Laboratorio de desafíos: Creación de un entorno de red de VPC para the Café

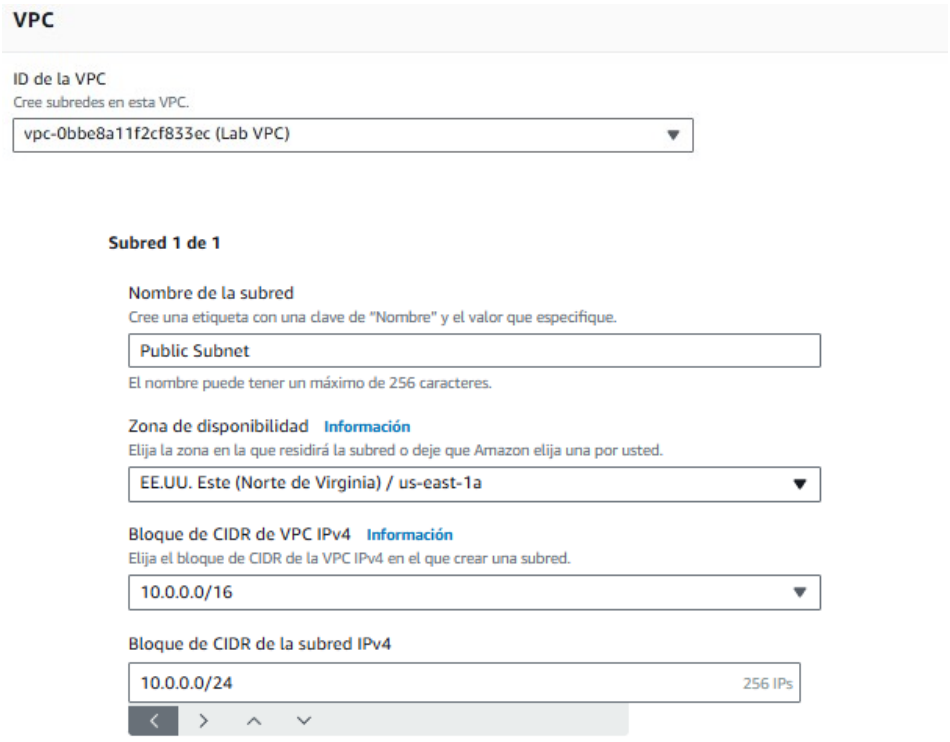
En este Laboratorio vamos a crear un entorno de redes en AWS e implementar capas de seguridad para proteger los recursos.

Una solicitud empresarial para la cafetería: crear una red de VPC que permita al personal de la cafetería administrar de forma remota y segura el servidor de aplicaciones web (Desafío n.º 1)

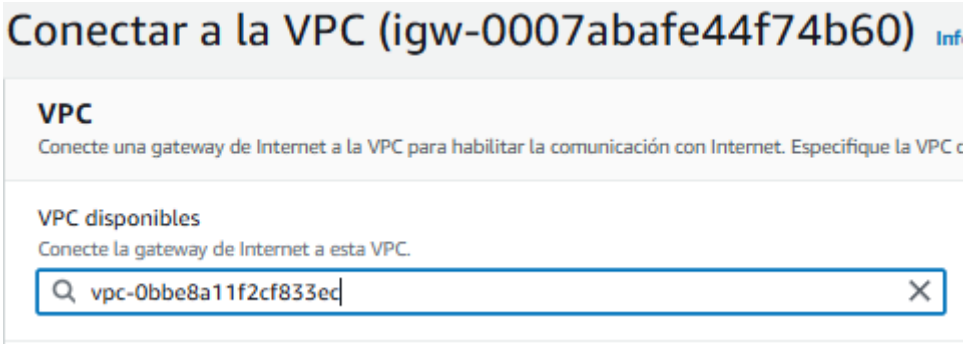
Tarea 1: creación de una subred pública

Abrimos la consola VPC y accedemos a la sección de subredes donde crearemos una con la VPC que nos ha creado el laboratorio.

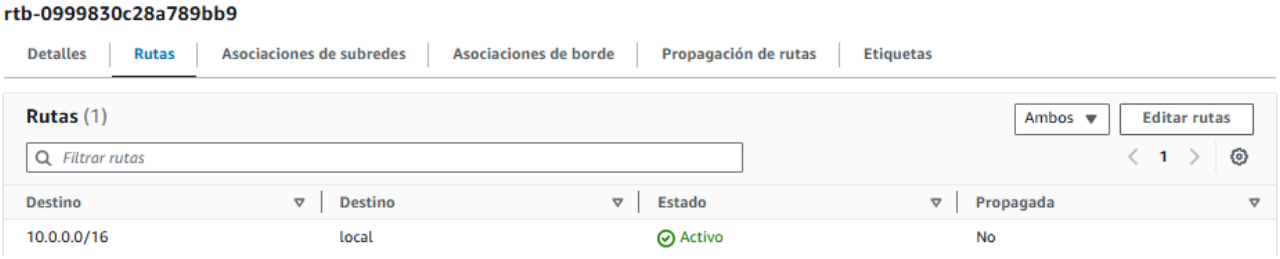
La subred debe tener las siguientes especificaciones:



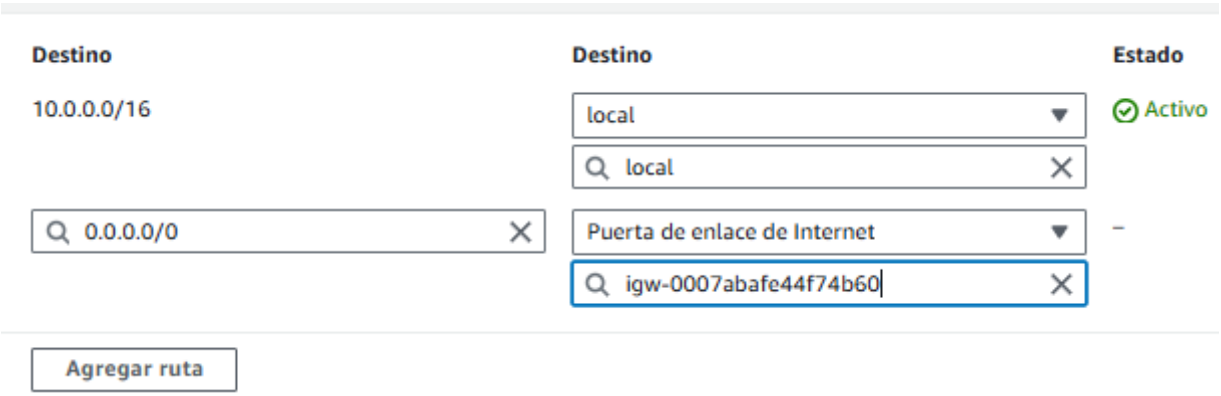
Una vez creada, debemos crear una puerta de enlace de internet y adjuntarla a nuestra VPC:



Por último vamos a editar nuestra tabla de enrutamiento y añadirle la ruta 0.0.0.0 :



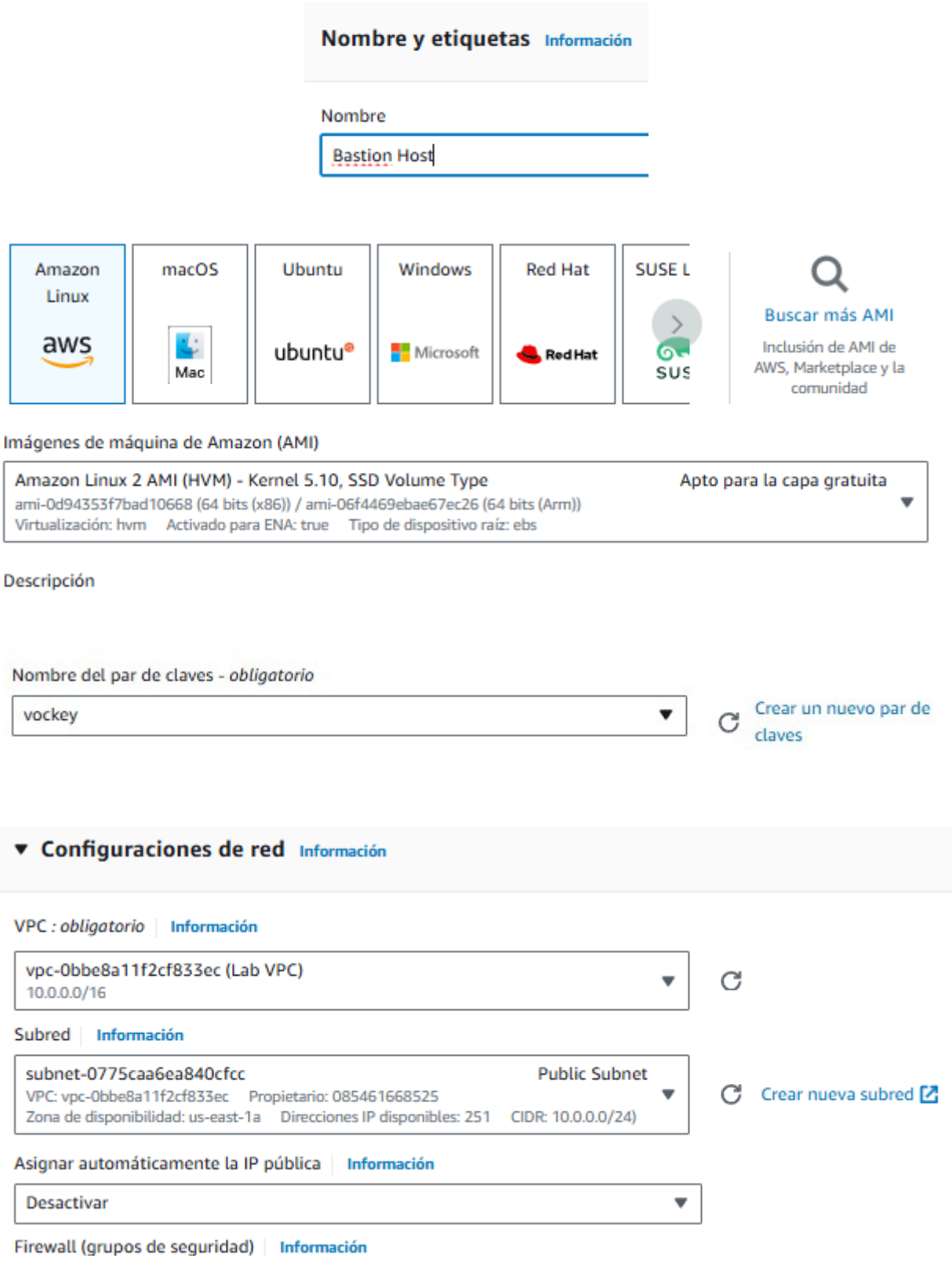
Esta es la tabla asociada a nuestra VPC



Agregamos esa ruta y le ponemos la puerta de enlace de internet que acabamos de crear. Una vez creada la asociamos a la subred pública.

Tarea 2: creación de un host bastión

Ahora crearemos un host de bastión en la subred pública que acabamos de hacer. Abrimos la consola EC2 y creamos una instancia con las siguientes especificaciones:



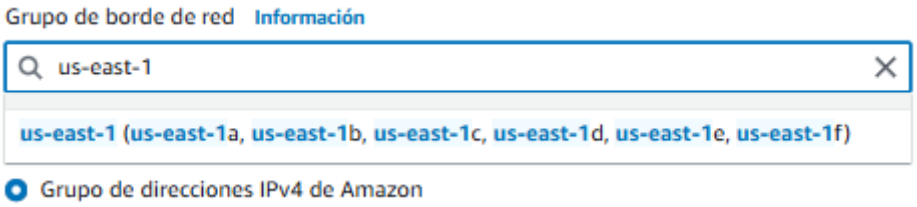
El resto lo dejamos por defecto.

Básicamente hemos creado una instancia con máquina principal Linux, que usa las claves de sesión Vodkey(por defecto), lo hemos metido en la Red Privada Virtual que venía creada por defecto, le hemos especificado que esté en la subred Pública y creado un grupo de seguridad que permita conexiones SSH desde mi IP.

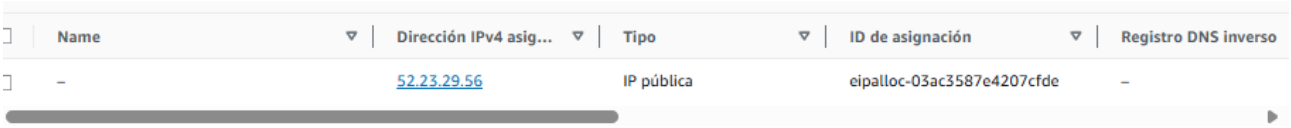
Tarea 3: asignación de una dirección IP elástica al host bastión

Una IP elástica es, básicamente, una IP estática que se puede asociar a una instancia EC2, y eso es lo que vamos a hacer ahora mismo, en la consola de EC2 nos vamos al panel izquierdo y buscamos IP elásticas:

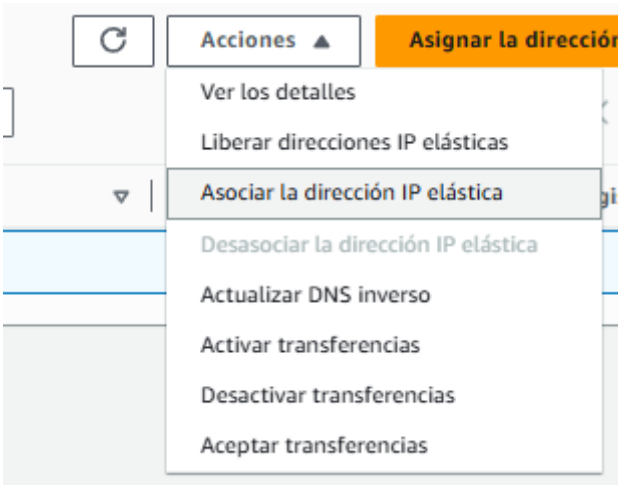
Aquí le damos a asignar la dirección IP elástica, y elegimos el grupo de borde de red, en este caso solo tenemos la zona en la que estamos trabajando:



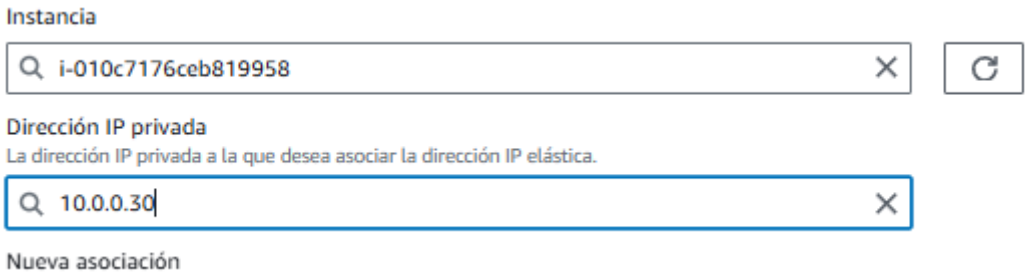
Le damos abajo a asignar y ya la tenemos creada, ahora solo queda asignarla a nuestra instancia:



Seleccionamos la IP elástica, pulsamos acciones y le damos a asociar la dirección IP:



Elegimos nuestra instancia y dejamos la IP privada que nos diga la página:



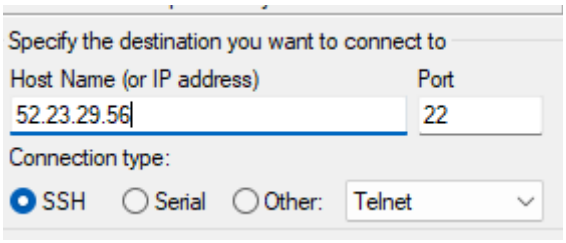
Si ahora nos vamos a nuestras instancias, vemos que la instancia tiene la misma IP pública que la elástica y la privada que tenía por defecto(dada por la propia subred):

Tarea 4: prueba de la conexión con el host bastión

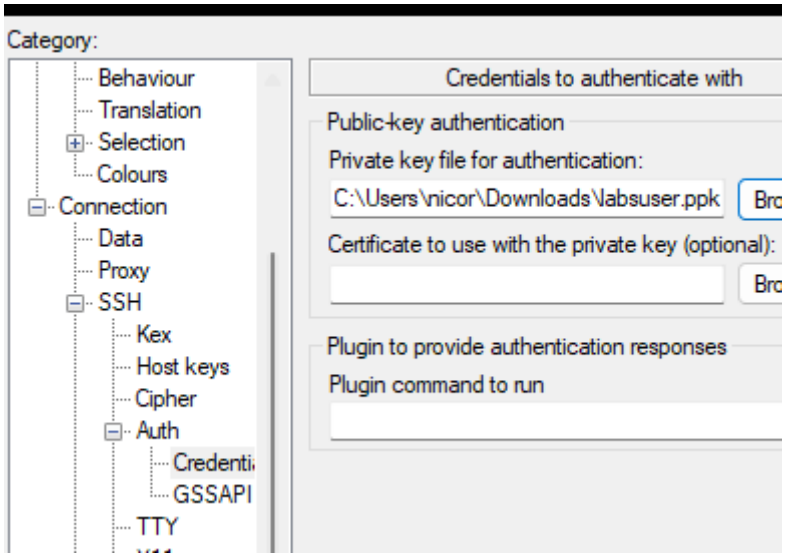
Vamos a probar la conexión a nuestro bastión que acabamos de crear utilizando la herramienta PuTTY, para ello necesitaremos las claves de acceso.pem de la par de claves Vodkey que podremos encontrar en los detalles del Laboratorio.

Configurar PuTTY es muy sencillo, solo tendremos que poner los siguientes datos:

La IP pública del host(IP elástica):



Y en esta ruta, poner el archivo de claves:



Connection/SSH/Auth/Credemtials

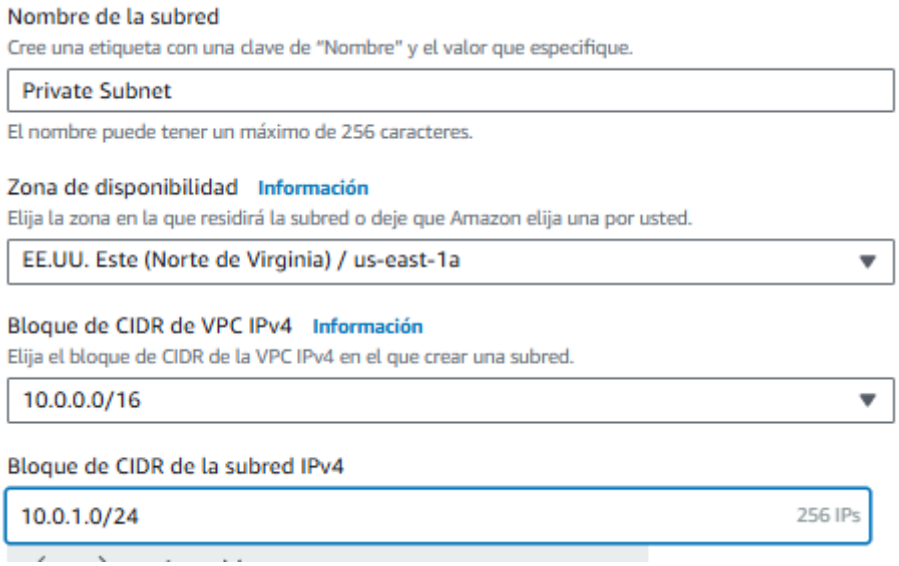
Le damos a conectar y listo:

Nos pedirá un usuario que también podemos poner uno por defecto en PuTTY

Tarea 5: creación de una subred privada

No todos los servicio pueden estar en subredes publicas debido a la poca seguridad de estas, servicios como bases de datos es mejor que se encuentren a salvo dentro de las subredes privada.

Vamos a crear una nueva igual que la tarea 1 pero vamos a hacerla privada.

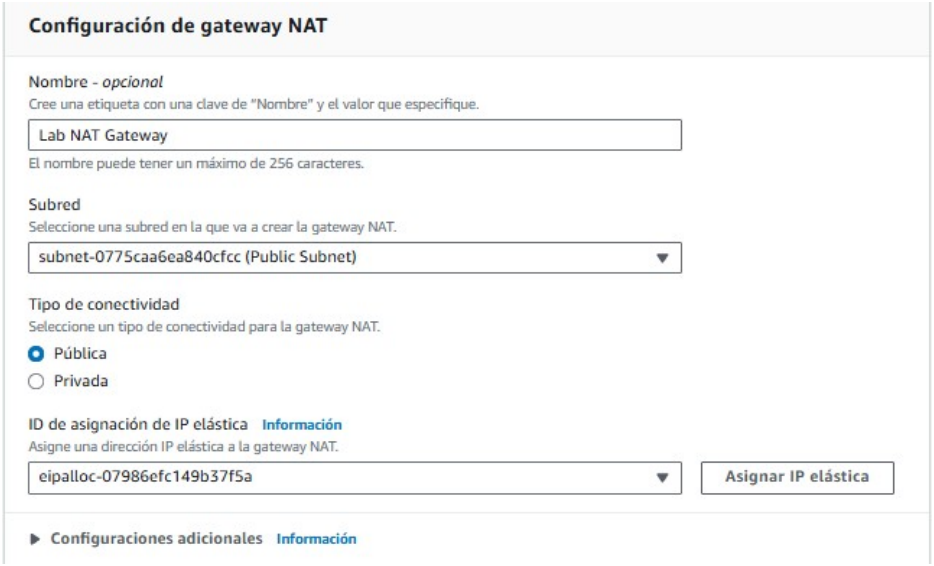


Ponemos esta configuración y le damos a crear subred.

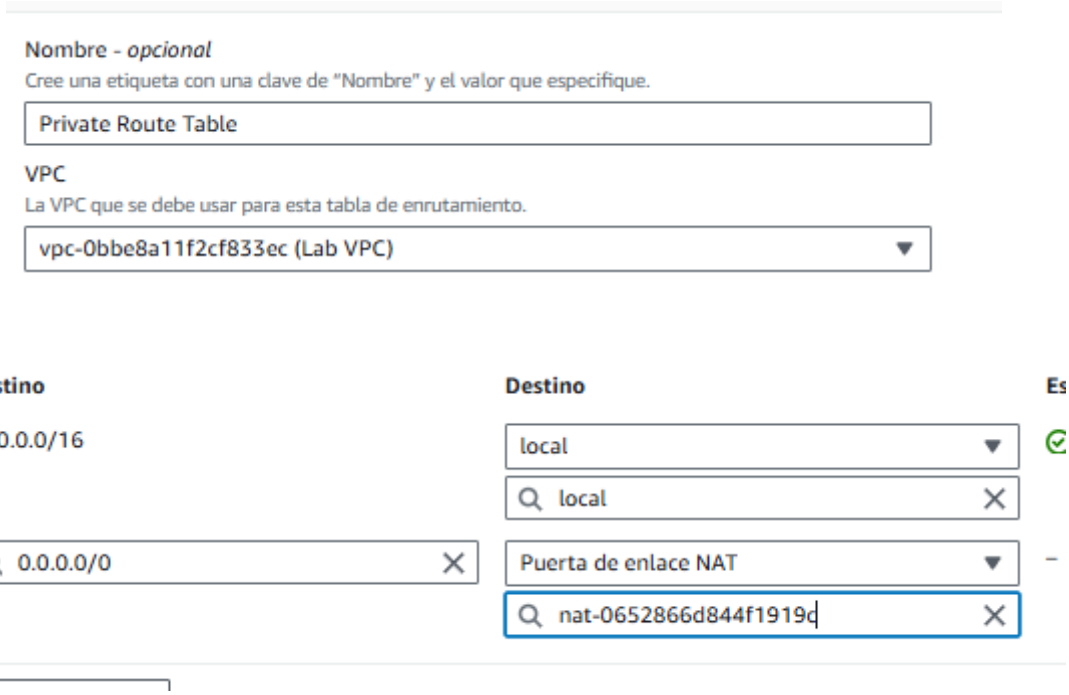
Tarea 6: creación de una puerta de enlace de NAT

Vamos a crear una puerta de enlace para que los elementos de la subred privada puedan conectarse a internet.

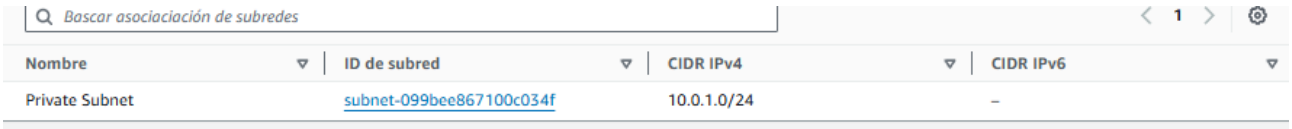
Le damos a crear gateway NAT y ponemos lo siguiente:



Ahora necesitaremos crear una nueva tabla de rutas, la crearemos con las siguientes especificaciones:

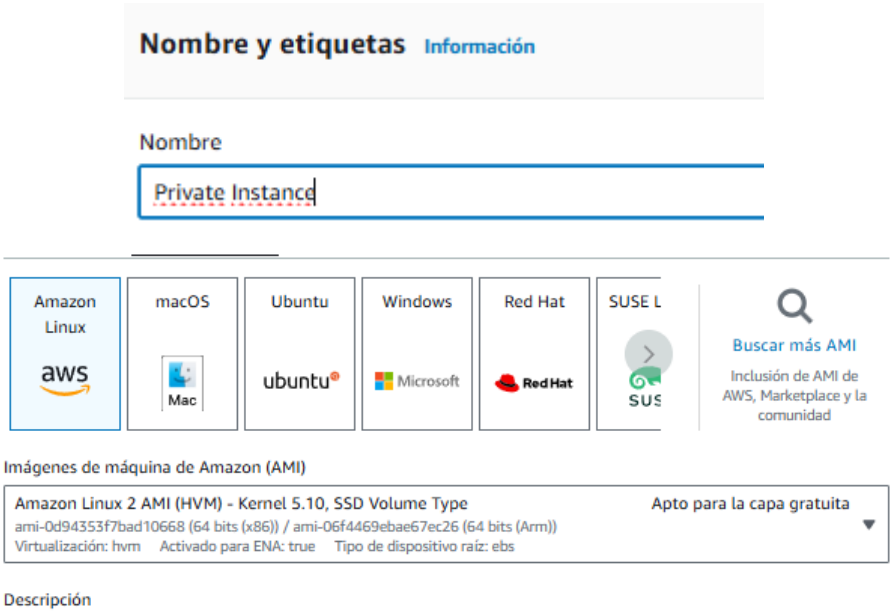


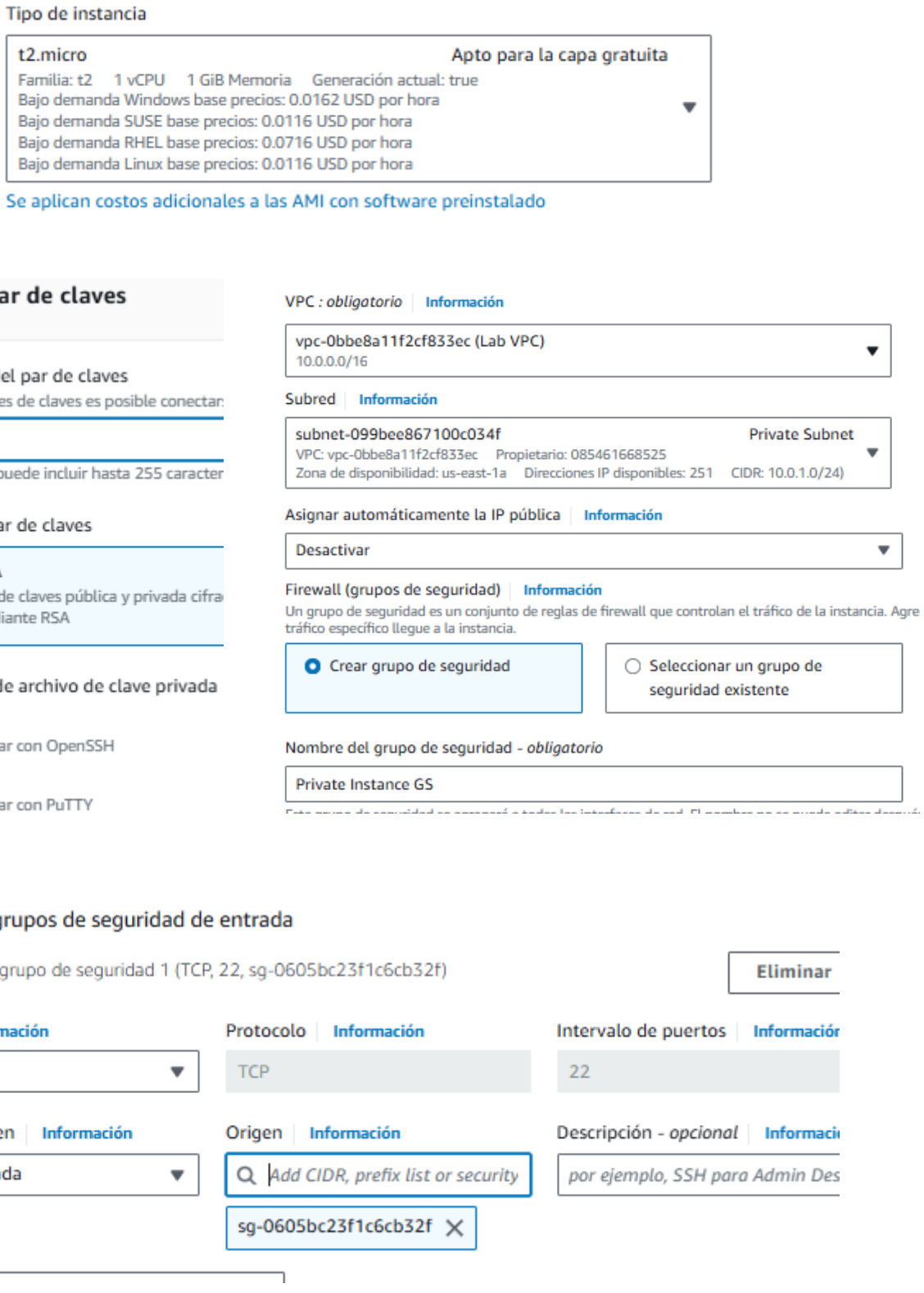
Y por ultimo adjuntamos la subred privada a la nueva tabla de enrutamiento.



Tarea 7: creación de una instancia de Amazon EC2 en la subred privada

Vamos a crear una nueva instancia con las siguientes especificaciones:

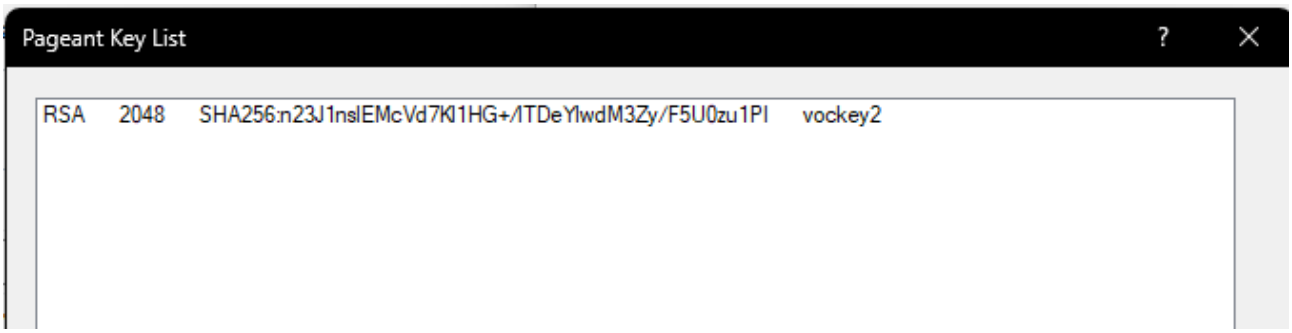




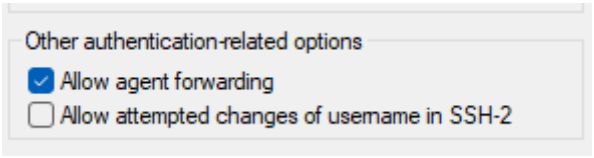
El resto lo dejamos por defecto y le damos a lanzar.

Tarea 8: configuración del cliente SSH para acceso directo de SSH

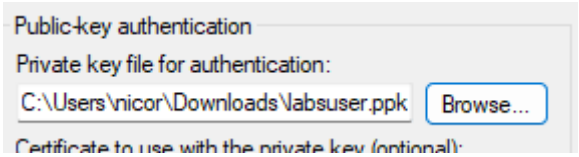
Para esta tarea necesitaremos instalar Pageant y dejarlo abierto en segundo plano. Lo abrimos desde la flechita de Windows y le damos a añadir clave(Add Key) y seleccionamos la clave que nos descargamos antes vodkey2.ppk.



Agregamos también la clave anterior labuser.ppk y cerramos Pegeant. Ahora abrimos PuTTY y nos vamos a **Connection > (Conexión) SSH > Auth** (Autenticación):



Ponemos esto así, en credenciales, ponemos la clave labuser.ppk:

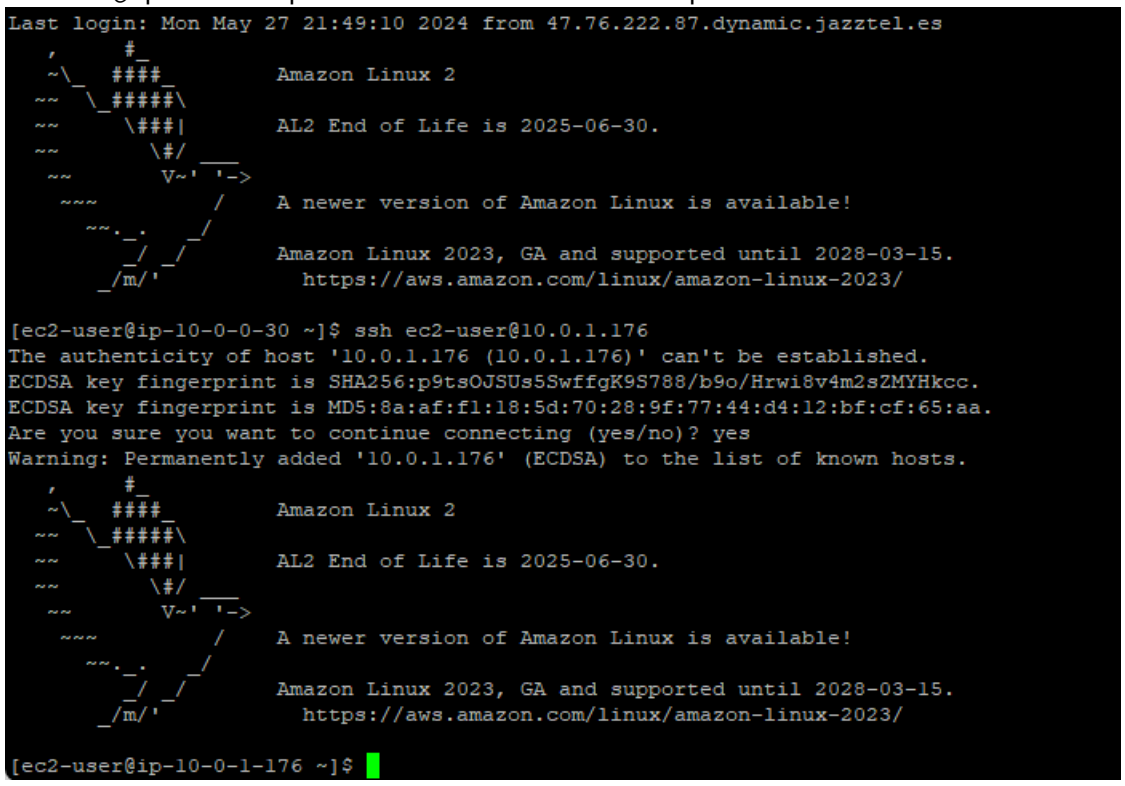


Debemos poner la IP de la instancia a la que nos queremos conectar(Bastion Host) y conectarnos con PuTTY.

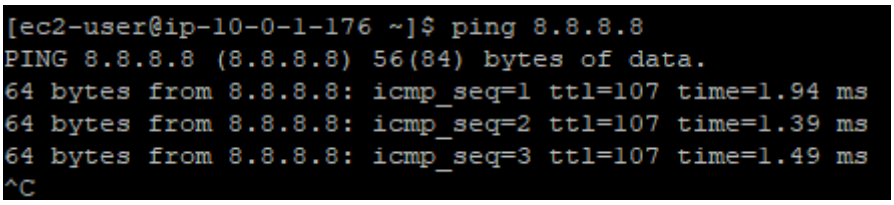
Tarea 9: prueba de la conexión SSH desde el host bastión

Vamos a conectarnos a la instancia privada a través de ssh, para ello debemos poner el siguiente comando:

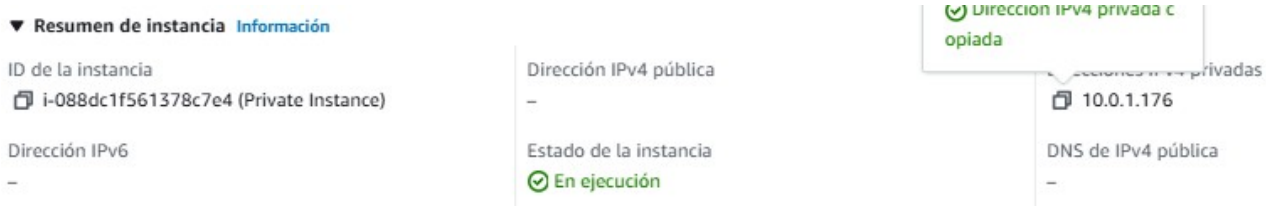
```
ssh ec2-user@<private-ip-address-of-instance-in-private-subnet>
```



Estando conectados a la instancia privada vamos a intentar hacer un ping a google:



Vemos que tiene internet. Si nos fijamos, la instancia privada no tiene IP pública:

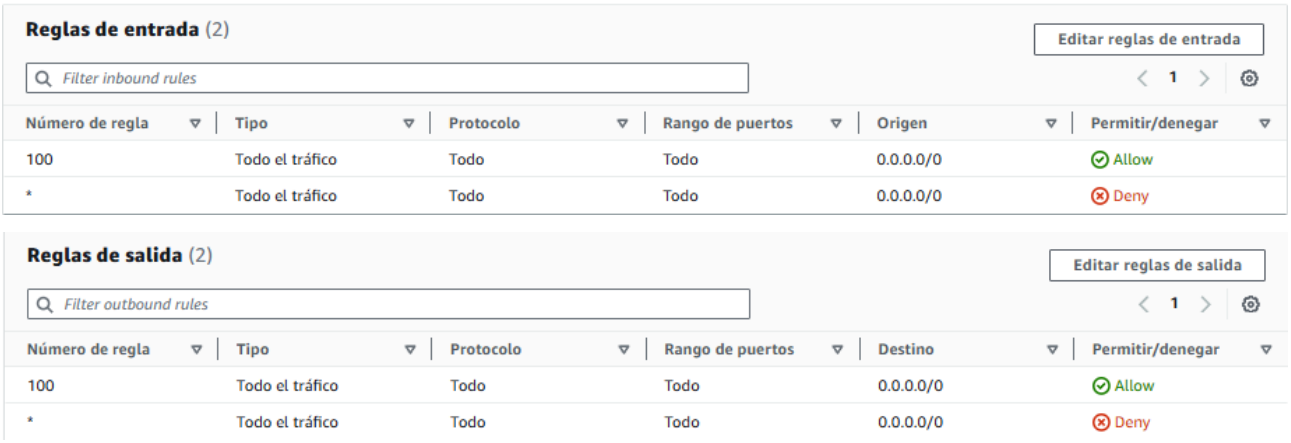


Nuevo requisito empresarial: Mejora de la capa de seguridad para recursos privados (Desafío n.° 2)

Tarea 10: creación de una ACL de red

Las ACL de red proporcionan una capa adicional de protección. Vamos a crear una ACL de red personalizada para controlar el tráfico hacia y desde la *Private Subnet*.

Nos vamos a la consola VPC y miramos la ACL predeterminada:



Reglas de entrada (2)

Editar reglas de entrada

Filter inbound rules

1

Número de regla	Tipo	Protocolo	Rango de puertos	Origen	Permitir/denegar
100	Todo el tráfico	Todo	Todo	0.0.0.0/0	Allow
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny

Reglas de salida (2)

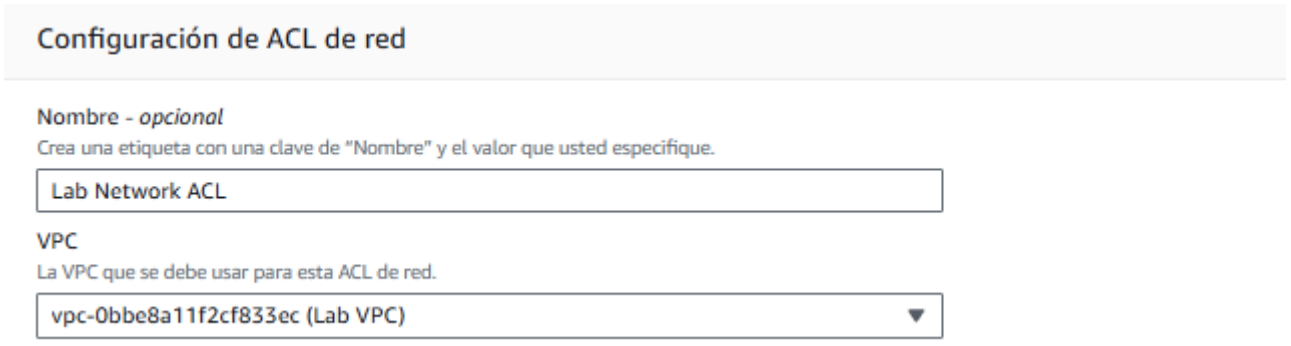
Editar reglas de salida

Filter outbound rules

1

Número de regla	Tipo	Protocolo	Rango de puertos	Destino	Permitir/denegar
100	Todo el tráfico	Todo	Todo	0.0.0.0/0	Allow
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny

Vemos que la configuración por defecto deniega todo el tráfico.Vamos a crear una personalizada con las siguientes especificaciones:



Configuración de ACL de red

Nombre - *opcional*

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Lab Network ACL

VPC

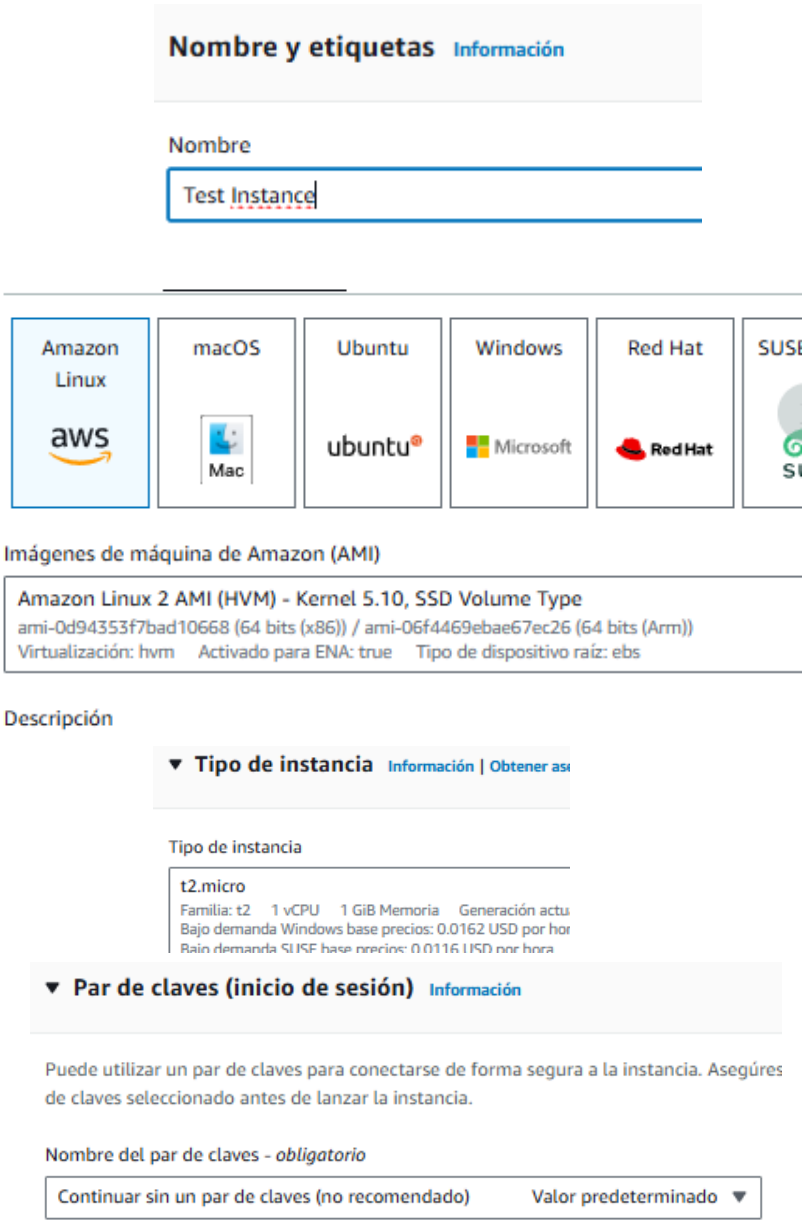
La VPC que se debe usar para esta ACL de red.

vpc-0bbe8a11f2cf833ec (Lab VPC)

Creo que no lo he entendido muy bien, ya permite el tráfico por defecto…

Tarea 11: prueba de la ACL de red personalizada

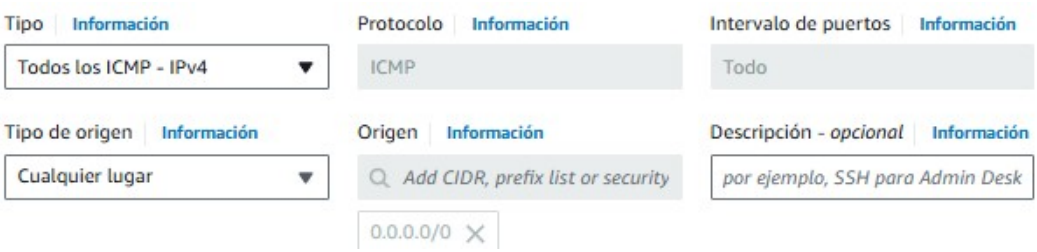
Vamos a crear una instancia EC2 en la subred publica con las siguientes especificaciones:



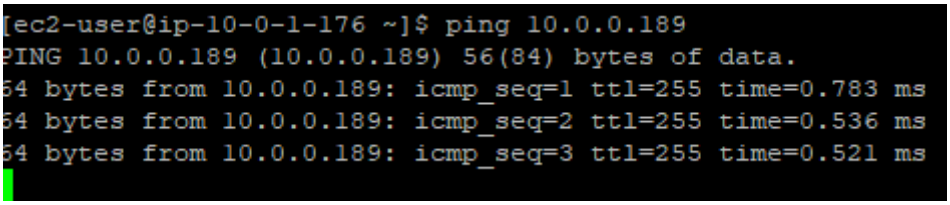
No nos vamos a conectar

Lo ponemos en la VPC nuestra y en la subred publica.

Y creamos un GS que permita ICMP desde todos lados:

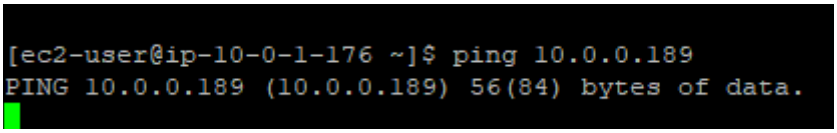


Creamos la instancia y probamos a hacer un ping a la nueva máquina:



Vamos a probar a denegar toda conexión ICMP desde la ACL a la ip de la máquina anfitriona.

Añadiendo esa regla ya no debería dejarnos hacer ping desde la máquina:



Vemos que ya no hace ping, es importante el orden de permitir/denegar acceso. Hasta aquí el Laboratorio, vamos con las preguntas:

¿Para qué sirve la puerta de enlace de Internet en la subred pública?

- Permite que la subred pública tenga acceso a internet

¿Qué permite a la instancia de la subred privada conectarse a Internet para poder descargar actualizaciones?

- El gateway NAT

¿Se puede acceder a la instancia en la subred privada directamente desde Internet?

- No, no tiene IP pública

¿Por qué se utilizan dos pares de claves diferentes para acceder a la instancia privada y al host bastión?

- Usar 2 pares de claves ayudan al factor riesgo de la instancia Bastion Host

¿Puede el host bastión utilizar ping y obtener una respuesta de la instancia en la subred privada?

- No, no puede

¿Qué reglas de grupo de seguridad permiten a la instancia de EC2 privada recibir el tráfico de retorno cuando hace ping a la instancia de prueba?

- Las de salida de la privada y las de entrada de test