GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro
GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació
CFR CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES
FPcv
Formació Professional Comunitat Valenciana

NAT Gateway - subredes privadas

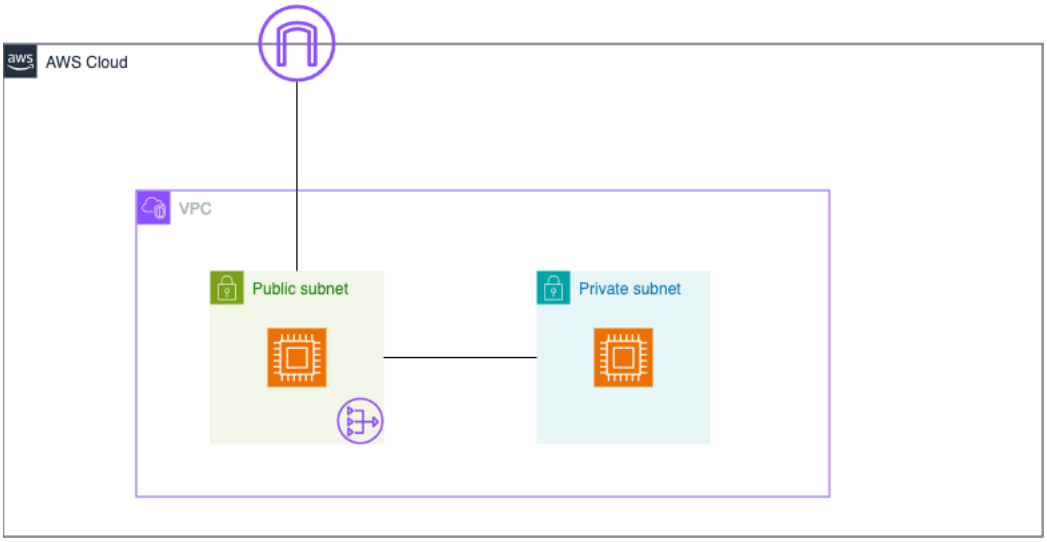
Reglas encadenadas y NACL

Escenario 3
Conexión SSH 7
NACL (network Access control list) 11
Escenario 11
VPC 11
Reglas encadenadas 16
Tareas 18

Escenario

El escenario propuesto que vamos a desarrollar es el siguiente, una subred pública y una subred privada, la cual sólo tendrá acceso al exterior pasando primero por la subred pública:

- Direccionamiento VPC: 172.16.0.0/16
- Direccionamiento subred pública: 172.16.0.0/20
- Direccionamiento subred privada: 172.16.64.0/20



https://docs.aws.amazon.com/es_es/vpc/latest/userguide/vpc-nat.html

Primero se montará el escenario utilizando el panel de control y se revisarán las opciones y las tablas de enrutamiento que facilitan esta situación, si queréis ir más rápido o sois fans de la consola también podéis enlazar con el tema anterior y reutilizar el script para montar casi todo, sólo faltará el NAT Gateway y la subred privada.

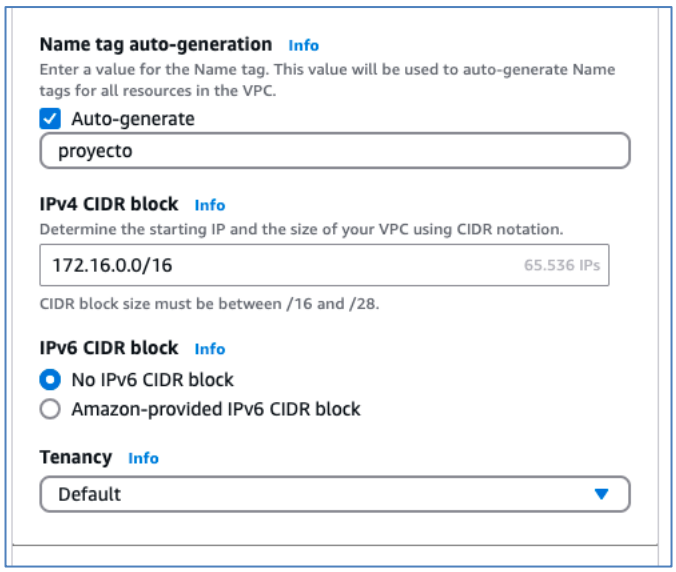
En nuestro caso podríamos crear una VPC y desde allí ya podríamos crear una subred privada, pero este NO es el caso de los pasos que vamos a seguir.

Aunque en nuestro caso, voy a reutilizar el script y a partir de ahí añadir la subred privada y los elementos que nos hagan falta. Es decir, añadir una subred pública, con un internet gateway y la tabla de enrutamiento para salir al exterior, para montar la VPC y la subred pública podéis usar la interfaz web de la consola de administración. ASUMO a partir de aquí que lo hacéis con la interfaz gráfica.

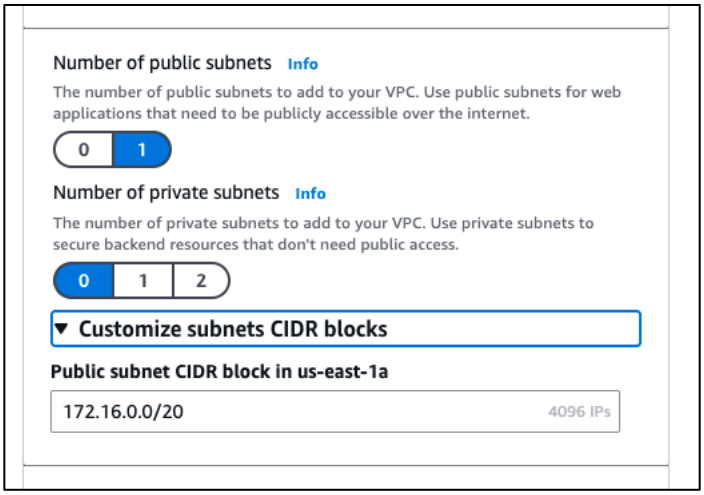
Resumiendo:

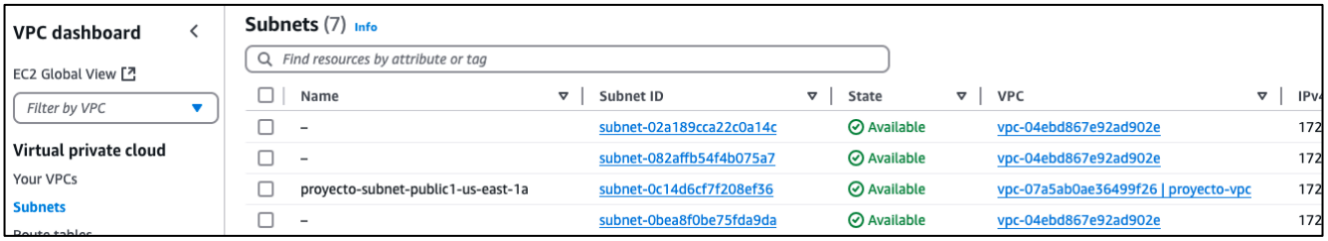
Tenemos una VPC, una subred pública, un IGW y una tabla de enrutamiento.

A continuación, se muestra el direccionamiento de la VPC:

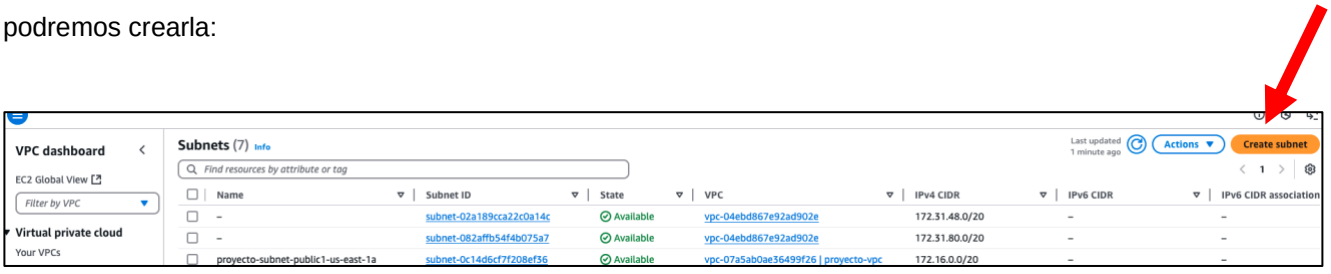


Y ahora el direccionamiento de la subred pública (la subred privada la crearemos más adelante)

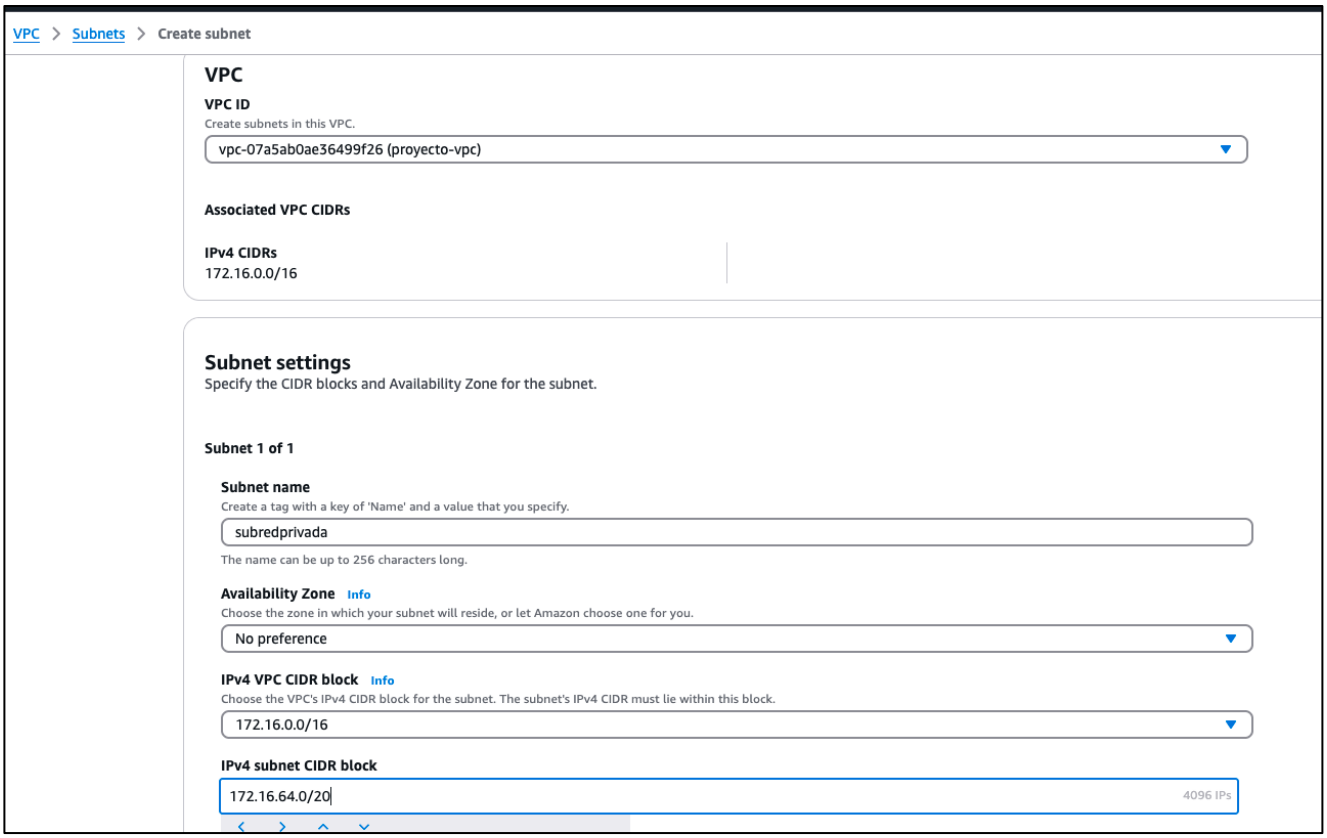




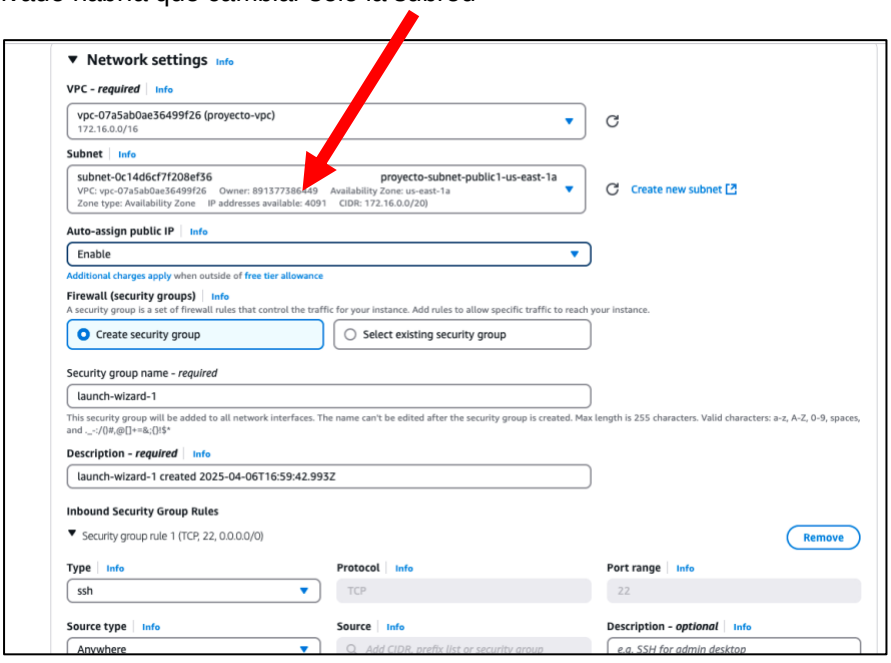
Ahora partiendo de aquí lo primero es crear una subred (que será la privada). Desde el menú de Subnets podremos crearla:



Al crearla con las siguientes opciones:

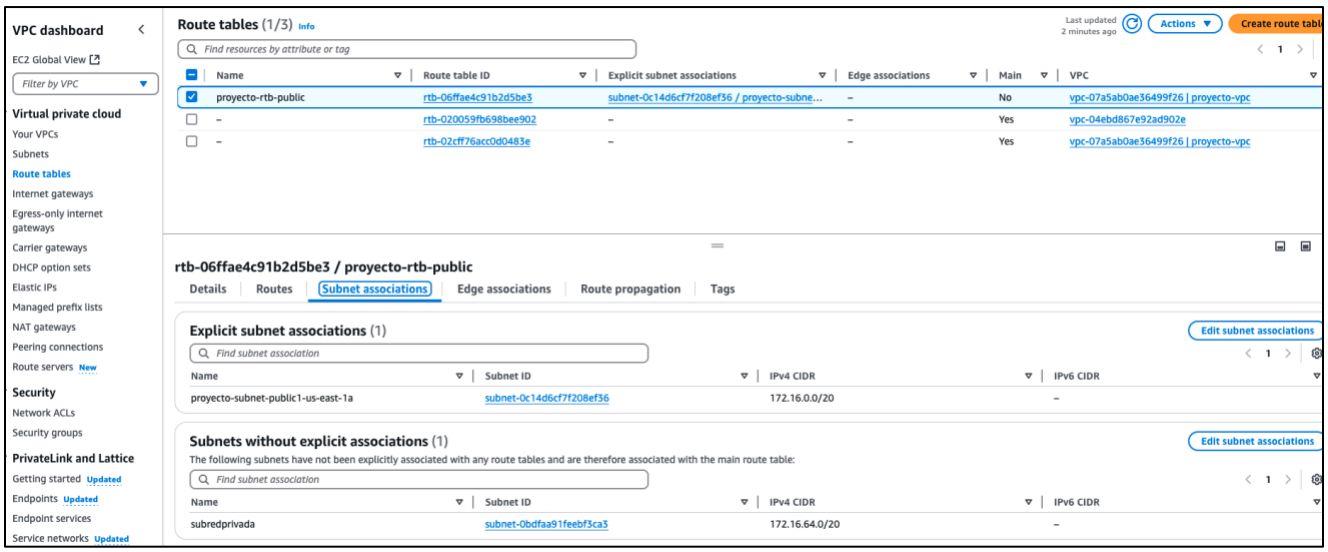


Y una ec2 para la subred pública y otra para la subred privada. Se muestra la configuración para el ec2 público, para el privado habría que cambiar sólo la subred



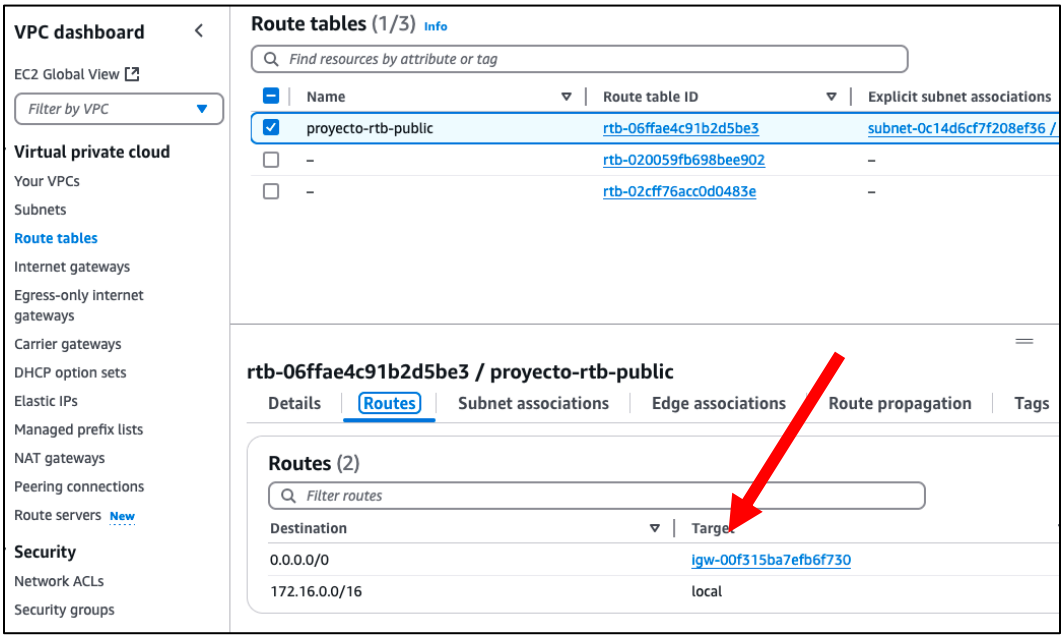
Miramos la ip pública del ec2 creado en la subred privada e intentamos hacer un ssh, la respuesta es que NO se puede acceder. NO está asociada la subred en el internet gateway para poder enrutarlo hacia fuera.

Si comprobamos la tabla de enrutamiento desde el menú VPC -> Route tables podremos ver que tenemos una tabla asociada a la VPC en la cual solo hay asociada una subred (siendo la pública solamente).



La subred privada nos aparece en la pestaña “Subnets without explicit associations”, lo que quiere decir que está preparada para ser añadida a la tabla de enrutamiento, pero aún no lo hemos hecho.

Realmente lo que pretendemos es hacer que la subred privada salga a través del a subred pública, para ello cada subred tiene su propia tabla de enrutamiento, la subred pública tiene una ruta hacia el internet gateway para poder salir.



En este punto podríamos conectarnos por ssh a la instancia de la red pública y hacer ping a www.google.es y funcionaría y desde esta instancia conectarnos por ssh a la instancia de la subred privada, lo que pasa es que aún falta conocer un par de comandos que veremos más adelante para poder conectarnos, pero si alguno se atreve y lo logra el ping desde la subred privada NO funciona.

```
[ec2-user@ip-172-16-2-45 ~]$ ping www.google.es
PING www.google.es (142.251.179.94) 56(84) bytes of data.
64 bytes from pd-in-f94.1e100.net (142.251.179.94): icmp_seq=1 ttl=56 time=1.68 ms
64 bytes from pd-in-f94.1e100.net (142.251.179.94): icmp_seq=2 ttl=56 time=1.71 ms
^C
--- www.google.es ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.677/1.692/1.708/0.015 ms
[ec2-user@ip-172-16-2-45 ~]$ ssh 172.16.68.71
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Sun Apr  6 17:18:34 2025 from 172.16.2.45
[ec2-user@ip-172-16-68-71 ~]$ ping www.google.es
PING www.google.es (142.250.31.94) 56(84) bytes of data.
^C
--- www.google.es ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3110ms
```

Ahora vamos a crear una tabla de enrutamiento para la subred privada (aunque podríamos usar la tabla que ya hay creada).

Llegados a este punto, vamos a explicar cómo poder hacer estas pruebas y arrastrar las credenciales (labuser.pem) ya que vamos a usar las mismas para las dos instancias, aunque también se podría hacer usando diferentes credenciales.

Conexión SSH

Seguiremos los pasos indicados para equipos Linux. En primer lugar, comprobamos que las claves privadas tienen los permisos adecuados. Desde el terminal ejecutaremos los siguientes comandos:

- Ejecutamos ssh-agent en 2º plano:

eval $(ssh-agent)

- Cargamos en memoria la clave privada de la instancia :

ssh-add labsuser.pem

- Podemos ver las claves privadas mediante el comando:

ssh-add -l

- Nos conectamos en primer lugar a la instancia de la subred pública. Como se puede comprobar, al realizar la conexión también tenemos disponible en memoria, la clave privada del servidor app.

ssh -i labuser.pem -A ec2-user@noombrednsdelainstancia

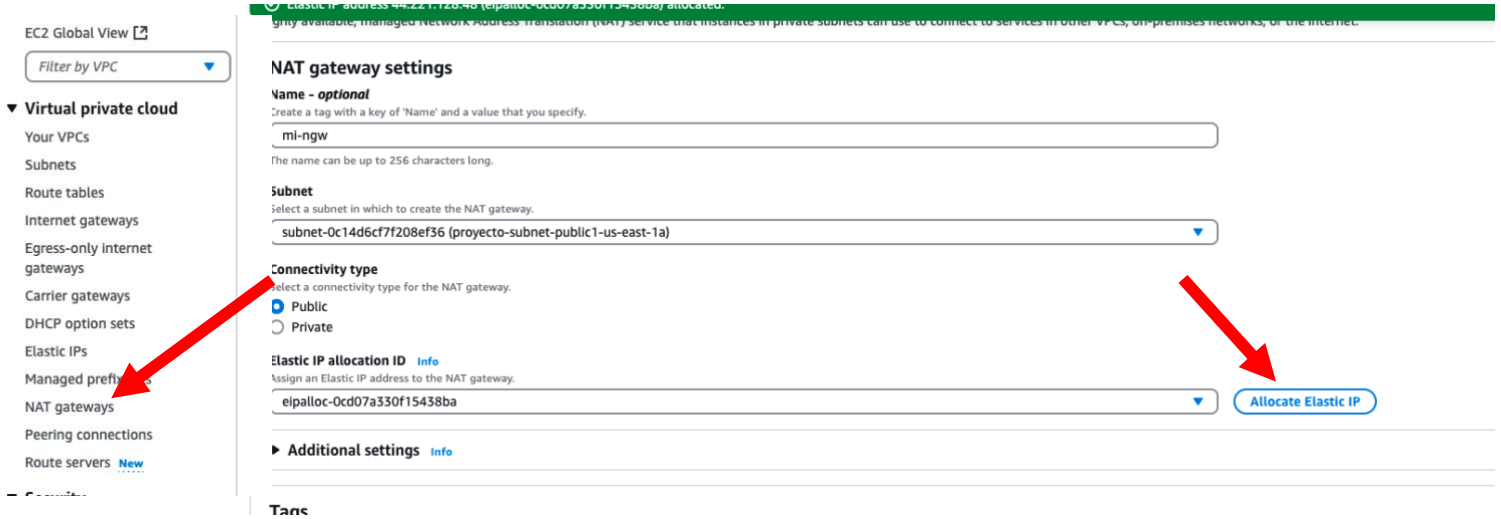
- Seguidamente nos conectamos a la instancia de la subred privada

ssh direccionipprivada

- Cuando realices la conexión ssh deberás usar el parámetro -A que es el que permite el reenvío de clave privada.

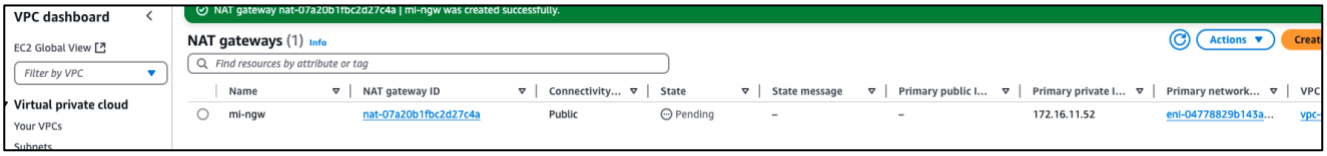
Una vez ya hemos logrado tener acceso a la instancia de la subred privada si intentamos hacer por ejemplo un ping a www.google.es veremos que no somos capaces. Hasta ahora lo que hemos logrado hacer es llegar hasta la instancia, pero ¿y si la instancia quiere actualizarse o tener acceso a Internet por cualquier motivo? Para esta casuística aparece el servicio NAT Gateway, que lo que nos permite es conectarnos/establecer una conexión con el exterior y que nos devuelvan respuesta, pero si se intentase establecer una conexión desde el exterior esta NO sería posible ya que el dispositivo no capacita para conectarte desde fuera.

Lo primero es crear un nat gateway desde el menú VPC:

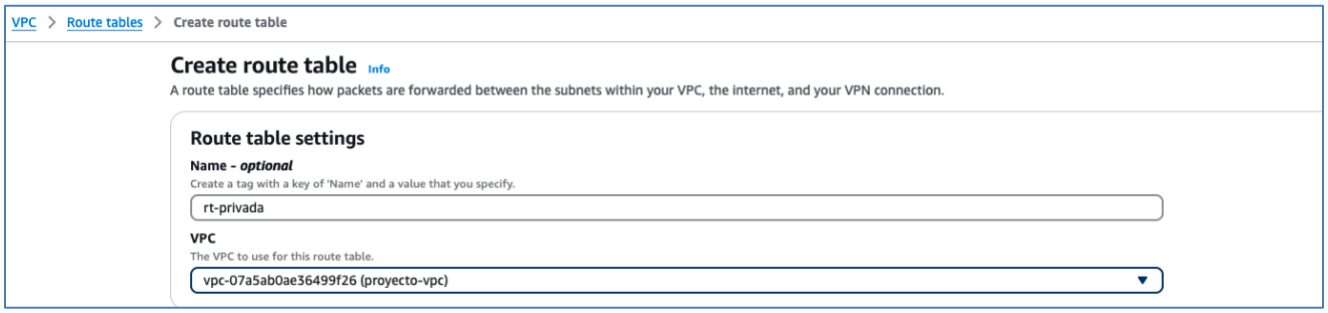


Aquí aparece por primera vez el concepto de ip elástica, una ip elástica es una ip pública que vamos a poder reutilizar en cualquier servicio, es decir si hubiera un servicio que necesitase de una ip, o bien puedo utilizar las que AWS me da de normalmente de forma dinámica o si ya necesitase una estática que no varíe podría utilizar la ip elástica, por supuesto reservar una ip de esta forma conlleva un gasto asociado.

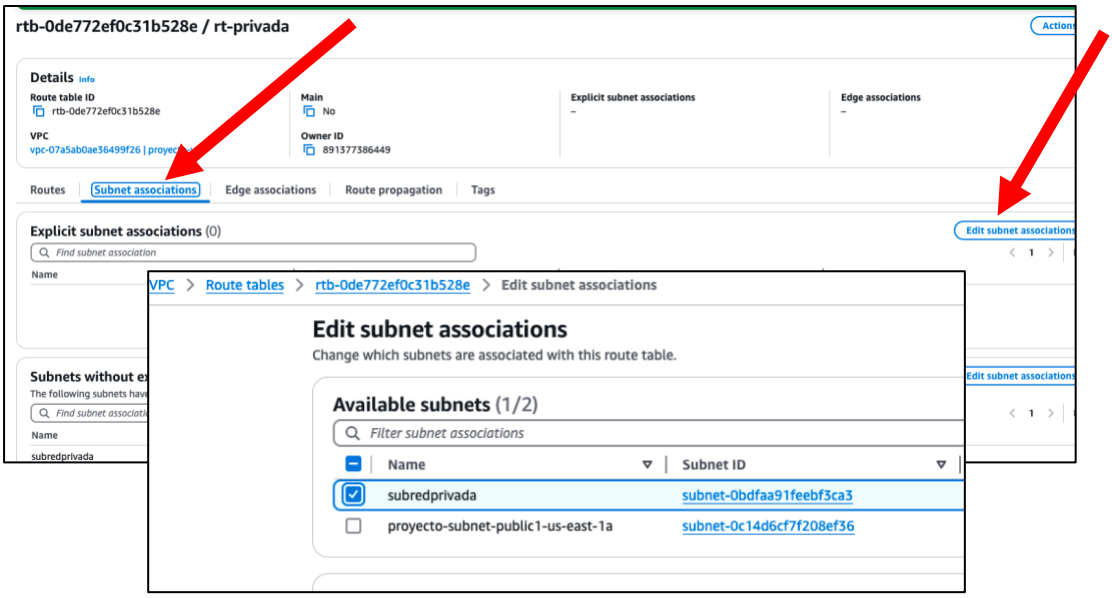
Ya que este servicio necesita de una, si no tenemos una haremos clic en asignar ip elástica y nos creará una (es un coste adicional el tener una ip elástica). La creación del nat gateway lleva un rato y habrá que esperar a que esté en estado “available”. Para este caso el nat gateway lo vamos a crear en la subred pública (ya veremos más adelante por qué).



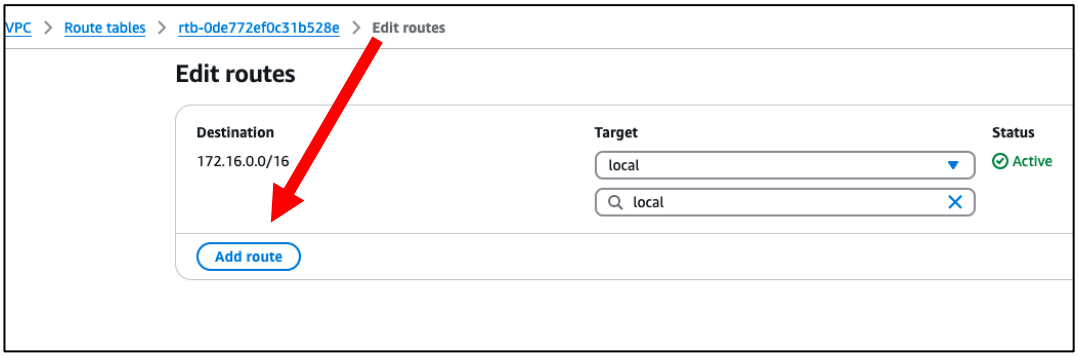
Ahora vamos a configurar la subred privada para que tenga conexión al exterior. Para ello vamos a crear una tabla de enrutamiento para este dispositivo desde el menú VPC.



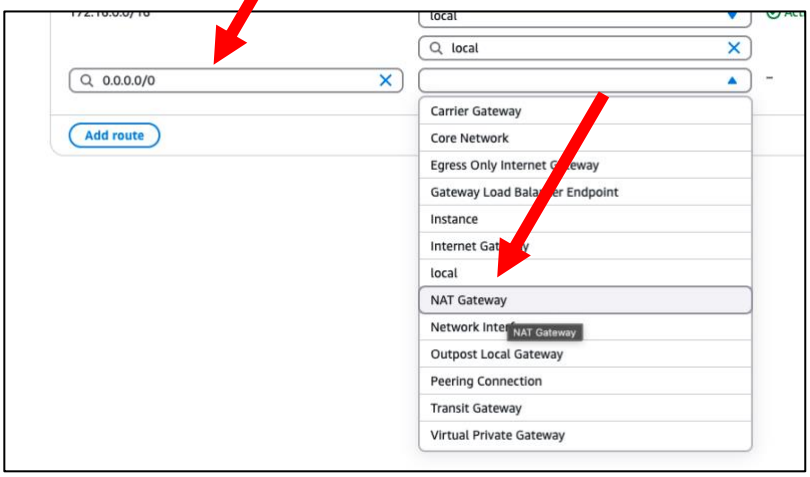
Cuando se cree esta tabla le asociaremos la subred privada desde la pestaña “subnet associations” haciendo click en “Edit subnet associations”

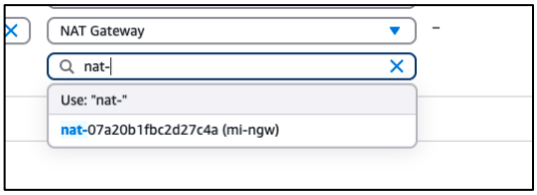


Cuando esté disponible iremos a la tabla de enrutamiento de la subred privada (pestaña routes) y podemos ver las rutas preconfiguradas:



Ahora añadiremos una ruta para redirigir el tráfico que vaya a Internet hacia el nat gateway y éste ya se encargará de dar salida.





Ahora podremos hacer dos comprobaciones:

- NO podemos hacer ping desde el exterior:

```
Last login: Sat Apr  5 11:19:14 on ttys003
jorge@mjolnir Downloads % ssh -i labsuser.pem ec2-user@34.232.109.141
```

- Cuando hagamos ping desde la ec2 de la red privada a Google SÍ que nos devolverá respuesta.

```
[ec2-user@ip-172-16-68-71 ~]$ ping www.google.es
PING www.google.es (142.251.179.94) 56(84) bytes of data.
64 bytes from pd-in-f94.1e100.net (142.251.179.94): icmp_seq=1 ttl=105 time=3.20 ms
64 bytes from pd-in-f94.1e100.net (142.251.179.94): icmp_seq=2 ttl=105 time=2.27 ms
64 bytes from pd-in-f94.1e100.net (142.251.179.94): icmp_seq=3 ttl=105 time=2.30 ms
^C
```

NACL (network Access control list)

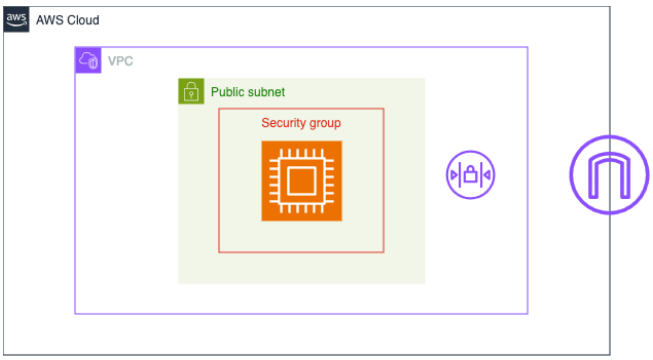
Una NACL es un componente de seguridad que actúa como un firewall (es un firewall) a nivel de subred dentro de una VPC. Hasta ahora hemos estado trabajando con los grupos de seguridad que son reglas con estado, es decir, cuando se establece una conexión ésta se puede devolver y NO es necesario habilitar una regla que lo permita explícitamente. Sin embargo, AWS ofrece otro nivel de seguridad y son las NACL, ACL network o ACL de red.

Es decir, las reglas de seguridad con estado, identificando por ejemplo el caso de un ping, cuando realizamos un ping y añadimos en el grupo de seguridad la regla que permite el ICMP, cuando se realiza el ping la entrada del ping se permite e implícitamente se permite la salida por cualquier puerto ya que es una conexión establecida. Sin embargo, en el caso de las NACL este permiso implícito NO es dado, hay que configurar tanto las reglas de entrada como las de salida.

El objetivo de la práctica es comprobar que los grupos de seguridad son capaces de guardar el estado y la ACLs de red no guardan el estado, para ello montaremos en una VPC una subred pública con su correspondiente EC2, permitiremos la entrada del ping mediante una NACL, pero NO la salida, para comprobar que el ping NO sale y luego más tarde lo permitiremos.

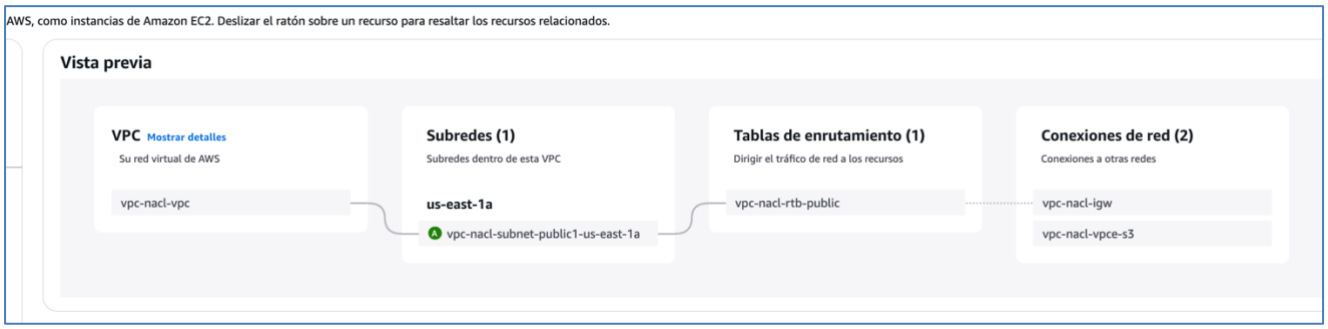
Antes de continuar recuerdo que es recomendable eliminar todo lo que hemos hecho anteriormente para no confundirnos y tener los siguientes conceptos claros. Se puede realizar un reset también del laboratorio, pero dejará éste inaccesible durante un buen rato mientras realiza la limpieza del lab.

Escenario

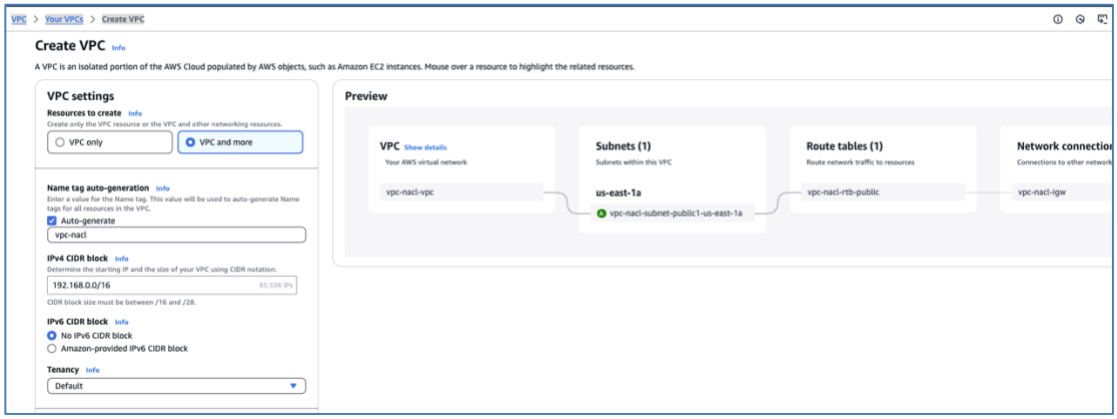


VPC

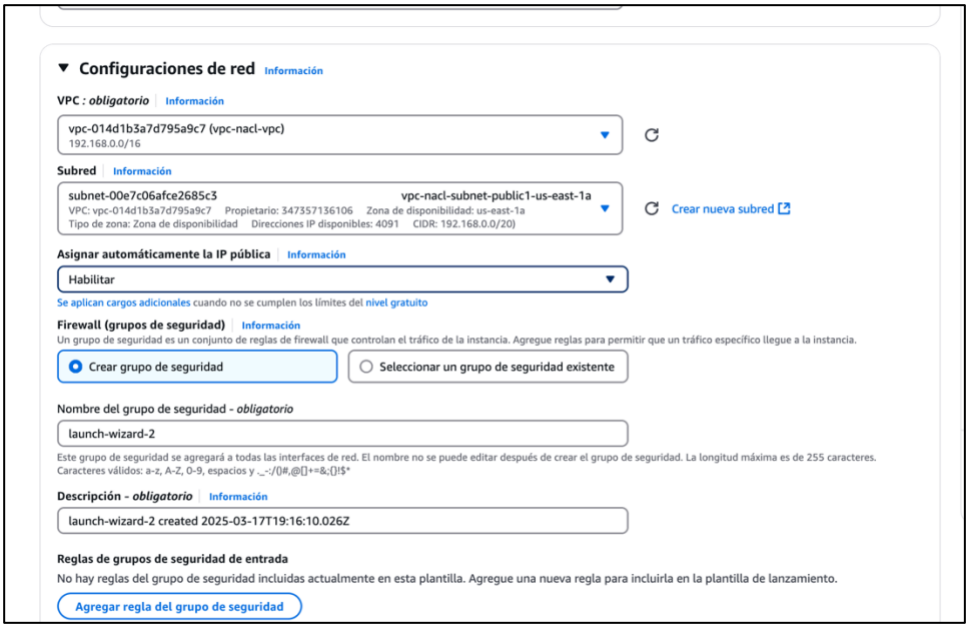
Lo primero es crear la VPC junto con la subred. Para ello seguiremos las siguientes capturas:



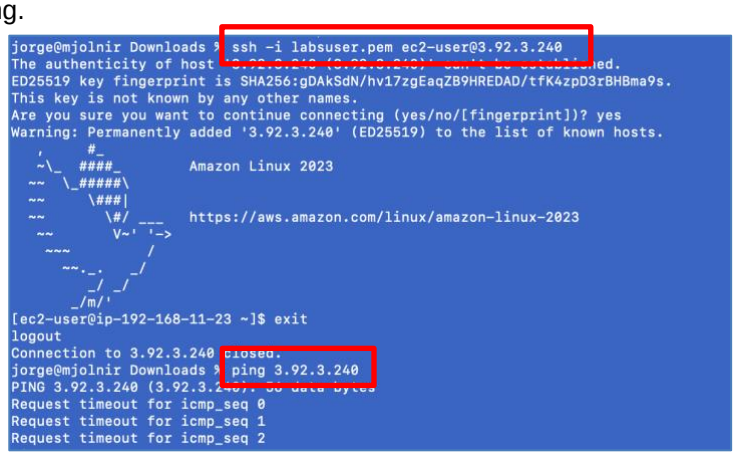
Además, como no vamos a crear redes privadas no nos hará falta crearlas.



Una vez creada la infraestructura pasaremos a lanzar la instancia dentro de la VPC.



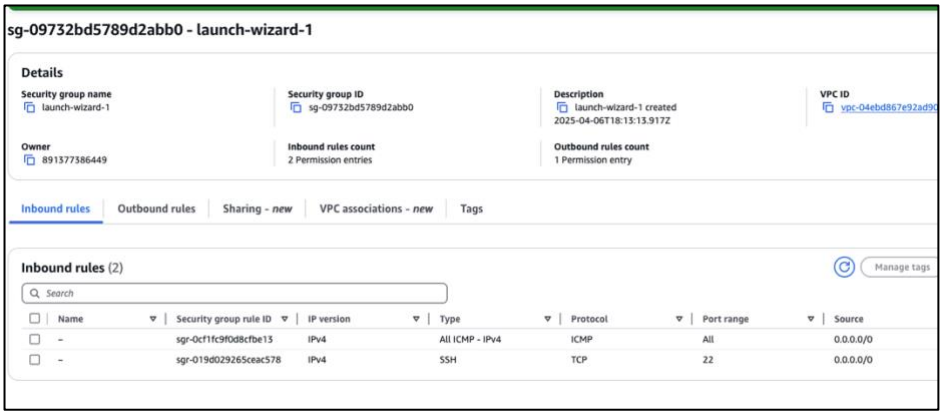
Como siempre, podemos entrar por ssh y ver que está hábil la instancia y, ya que estamos, también podemos probar el ping.



Previamente vamos a modificar el grupo de seguridad y permitir el ping y ver que funciona. Una vez hecha esta comprobación vamos a jugar con las NACL para activar el ping, aunque sea un poco más laborioso.

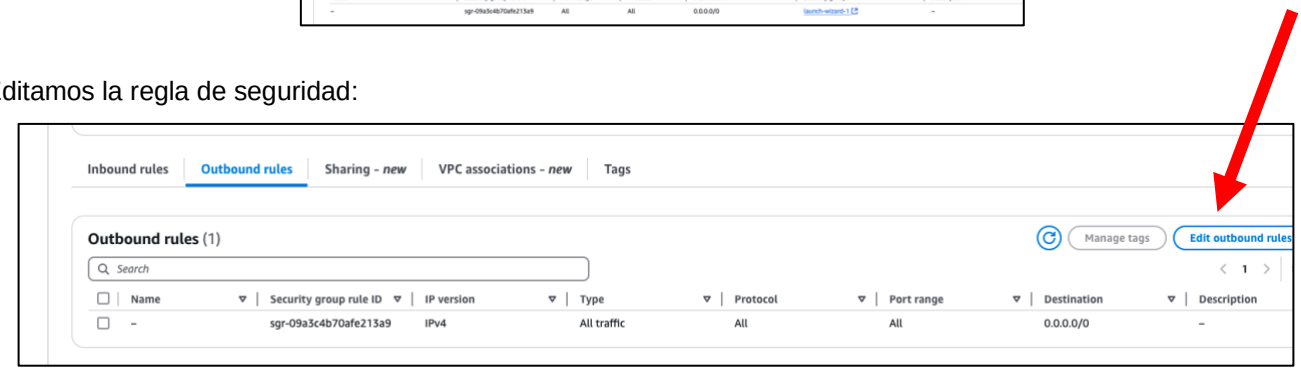
Hay que tener en cuenta que por defecto TODO el tráfico entrante se deniega. Por lo tanto, daremos permiso al protocolo ICMP en una regla de entrada y salida del ping y luego denegaremos la salida del ping y ver como ya no responde.

El ec2 con el grupo de seguridad configurado para permitir el ping tendría un aspecto como el siguiente:

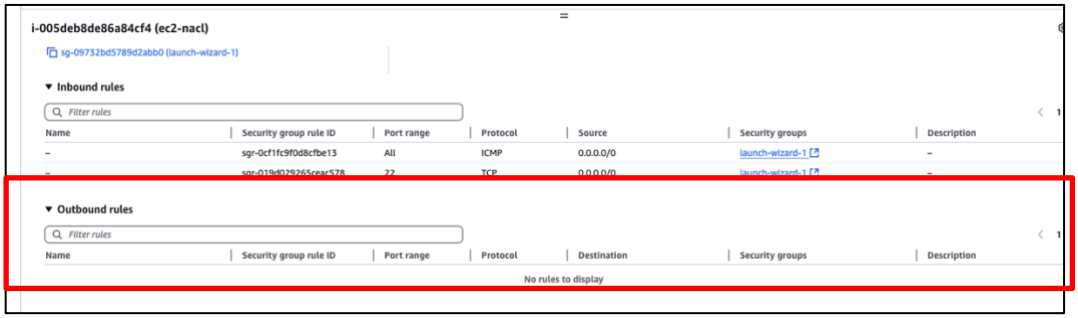


Primero la regla de seguridad con la regla de salida.

Editamos la regla de seguridad:

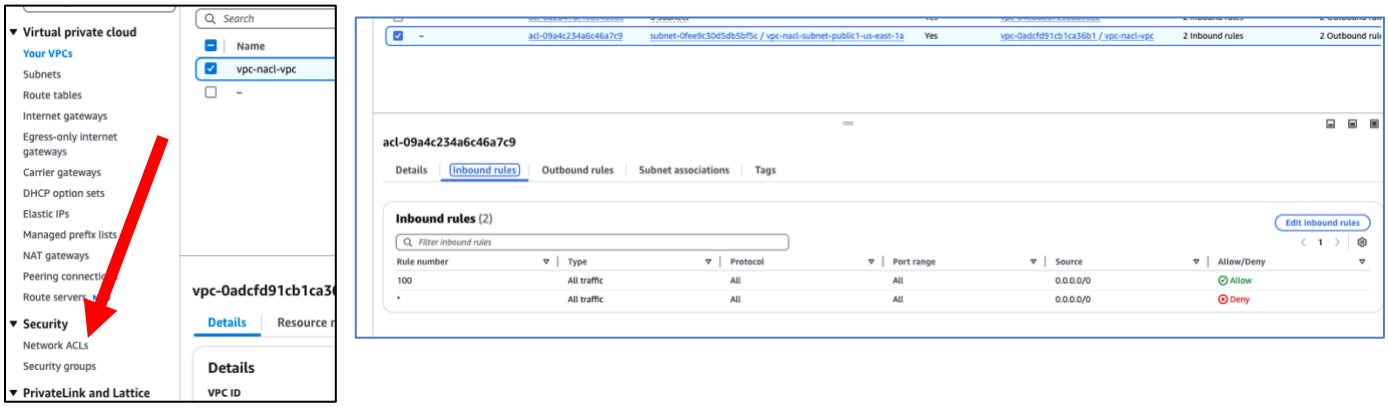


Una vez eliminada la regla:



Y podemos comprobar que el ping sigue funcionando:

Ahora crearemos la NACL en la VPC con la que estamos trabajando. Se crea justo desde el menú de VPC junto con las reglas de seguridad. En este paso ahora faltaría asociarlo a una subred o conjunto de subredes a controlar.



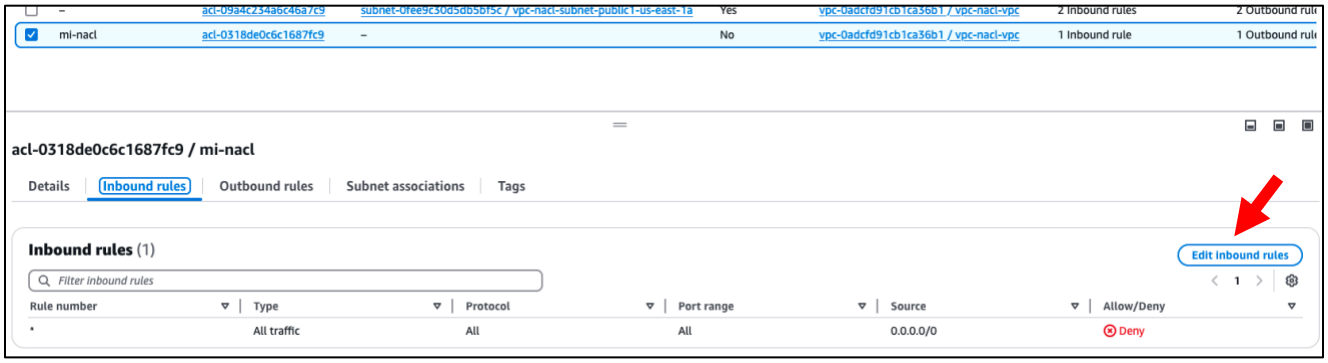
Por defecto podemos comprobar que ya existe una NACL asociada a la VPC, que permite todo el tráfico de entrada y salida. Desde el menú de ACL de red seleccionando la regla creada podremos modificar las reglas de entrada y salida.

Ahora crearemos el NACL en la VPC con la que estamos trabajando.

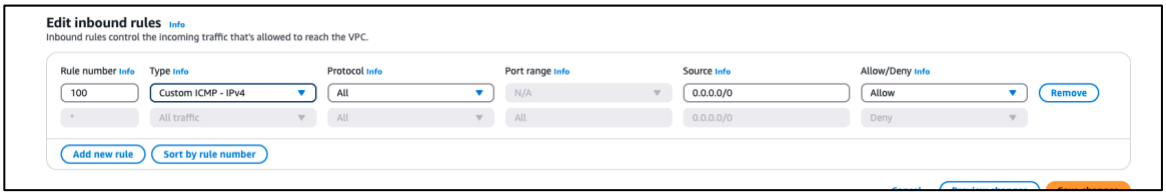
Y comprobamos que tiene asociada la subred pública desde la pestaña “subnet associations”

Desde el menú ACL de red, seleccionando la regla creada, podremos modificar las reglas de entrada y salida. Las pruebas serán las siguientes:

- Añadir regla de entrada ICMP. El ping NO funciona. Desde la regla NACL en la pestaña Inbound rules



Desde el botón “edit inbound rules” podremos añadir la regla nueva:



Y ahora ya nos aparece la nueva regla:

Cabe destacar que las reglas se evalúan con una prioridad ascendente y en cuanto la satisface ya no se comprueban las de menor prioridad.

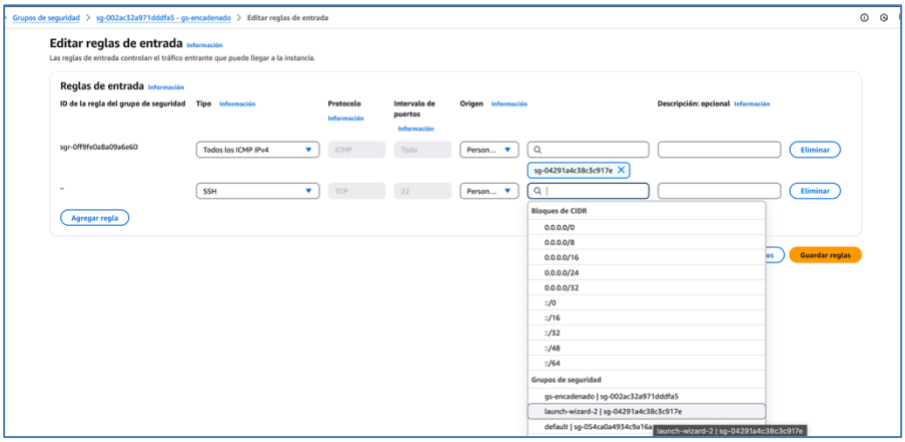
```
jorge@mjolnir Downloads % ping 54.87.133.32
PING 54.87.133.32 (54.87.133.32): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
```

- Ahora añadiremos la regla de salida ICMP en la regla NACL. El ping SI funciona.

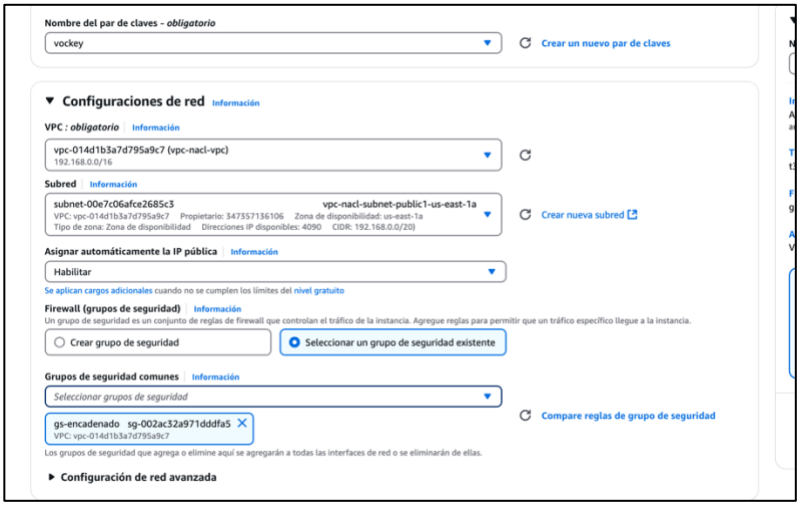
```
orge@mjolnir Downloads % ping 3.92.3.240
ING 3.92.3.240 (3.92.3.240): 56 data bytes
4 bytes from 3.92.3.240: icmp_seq=0 ttl=112 time=107.059 ms
4 bytes from 3.92.3.240: icmp_seq=1 ttl=112 time=115.187 ms
4 bytes from 3.92.3.240: icmp_seq=2 ttl=112 time=108.847 ms
4 bytes from 3.92.3.240: icmp_seq=3 ttl=112 time=105.259 ms
```

Reglas encadenadas

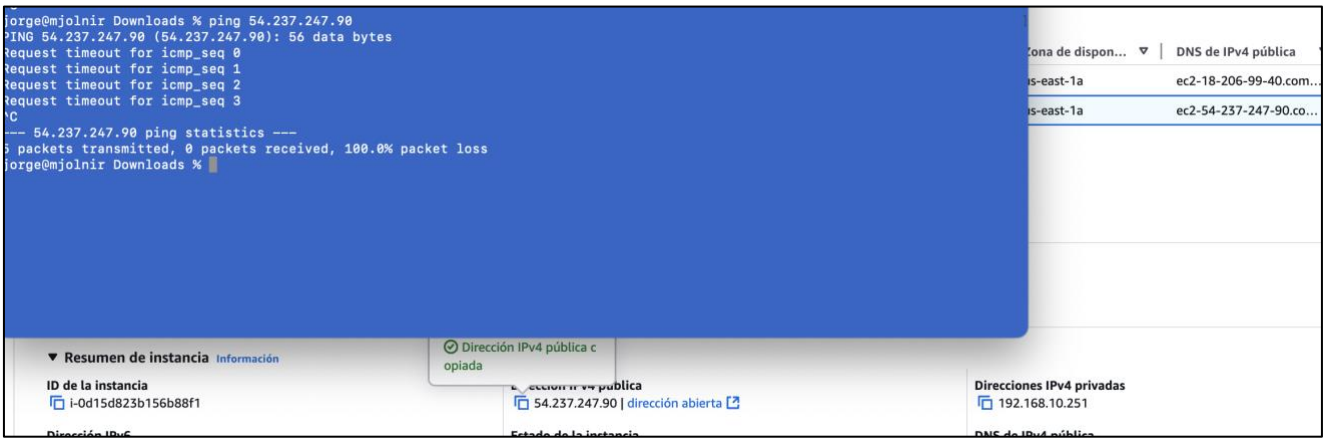
Ahora lo que vamos a hacer es crear un nuevo grupo de seguridad (con el nombre 'gs-encadenado' por ejemplo) y añadir una nueva regla de entrada, asignándole como origen el grupo de seguridad que tiene la instancia primera.



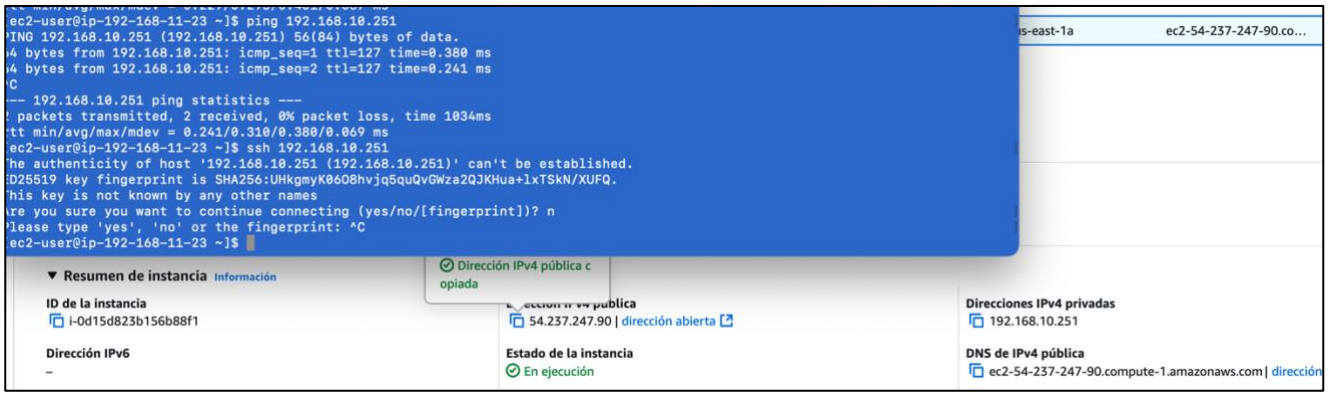
A la hora de crear la instancia ec2 le asignamos al nuevo grupo de seguridad 'encadenado', en lugar de a configurar es una nueva regla de seguridad y lo que le vamos a asignar como



Y cuando queramos por ejemplo hacer un ping desde fuera (desde el ordenador local, por ejemplo):



Vemos que no lo permite, pero sin embargo si lo realizamos desde dentro de la primera instancia creada, SÍ que lo permite:



Cabe recordar que para conectarse a la primera instancia tendremos que usar el parámetro -A en la conexión y cargar el certificado en memoria.

Tareas

- La tarea consiste en realizar un despliegue de una típica arquitectura de dos capas, donde en la parte pública tendremos un servidor web, y en la privada un servidor de base de datos:
  - Crea una VPC con dos subredes, una pública y otra privada. Para que desde la subred privada se pueda acceder al exterior, deberás utilizar un NAT Gateway.
  - En la subred pública lanza una instancia EC2 e instala un servidor web Apache, que será accesible desde cualquier equipo externo a la VPC por el puerto 80, utilizando tanto su nombre DNS como su dirección IP pública.
  - En la subred privada, lanza otra instancia EC2 e instala un servicio de MySQL.
  - Los grupos de seguridad asociados a las instancias deben permitir sólo el tráfico necesario, utilizando una regla encadenada en el caso del grupo de seguridad asociado a la instancia de base de datos, de manera que sólo acepte tráfico entrante del protocolo adecuado desde la instancia del servidor web
  - Conéctate con ssh a la instancia de la subred pública, y realiza una prueba de conexión al servidor de base de datos, utilizando para ello la aplicación del cliente de mysql que tendrás que instalar previamente

Adjunta a la tarea las siguientes capturas: mapa de la VPC, configuración de las reglas de entrada de los grupos de seguridad de las dos instancias, conexión al servidor Apache desde un navegador y conexión al servicio de base de datos desde la instancia del servidor web