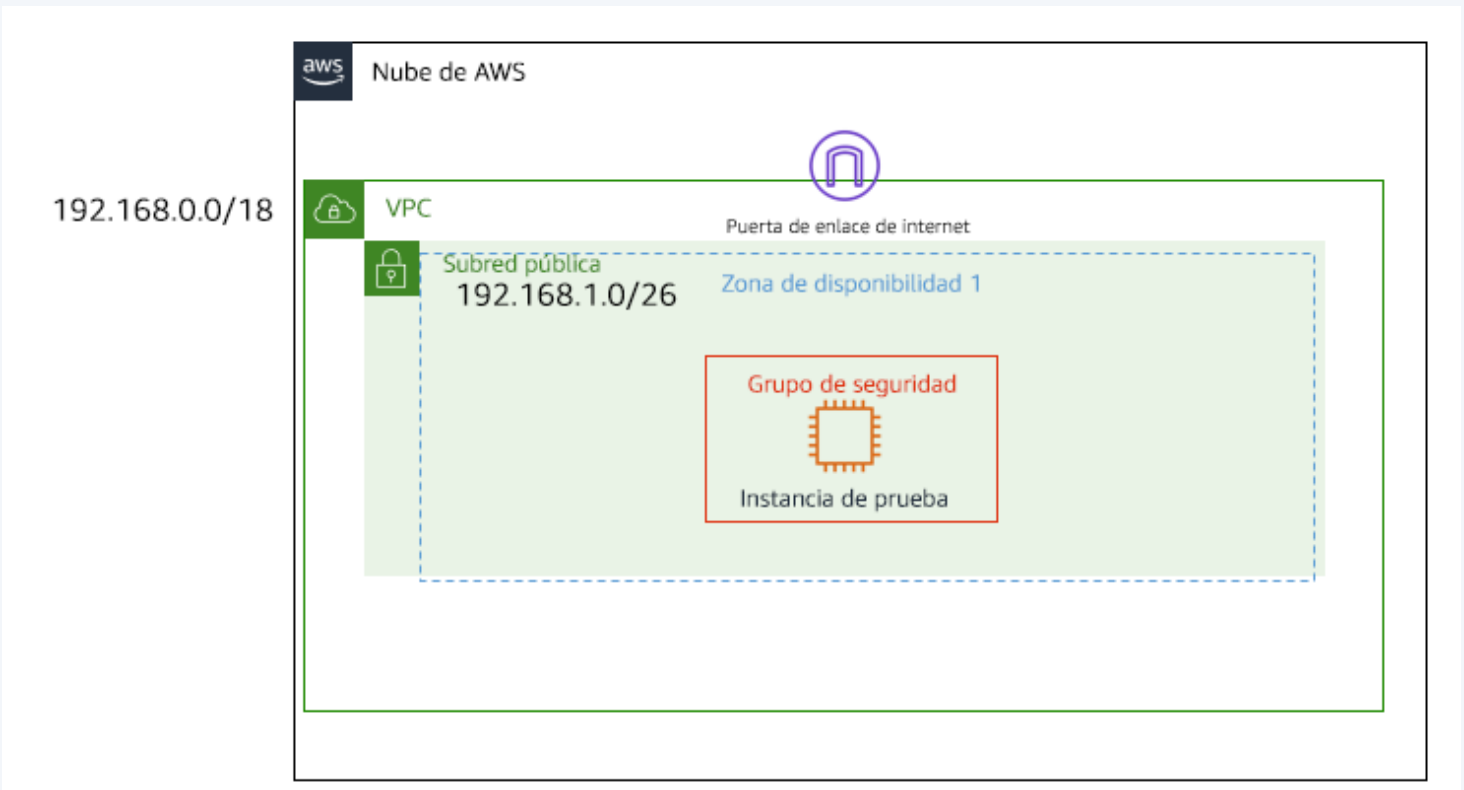
19°

Lab - AWS re/Start

Creación de recursos de redes dentro de una VPC



SWIPE

Tarea 01

Resolviendo el Ticket de Brock

¡Hola, equipo de soporte en la nube!
Hace unos días, me puse en contacto con ustedes para solicitar ayuda a fin de **configurar mi VPC**. Pensé que sabía adjuntar todos los recursos para establecer una **conexión a Internet**, pero ni siquiera puedo hacer ping por fuera de la VPC. ¡Todo lo que necesito es hacer ping! ¿Me pueden ayudar a configurar mi VPC donde tenga conectividad de red y pueda hacer ping? A continuación, se encuentra la arquitectura.
¡Gracias!
Brock, propietario de la empresa emergente

Nota, es conveniente recordar que para que los servicios dentro de una **subred pública tengan conexión a internet** es necesario una **puerta de enlace de internet (IGW)**. Y si quiero que un servicio dentro de una *subred privada* tenga conexión a internet, debemos usar *una puerta de enlace NAT* (el cual estará dentro de la subred pública).

Tarea 01

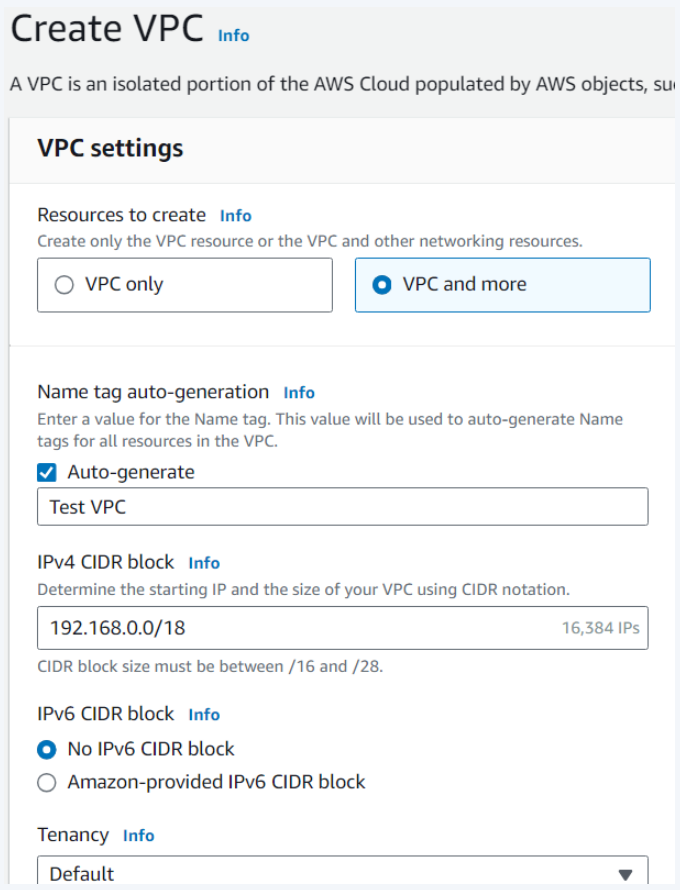
OJO:

- Los **grupos de seguridad** funcionan al **nivel de la instancia y tienen estado (stateful)**, lo que significa que **bloquean todo de forma predeterminada**.

- Las **NACL** funcionan al **nivel de la subred** y **no tienen estado**, lo que significa que **no bloquean nada de forma predeterminada**.

- una **tabla de enrutamiento** contiene las reglas o **rutas** que determinan **a dónde se dirigirá el tráfico** de red que se encuentra **en la subred y la VPC**

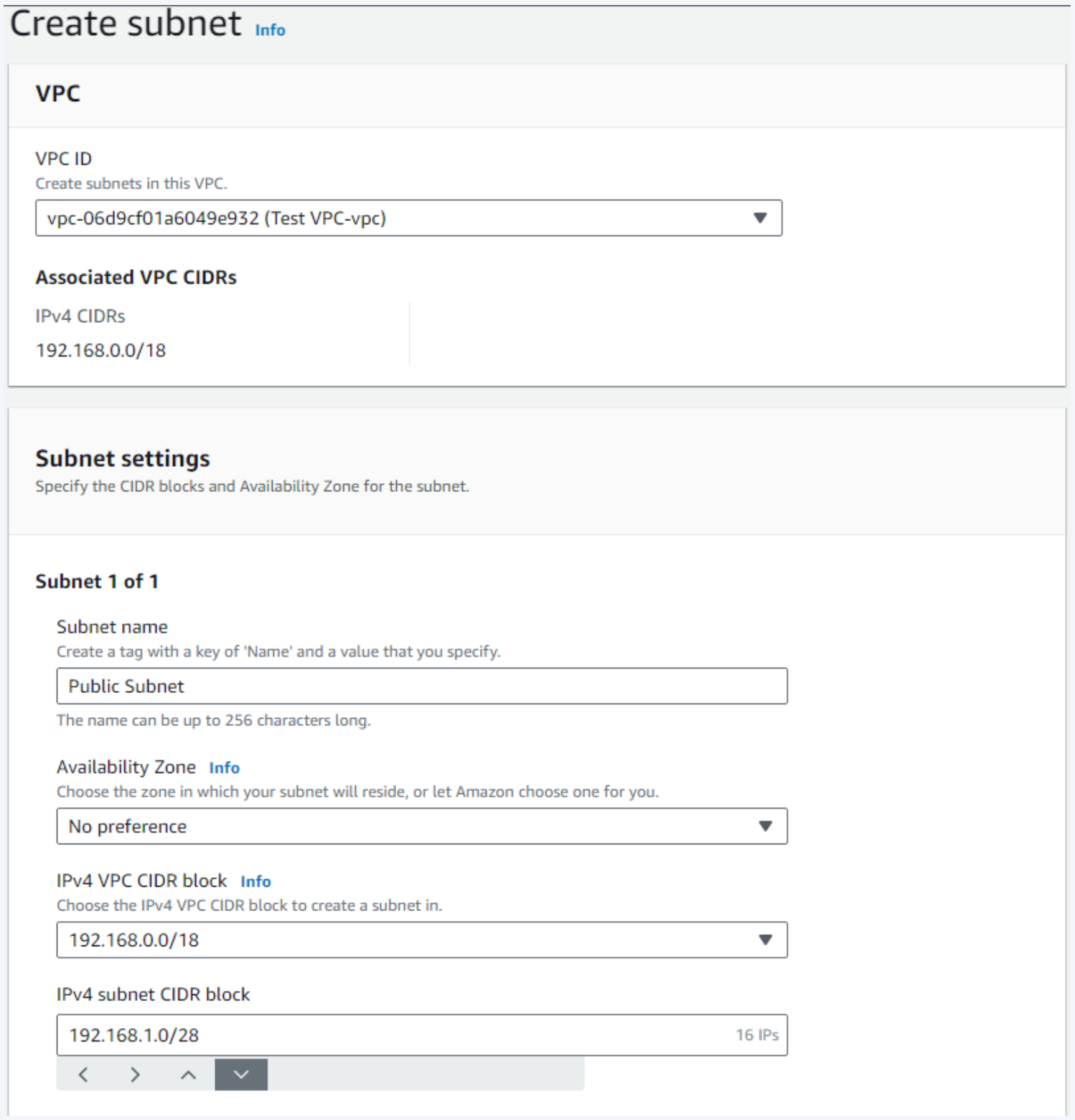
Empezamos por la creación de la VPC:



SWIPE

Tarea 01

Luego procedemos a **crear la subred** pública con el bloque CIDR de direcciones IP públicas requerido:



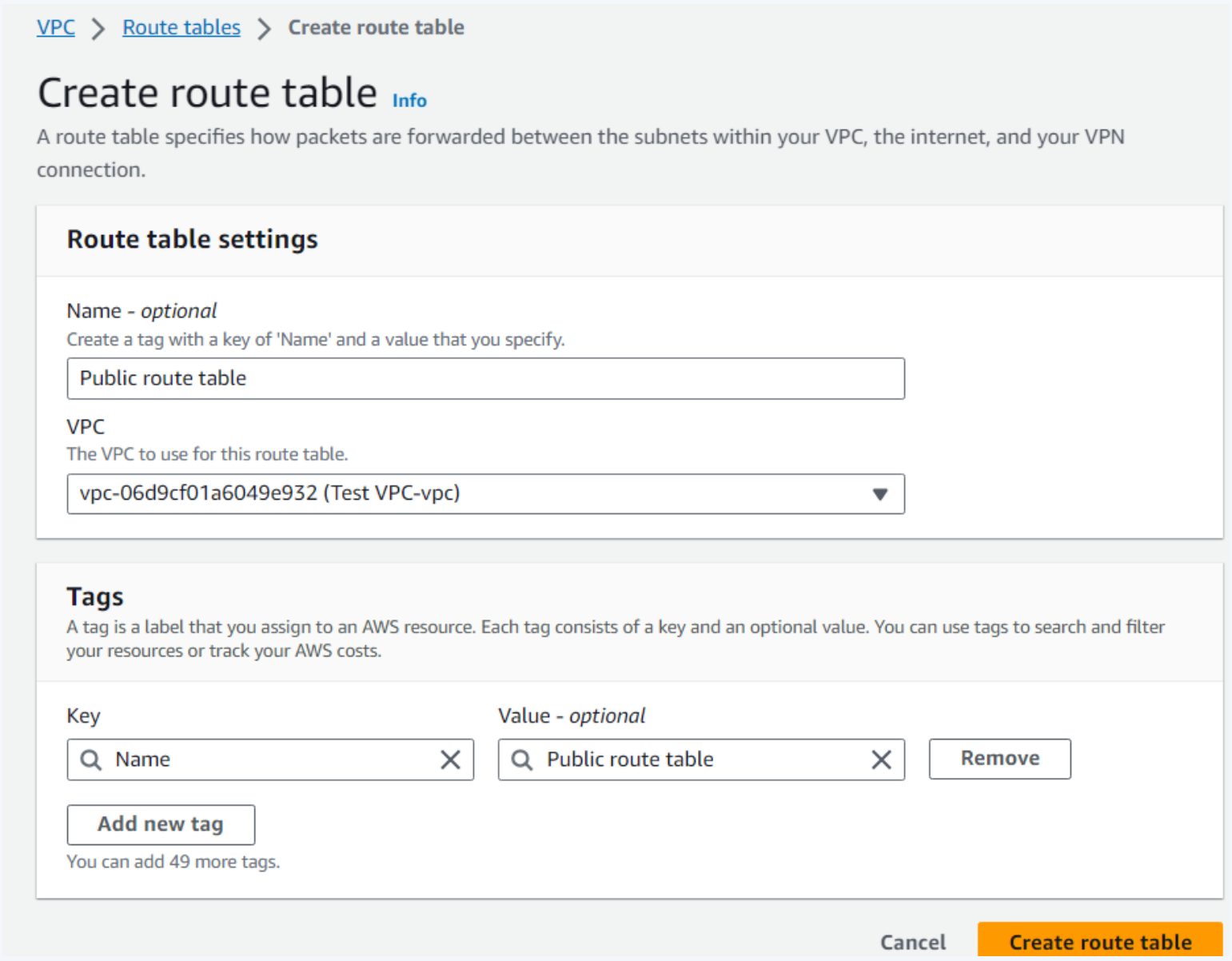
SWIPE

Tarea 01

Ahora, procedemos a crear la *tabla de enrutamiento*, que nos indicará **las direcciones IP y target** dentro de la VPC y subreds (dónde se dirige el tráfico), **define si una subred es pública o privada**.

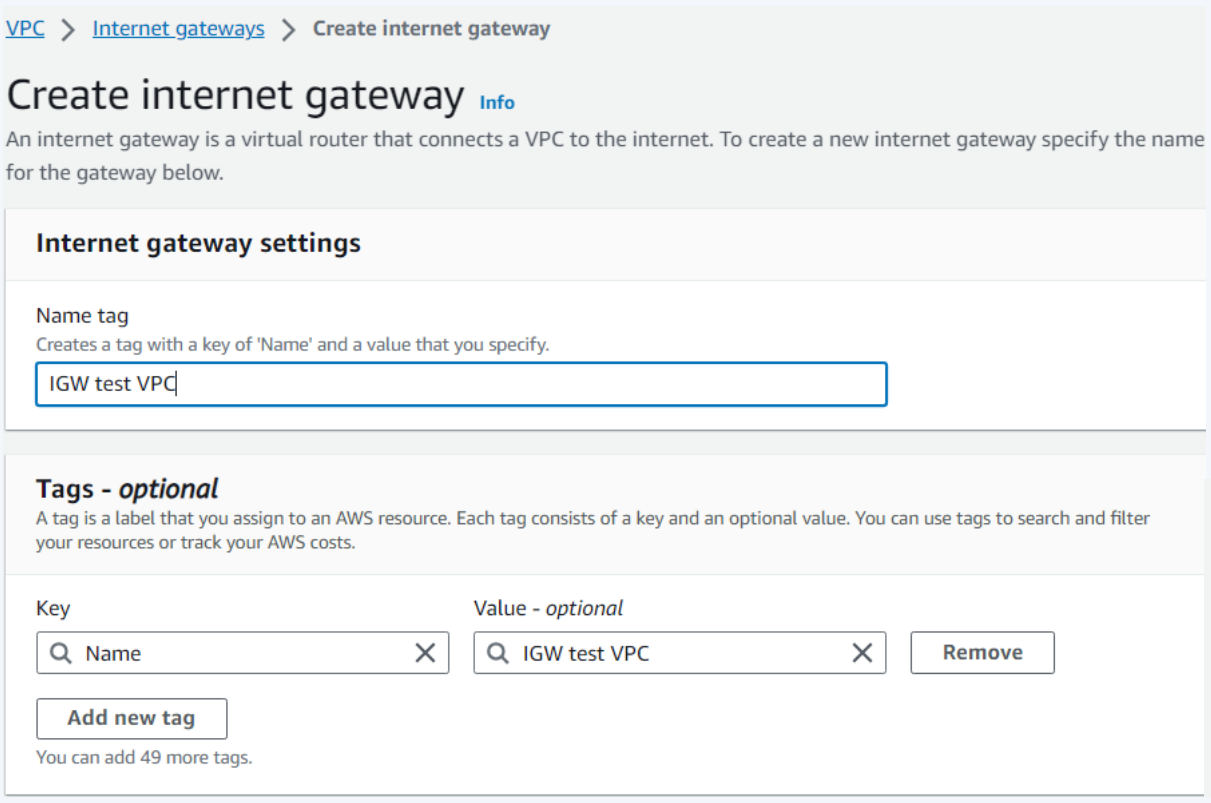
OJO:

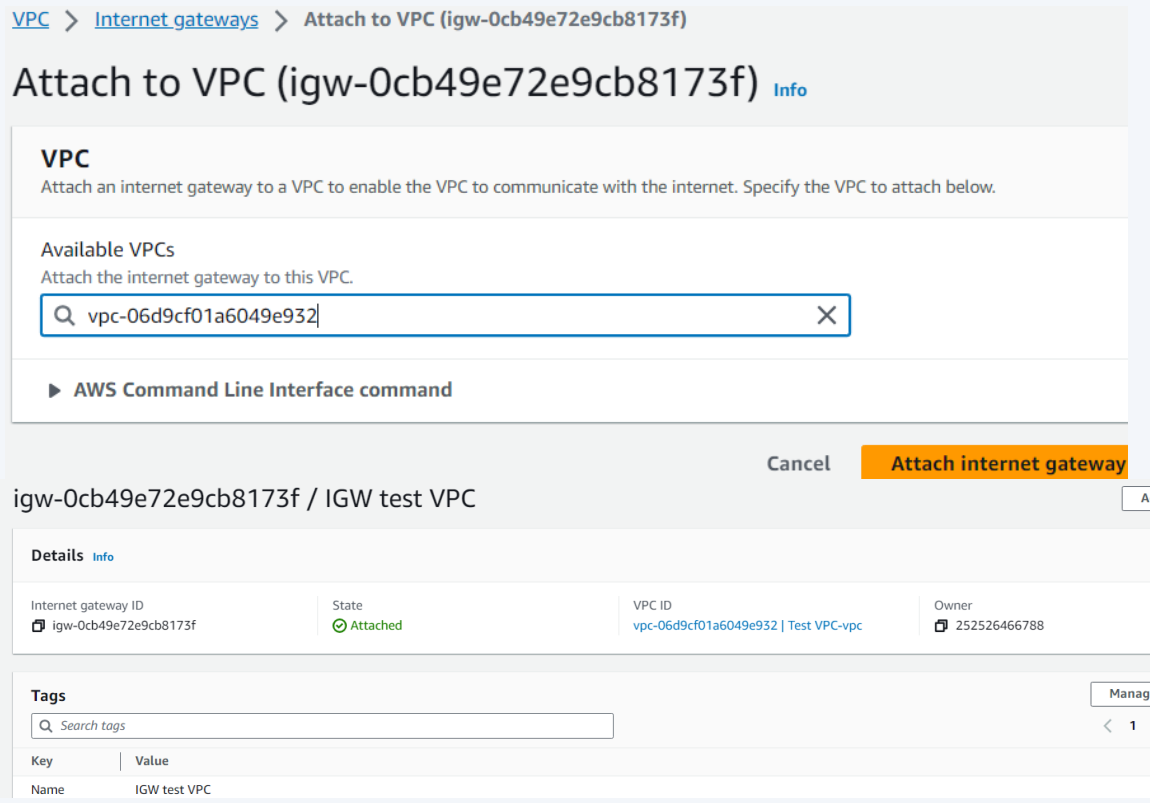
- Se debe asociar una tabla de enrutamiento a cada subred. Y se van asignando las rutas según se van creando los servicios en la VPC



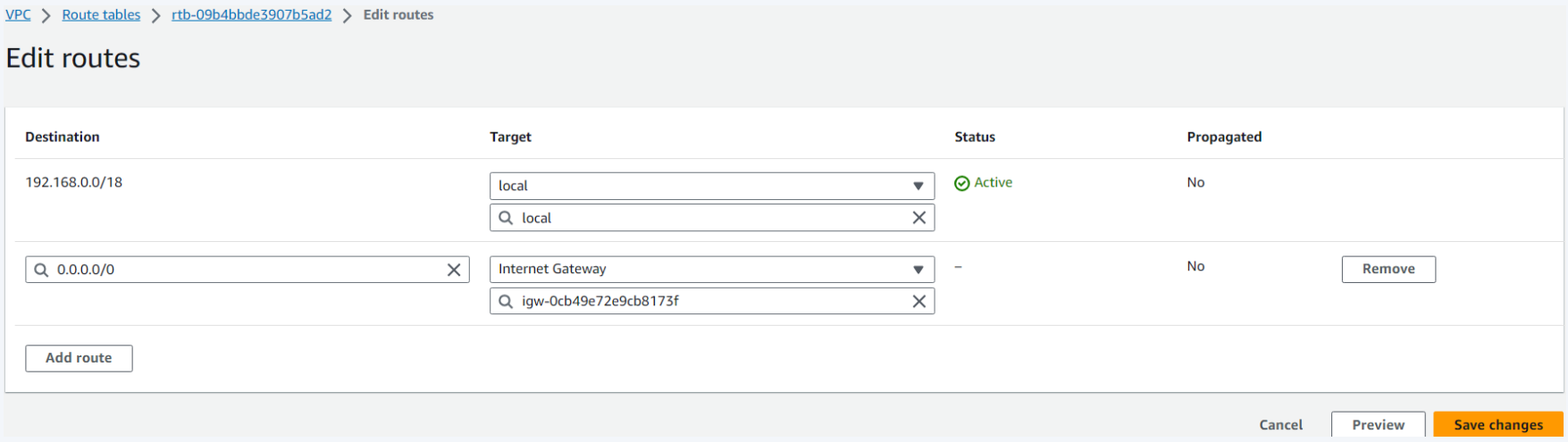
Tarea 01

Ahora, procedemos a crear la *puerta de enlace de internet (IGW)*. Y la adjuntamos a la VPC creada





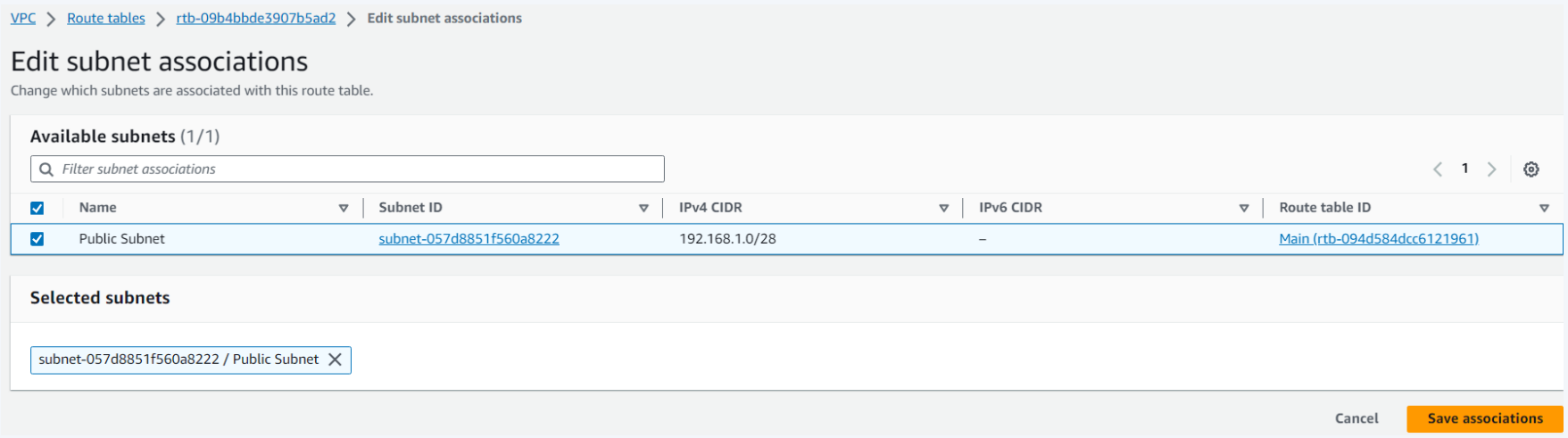
Ahora, procedemos a hacer que el tráfico que desea salir a internet de los servicios de la subred pública, debe pasar por el Internet Gateway



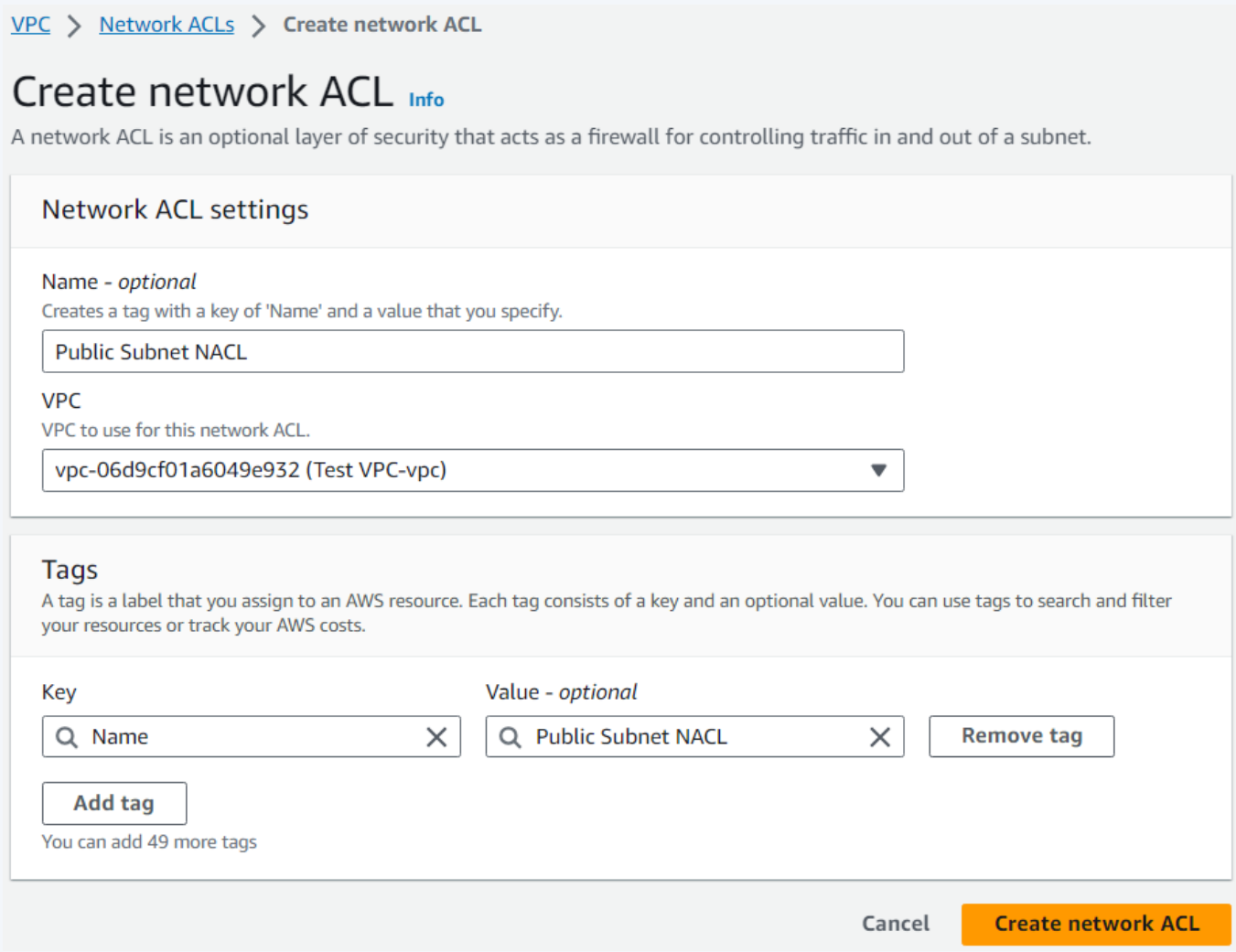
SWIPE

Tarea 01

Y ahora asociamos la tabla de enrutamiento a la subred pública que hemos creado



Ahora, procedemos a crear una *lista de control de acceso de red (NACL)*, que es un firewall de la subred.
OJO: Primero se evalúa la regla con el número menor



SWIPE

Tarea 01

Y debemos modificar las reglas de ingreso y salida de tráfico de la subred.
En el caso de **inbound rules**, indica que hay un solo número de regla, que es 100 y que establece que **todo el tráfico**, todos los protocolos y todos los rangos de puerto desde **cualquier origen (0.0.0.0/0) pueden ingresar (entrar) a la subred**. El asterisco *** indica que se rechaza todo** lo que **no coincida con esta regla**. Similar para outbound, pero para tráfico que sale de la subred a cualquier destino (0.0.0.0/0)

Details | Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (2)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Details | Inbound rules | Outbound rules | Subnet associations | Tags

Outbound rules (2)

Edit outbound rules

Filter outbound rules

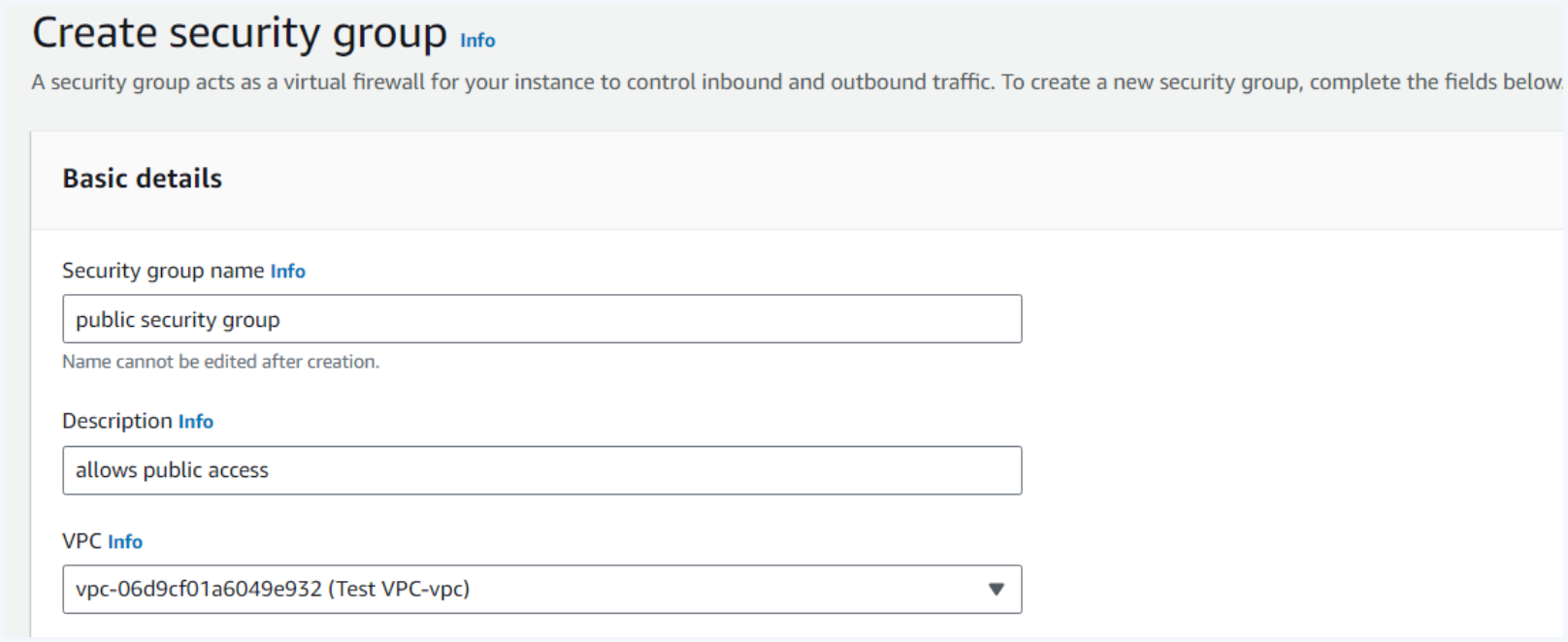
1

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

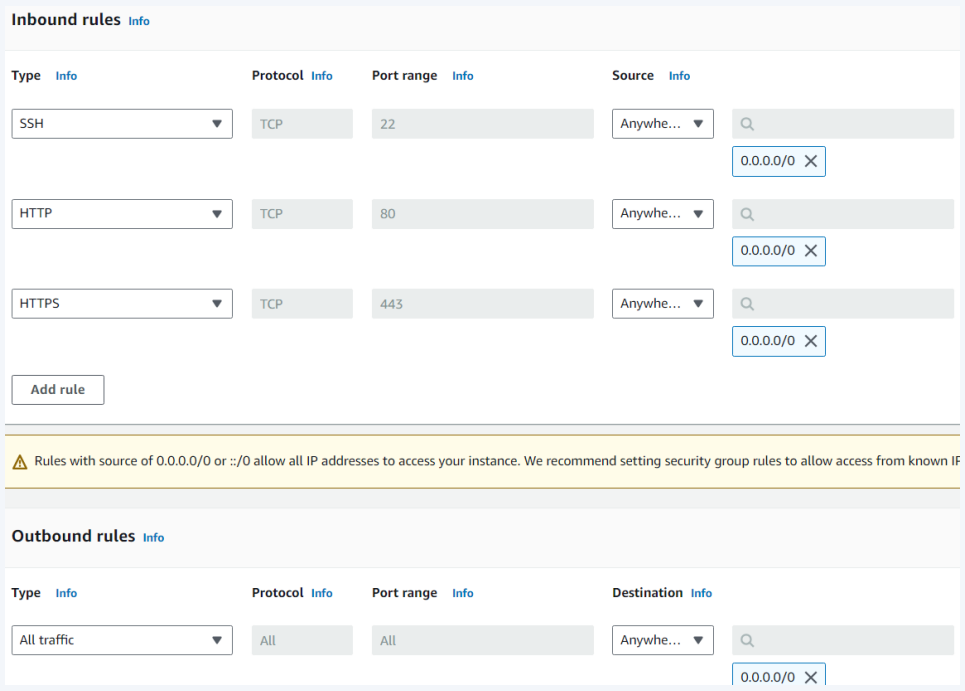
SWIPE

Tarea 01

Ahora procedemos a crear un **grupo de seguridad**, el cual es una capa de seguridad a nivel de instancia. Pero a diferencia de la NACL, **no pueden rechazar tráfico**.



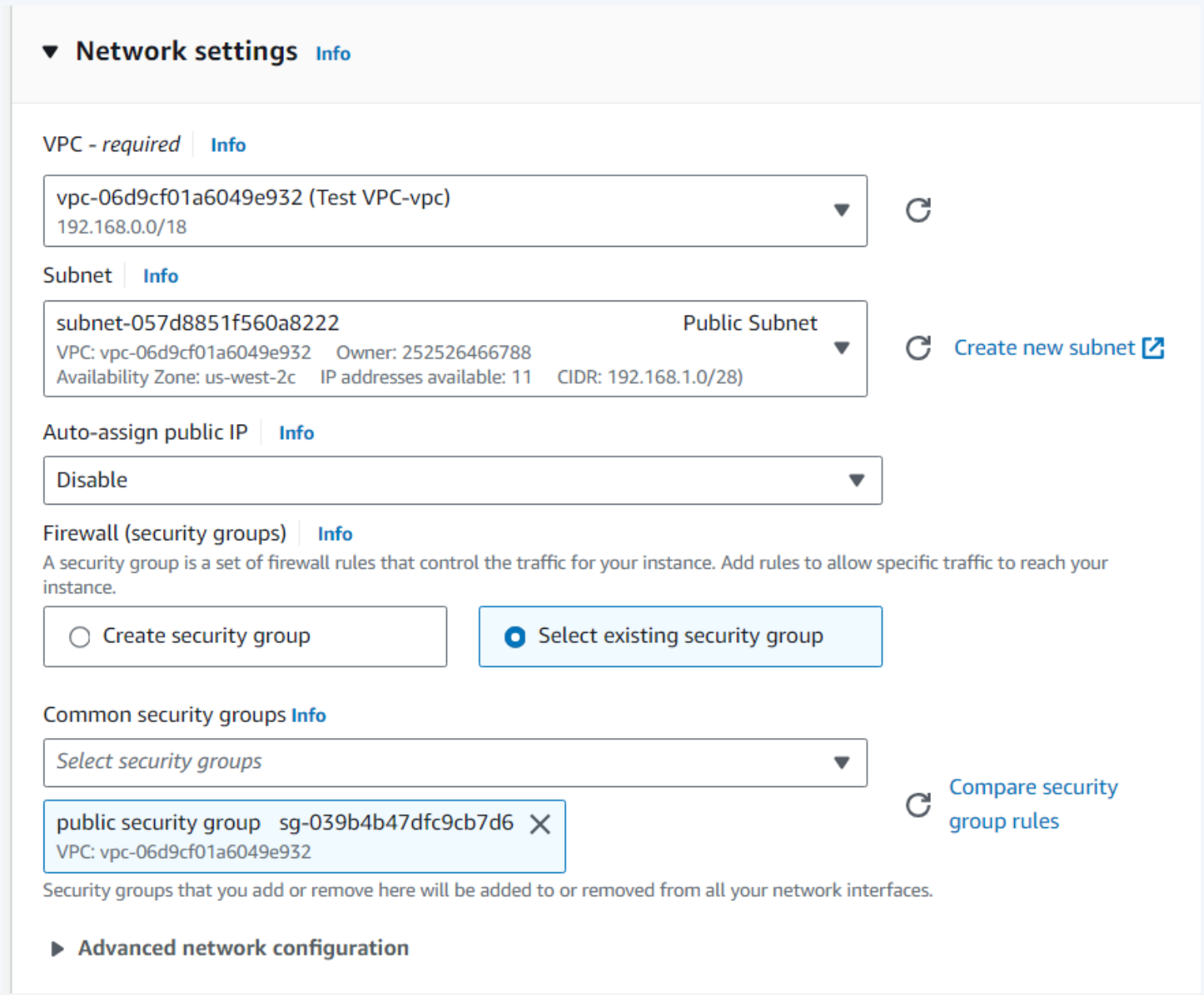
Para las **reglas de entrada**, está permitiendo los tipos de tráfico **SSH, HTTP y HTTPS**, cada uno con sus propios protocolos y rango de puertos. El origen desde el que este tráfico llega a la instancia **se puede originar desde cualquier lugar**. En el caso de las **reglas de salida**, está permitiendo todo el tráfico hacia afuera de su instancia.

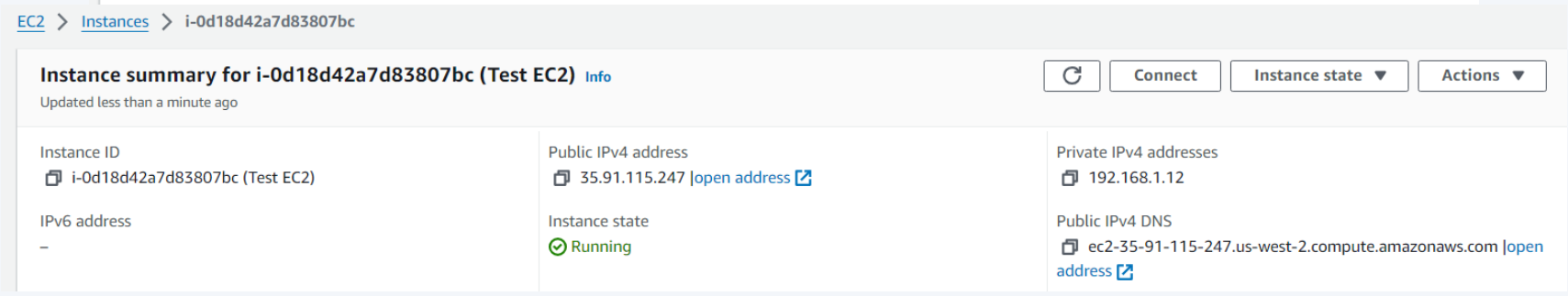


SWIPE

Tarea 01

Ahora creamos una instancia de EC2, la cual será desplegada dentro de la subred pública creada. Luego verificaremos si todos nuestros cursos de red que hemos creado están correctamente configurados

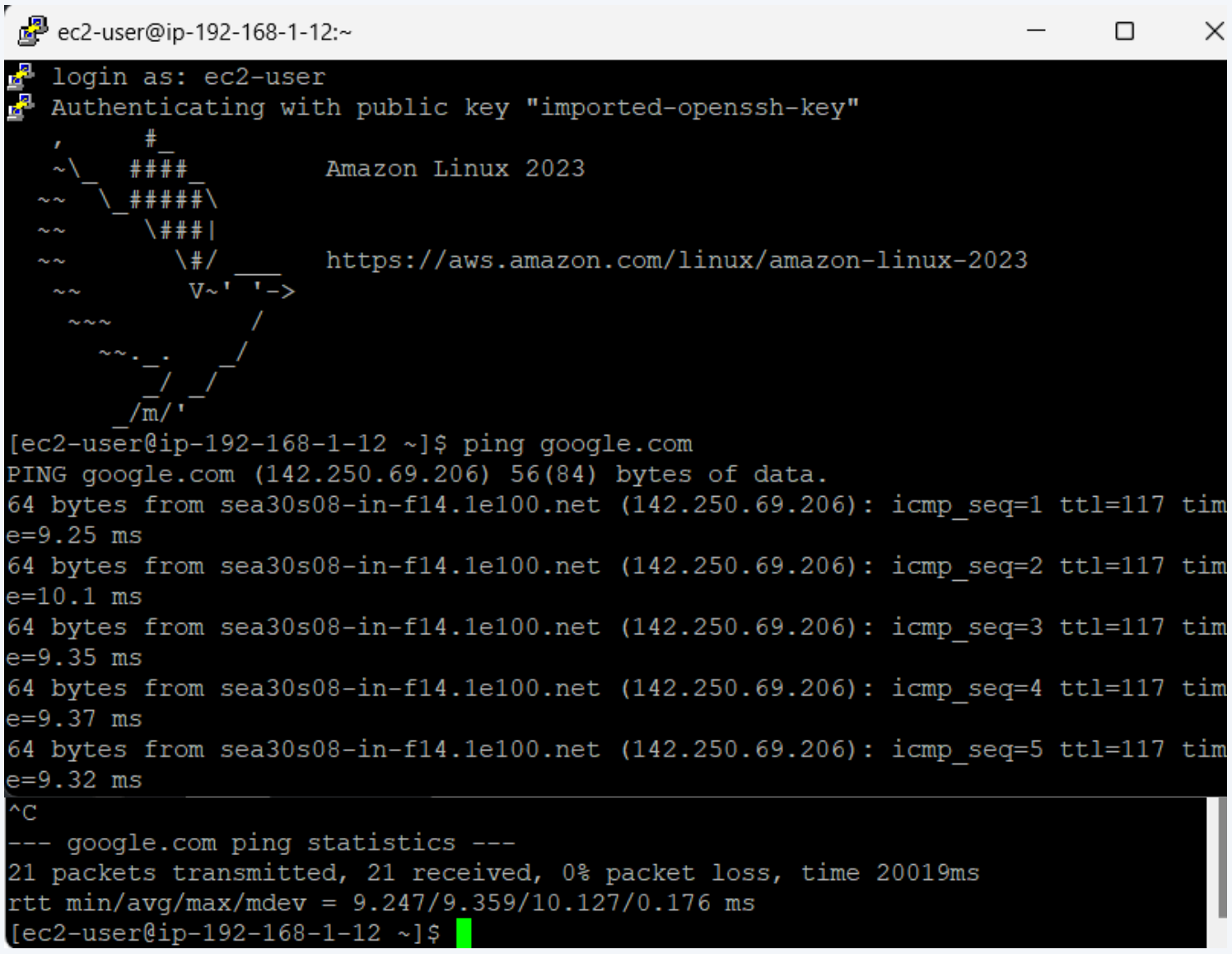




SWIPE

Tarea 01

Ahora mediante la conexión por SSH, verificaremos la conectividad:



Notamos que sí existe conectividad.

SWIPE