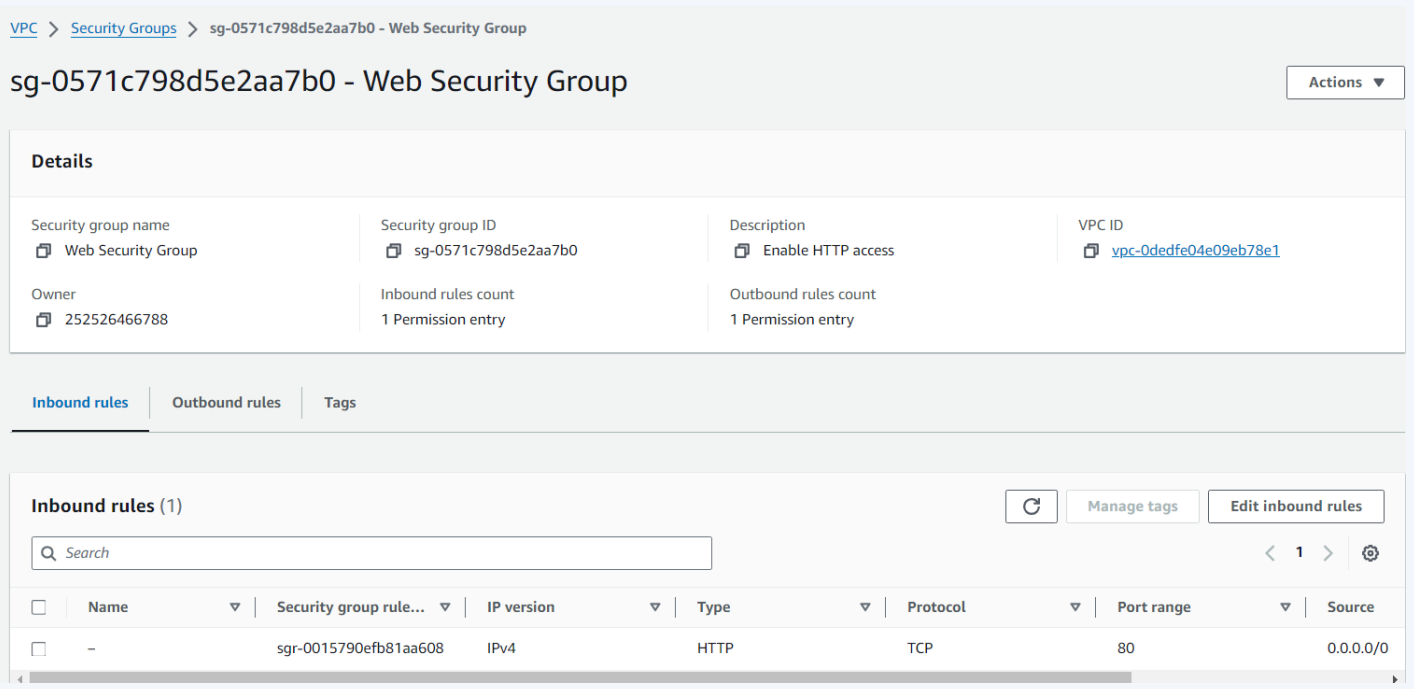


Ahora, procedemos a crear el grupo de seguridad para la instancia de EC2, donde se desplegará el servidor web.

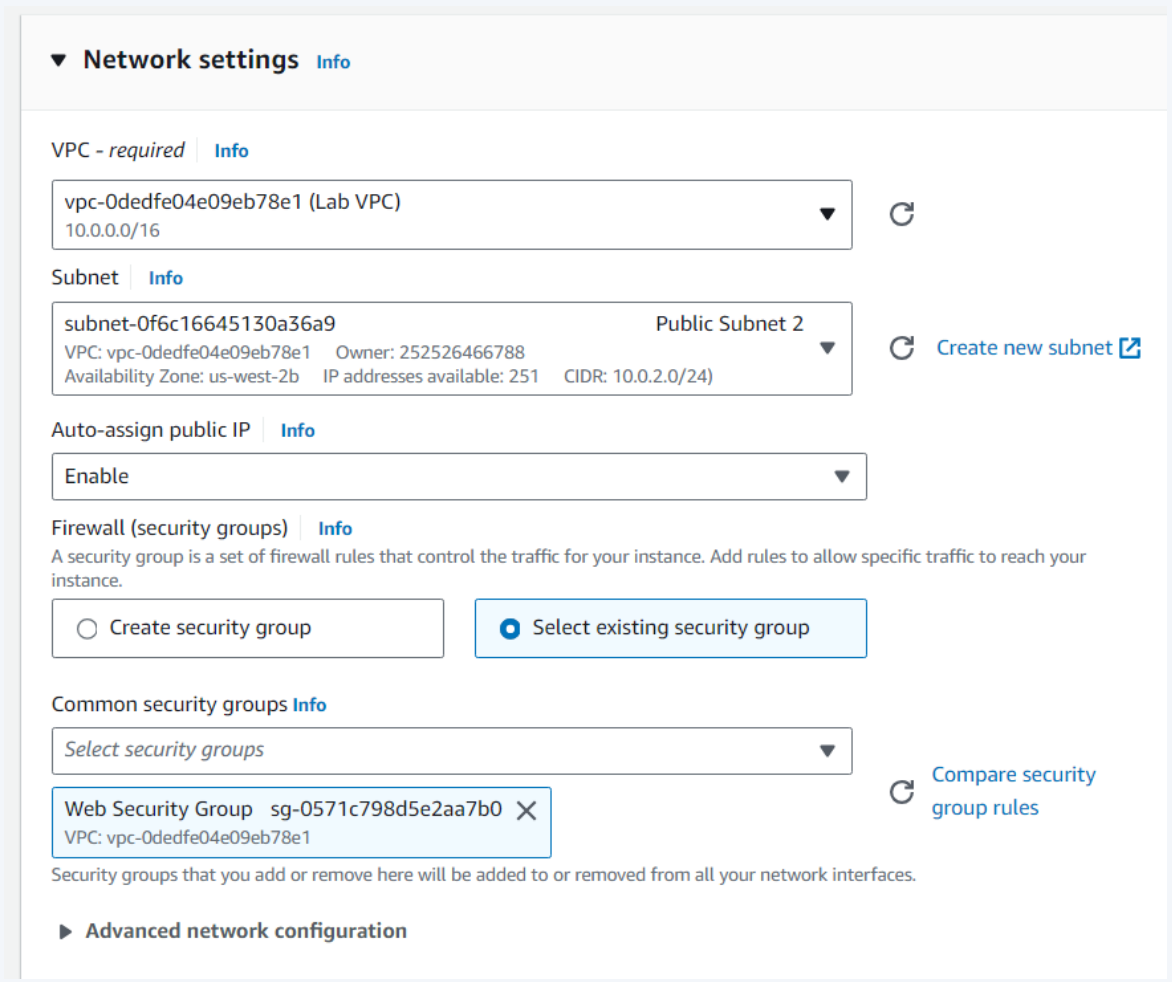
SWIPE

Tarea 01

En este caso permite el acceso a la instancia desde cualquier origen (0.0.0.0/0) via el protocolo HTTP.



Finalmente, creamos la instancia de EC2. Acá podemos ver su configuración de gestión de redes (*networking)*



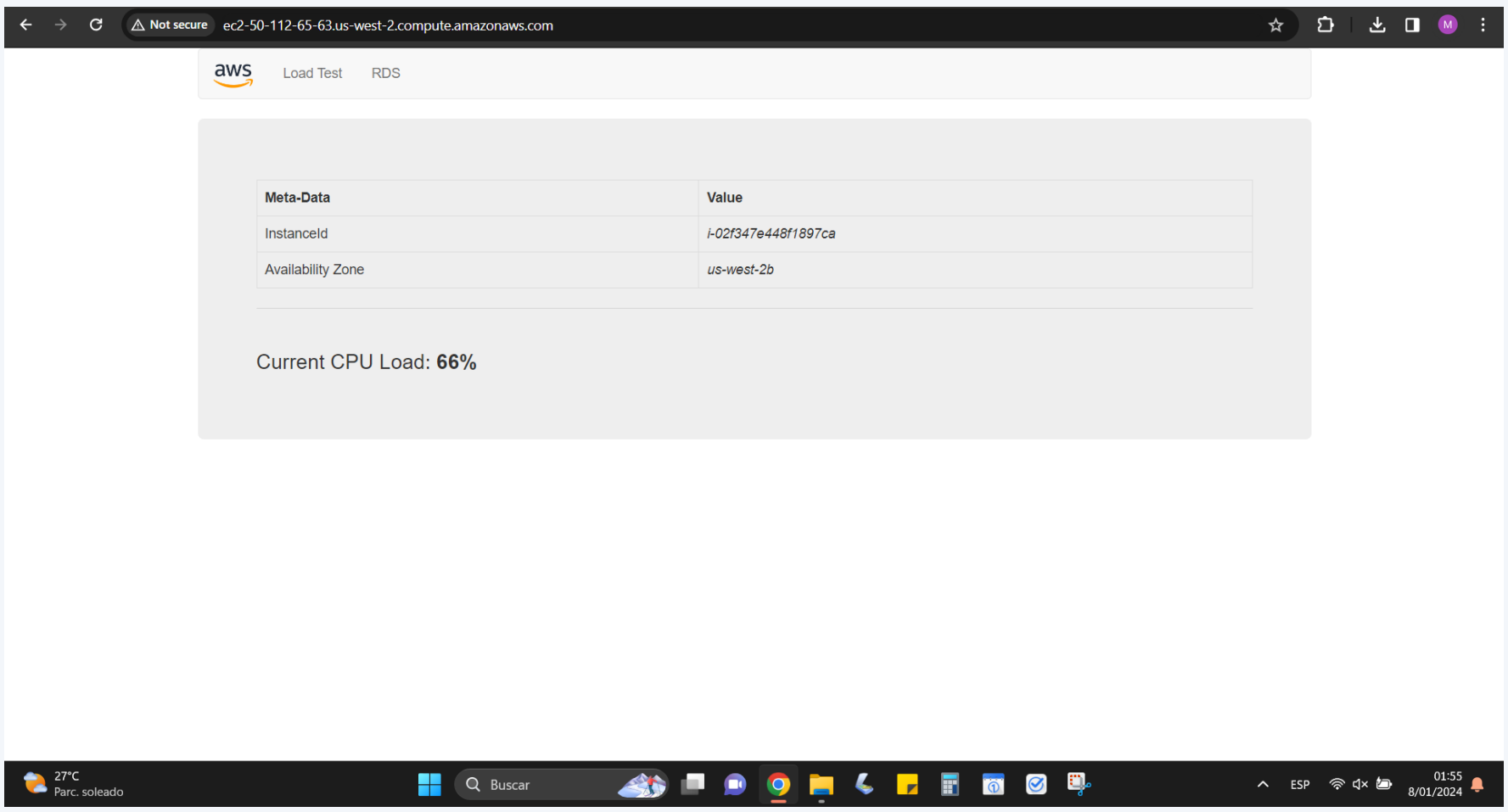
SWIPE

Tarea 01

Y también tenemos los *Datos de Usuario* utilizados para que la máquina virtual sea el servidor web

```
#!/bin/bash
#Install Apache Web Server and PHP
dnf install -y httpd mariadb105-server php
#Download Lab files
wget https://us-east-1-tcprod.s3.amazonaws.com/courses/CUR-TF-100-RSNETK/v3.0.0.prod-ea58589a/267-lab-NF-build-vpc-web-server/scripts/lab-app.zip
unzip lab-app.zip -d /var/www/html/
#Turn on web server
systemctl enable httpd
systemctl start httpd
```

A continuación se muestra la página web, lo que indica que el servidor tiene las correctas configuraciones de red. Cabe recalcar que pudimos verificarlos gracias a la **dirección pública IPv4 DNS**



SWIPE