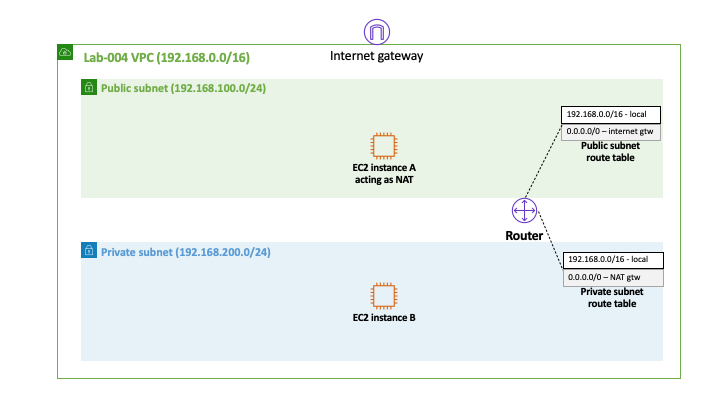
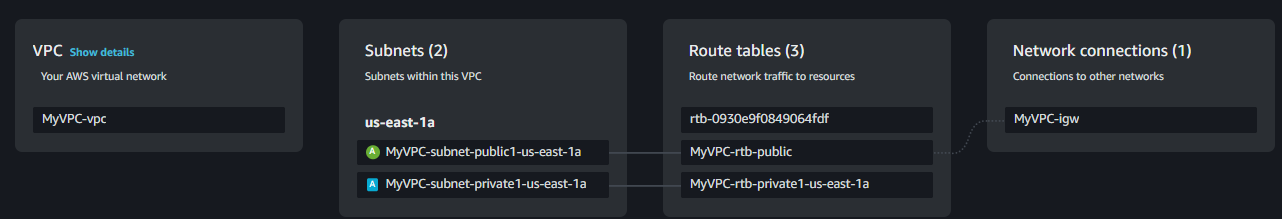
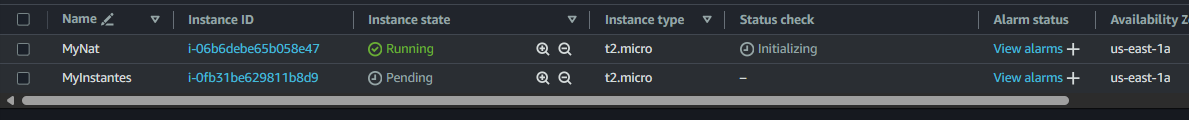
Configurar un Nat Instances



Crear las VPC, una publica y un privada.



Crear una instancia que va a trabajar como un NAT.



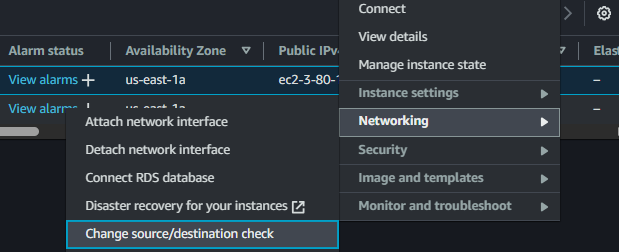
Para MyNat es necesario instalar los siguientes paquetes:

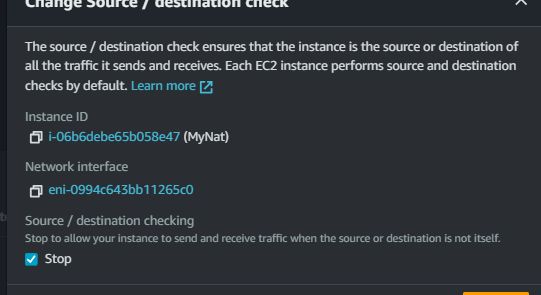
sudo yum install iptables-services -y

sudo systemctl enable iptables

sudo systemctl start iptables

Marca el siguiente check:





Nota: permite enviar y recibir trafico cuando la fuente no es la propia instancia.

Configurar aplicación:

Haga lo siguiente en la instancia para habilitar el reenvío de IP de forma que persista después del reinicio:

1. Mediante un editor de texto, como nano o vim, cree el siguiente archivo de configuración: /etc/sysctl.d/custom-ip-forwarding.conf.
2. Agregue la siguiente línea al archivo de configuración.

net.ipv4.ip\_forward=1

Guarde el archivo de configuración y salga del editor de texto.

Ejecute el siguiente comando para aplicar el archivo de configuración.

1. sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf

Ejecute el siguiente comando en la instancia y anote el nombre de la interfaz de red principal. Necesitará esta información para el siguiente paso.

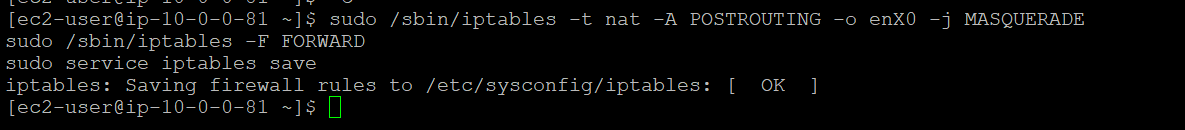
1. netstat -i

Ejecute los comandos siguientes en la instancia para configurar NAT. Si la interfaz de red principal no es eth0, reemplace eth0 por la interfaz de red principal que anotó en el paso anterior.

sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo /sbin/iptables -F FORWARD

sudo service iptables sabe



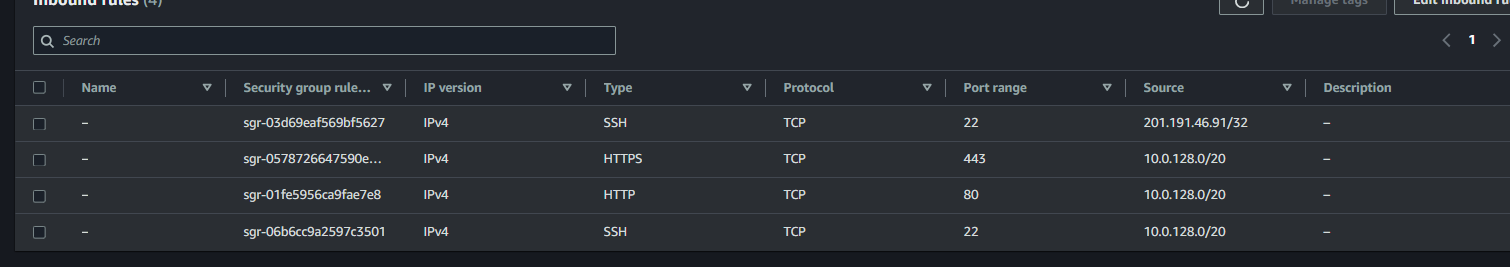
Security Group para el NAt Instances.

Agregue reglas para el tráfico entrante en Reglas entrantes de la siguiente manera:

Seleccione Agregar regla. Elija HTTP para Tipo e ingrese el rango de direcciones IP de su subred privada para Fuente.

Seleccione Agregar regla. Elija HTTPS para Tipo e ingrese el rango de direcciones IP de su subred privada para Fuente.

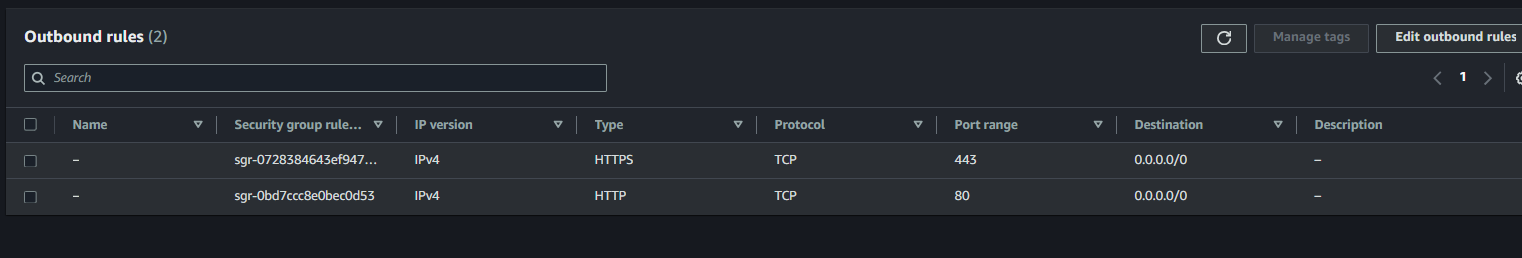
Seleccione Agregar regla. Elija SSH para Tipo e ingrese el rango de direcciones IP de su red para Origen.



Agregue reglas para el tráfico saliente en Reglas salientes de la siguiente manera:

Seleccione Agregar regla. Elija HTTP como Tipo e introduzca 0.0.0.0/0 como Destino.

Seleccione Agregar regla. Elija HTTPS como Tipo e introduzca 0.0.0.0/0 como Destino.



Elija Create Security Group (Crear grupo de seguridad).

Configurar route tables.

Que todo salga por el Nat Instances.

