

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

The screenshot shows the AWS EC2 Instances page. A context menu is open over an instance named "Proxy-NAT". The "Redes" (Network) option is selected. This leads to a modal dialog titled "Cambiar comprobación de origen y destino" (Change source/destination check). Inside the dialog, there is a section for "Comprobación de origen/destino" (Source/Destination check) with a checkbox labeled "Detener" (Stop) which is checked. At the bottom right of the dialog is a yellow "Guardar" (Save) button.

Grupos de Seguridad:

Grupo de Seguridad de la Instancia NAT:

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

sg-0123259dec0565003 - Proxy-Nat-GS

Reglas de entrada (3)

Name	ID de la regla del grupo	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
sgr-094f7d5286e9013	IPv4	Todo el tráfico	Todo	Todo		10.0.128.0/24	
sgr-05225ab1cf23562e0	IPv4	Todo el tráfico	Todo	Todo		0.0.0.0/0	
sgr-0675866fe2f29a04dd	IPv4	MYSQL/Aurora	TCP	3306	10.0.128.0/24		

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

sg-0123259dec0565003 - Proxy-Nat-GS

Reglas de salida (1)

Name	ID de la regla del grupo	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Destino	Descripción
sgr-06114a708fd0b114	IPv4	Todo el tráfico	Todo	Todo		0.0.0.0/0	

En asociaciones de VPC no debe haber nada

sg-0123259dec0565003 - Proxy-Nat-GS

Asociaciones de VPC

No se encontró ninguna asociación de VPC.
Este grupo de seguridad no tiene ninguna asociación de VPC.

Grupo de Seguridad Privado:

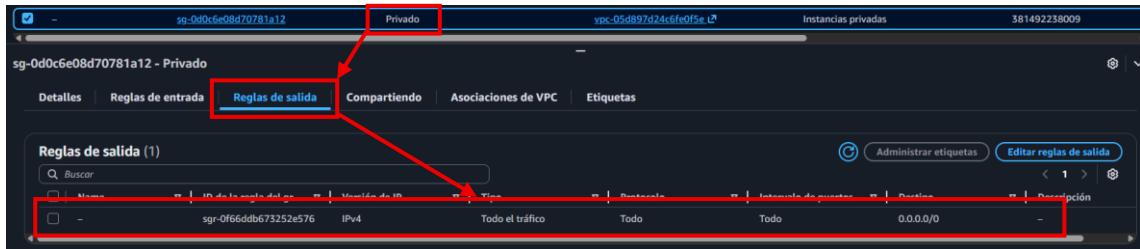
Reglas de entrada del grupo de seguridad de la subred privada (Servidores Web)

sg-0d0c6e08d70781a12 - Privado

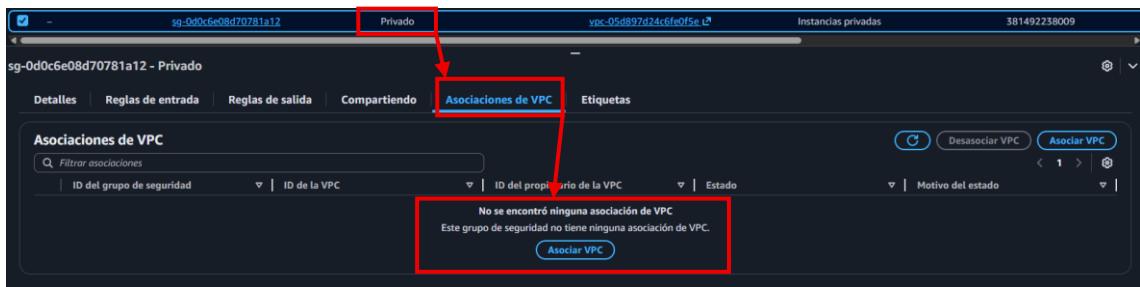
Reglas de entrada (2)

Name	ID de la regla del grupo	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
sgr-0145b9d641a4159ea	IPv4	Todo el tráfico	Todo	Todo		10.0.0.136/32	
sgr-0854b426400ccdf7fc	IPv4	MYSQL/Aurora	TCP	3306	10.0.128.0/24		

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

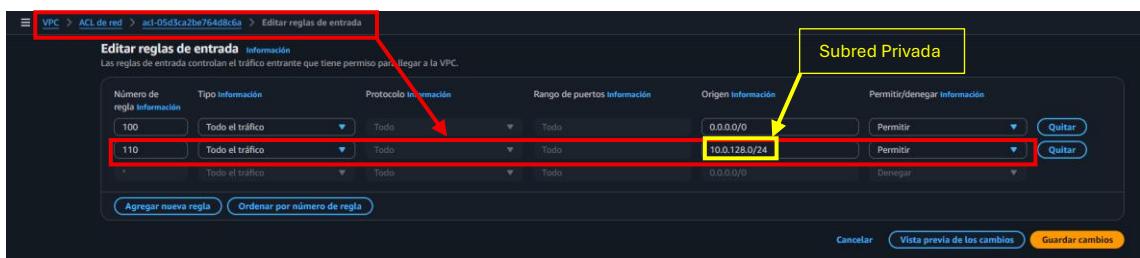


En asociaciones de VPC no debe haber nada

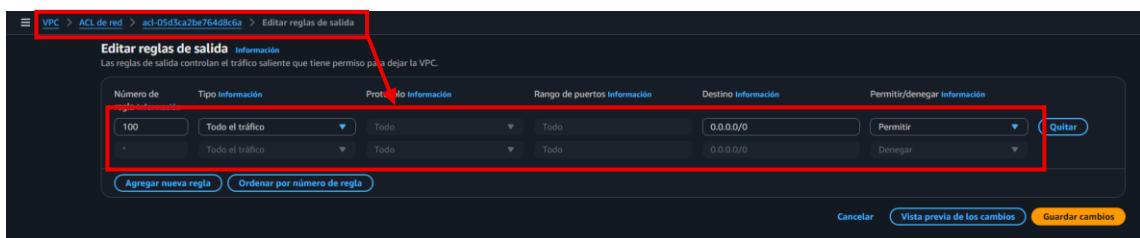


ACL de Red:

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 reenvío 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_forward=1

sudo nano /etc/sysctl.conf

#net.ipv4.ip_forward=1



net.ipv4.ip_forward=1

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

```
ubuntu@ip-10-0-0-138:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:ff:e1:cf:86:ed brd ff:ff:ff:ff:ff:ff
        inet 10.0.0.138/24 metric 100 brd 10.0.0.255 scope global dynamic ens5
            valid_lft 3402sec preferred_lft 3402sec
        inet6 fe80::8ff:e1ff:fecf:86ed/64 scope link
            valid_lft forever preferred_lft forever
```

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
```