Configurar Instancia NAT

AWS

Yeray Gutiérrez Mullor

Contenido

Instancia NAT: 2

Grupos de Seguridad: 2

Grupo de Seguridad de la Instancia NAT: 2

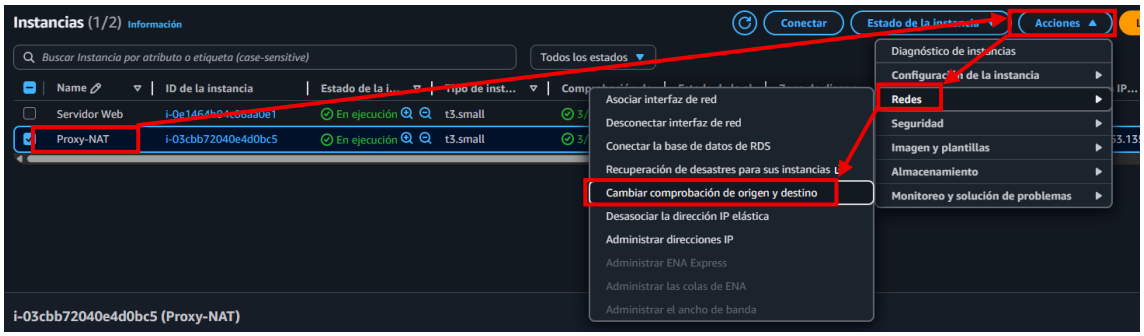
Grupo de Seguridad Privado: 3

ACL de Red: 4

Comandos en la Instancia NAT: 4

Instancia NAT:

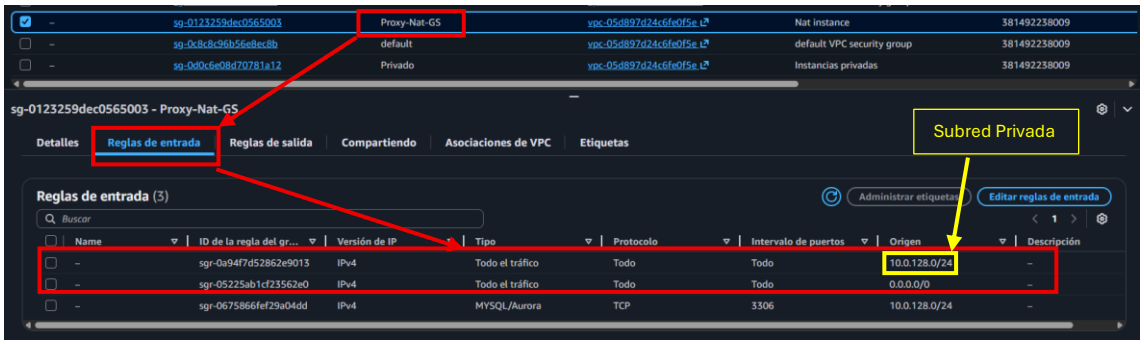
Desactivar la comprobación de origen y destino



Grupos de Seguridad:

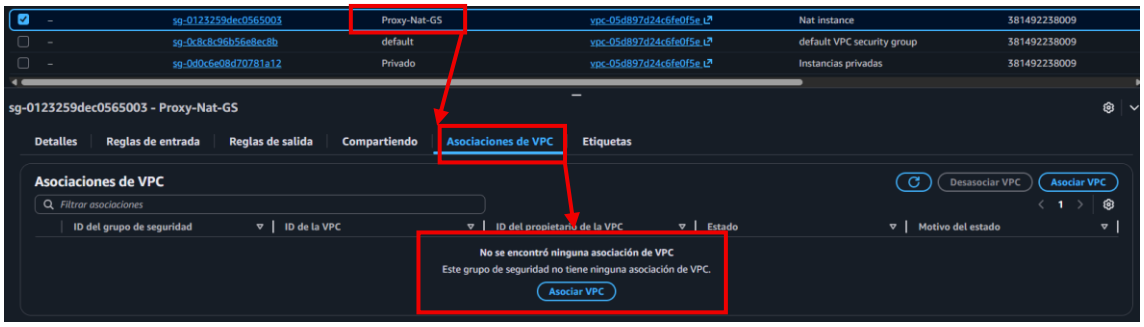
Grupo de Seguridad de la Instancia NAT:

Reglas de entrada para el grupo de seguridad del Bastión (Instancia NAT)



Reglas de salida para el grupo de seguridad del Bastión (Instancia NAT)

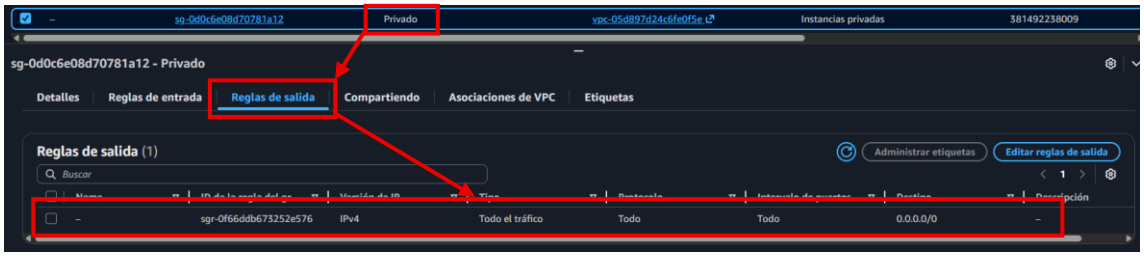
En asociaciones de VPC no debe haber nada



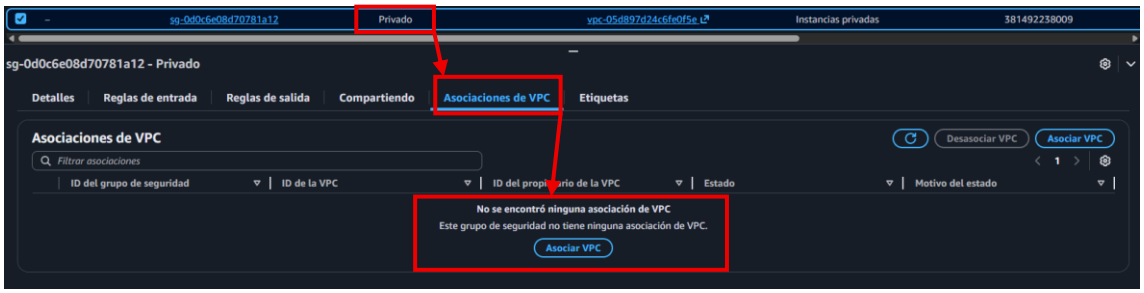
Grupo de Seguridad Privado:

Reglas de entrada del grupo de seguridad de la subred privada (Servidores Web)

Reglas de salida del grupo de seguridad de la subred privada (Servidores Web)

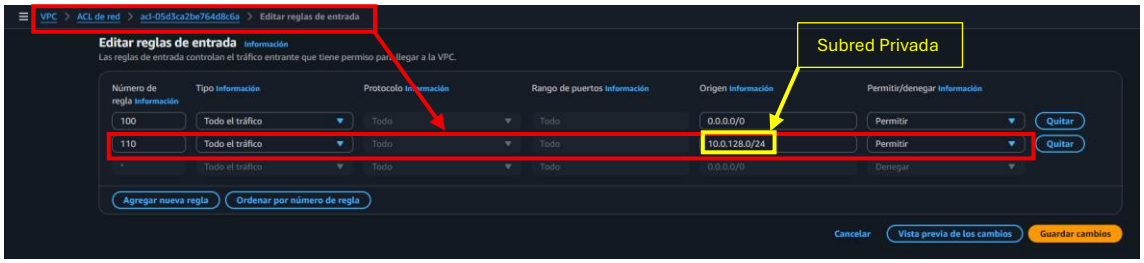


En asociaciones de VPC no debe haber nada

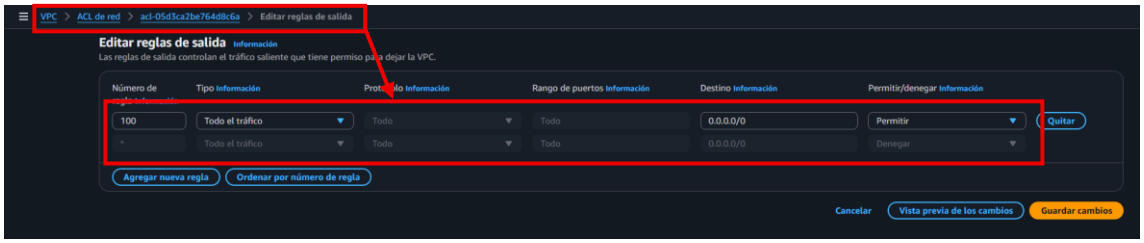


ACL de Red:

En el ACL de red de la vpc creada se debe añadir la regla 110 en reglas de entrada



En las reglas de salida no hay que añadir nada



Comandos en la Instancia NAT:

Actualizar repositorios de la instancia

sudo apt update

sudo apt upgrade

Comprobar el reenvio de paquetes IPv4 entre interfaces de red

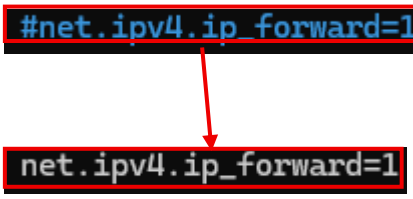
sysctl net.ipv4.ip_forward

Habilita el reenvío de paquetes IPv4 en el sistema, permitiendo que actúe como router entre redes

sudo sysctl -w net.ipv4.ip_forward=1

Abre el archivo /etc/sysctl.conf para descomentar la línea net.ipv4.ip_fordward=1

sudo nano /etc/sysctl.conf



Instala iptables-persistent, que permite guardar y restaurar automáticamente las reglas de iptables al iniciar el sistema

sudo apt install iptables-persistent

Guarda las reglas actuales de iptables/netfilter para que se restauren automáticamente al reiniciar el sistema.

sudo netfilter-persistent save

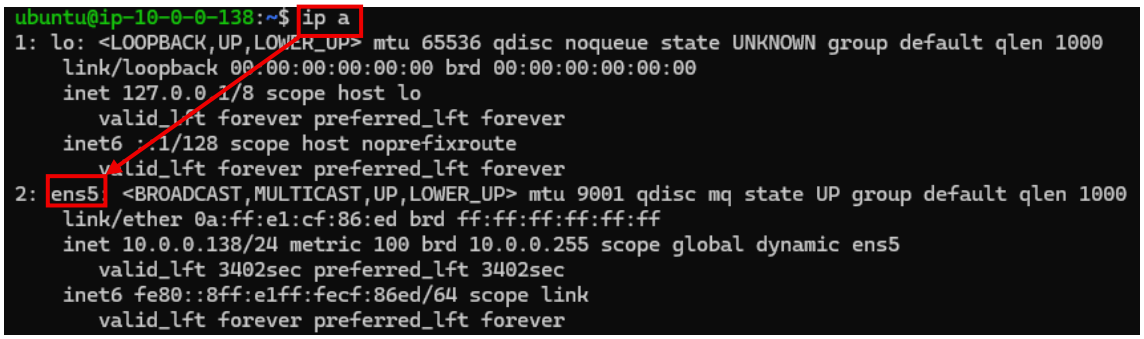
Muestra de forma detallada las reglas de la tabla NAT de iptables, ahí debe aparecer la tarjeta de red del equipo

sudo iptables -t nat -L -n -v

```
ubuntu@ip-10-0-0-138:~$ sudo iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 804 packets, 48744 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 585 packets, 30268 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 468 packets, 34462 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 17 packets, 1362 bytes)
 pkts bytes target     prot opt in     out     source               destination
  665 49220 MASQUERADE  0    --  *      ens5    0.0.0.0/0            0.0.0.0/0
```

Si no aparece, comprobar la tarjeta de red

ip a



Luego introducir este comando cambiando ens5 por el ID de la tarjeta

sudo iptables -t nat -A POSTROUTING -o ens5 -j MASQUERADE

Añadir permanentemente la opción net.ipv4.ip_forward=1 a /etc/sysctl.conf para habilitar el reenvío IPv4 al arrancar el sistema.

echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf

Muestra el valor actual de ip_forward en el kernel:

- 0 → deshabilitado (no se reenvían paquetes IPv4)
- 1 → habilitado (el sistema puede reenviar paquetes IPv4)

cat /proc/sys/net/ipv4/ip_forward