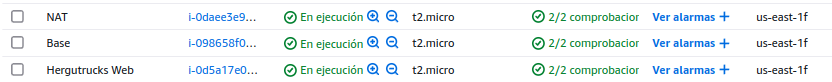
# **VPC**

La **instancia** de mi aplicación se llama **Hergutrucks Web**, y fue creada a partir de una imagen **AMI** de la instancia. Esto nos permite tener una versión preconfigurada de nuestra aplicación sobre la cual podremos realizar despliegues y configuraciones específicas.



### **Composición de la infraestructura**

1. **Hergutrucks Web (Aplicación)**:
   * Esta es la instancia principal que contiene la aplicación web o servicio que queremos ofrecer. Aquí se ejecuta el código que maneja la lógica de negocio de la aplicación. Puede estar configurada para interactuar con una base de datos, realizar consultas, y proveer una interfaz de usuario, entre otras tareas.
2. **Base (Base de Datos)**:
   * La base de datos que se utiliza para almacenar la información relacionada con la aplicación. En este caso, **PostgreSQL** es el sistema de gestión de bases de datos relacional que se utiliza para guardar todos los datos necesarios. Esta instancia está separada de la aplicación para garantizar la escalabilidad, seguridad y eficiencia.
3. **NAT (Instancia de red para acceso a Internet)**:
   * La instancia **NAT** actúa como un gateway, proporcionando acceso a Internet a las instancias que se encuentran en una **subred privada**. En nuestro caso, **PostgreSQL** necesita acceder a Internet (por ejemplo, para actualizaciones de paquetes o para realizar conexiones externas), y para esto utilizamos **NAT**. Sin esta instancia, las instancias privadas no podrían comunicarse con servicios externos.

### **Configuraciones Importantes**

### **Regla de IPTables para NAT**

En la instancia **NAT**, es necesario configurar una regla en **iptables** para permitir que actúe correctamente como un **NAT (Network Address Translation)**. Esto se logra con el siguiente comando:

iptables -t nat -A POSTROUTING -o INTERFAZ -j MASQUERADE

Esta regla establece que todo el tráfico que sale de la instancia **NAT** sea "enmascarado", es decir, se reemplaza la dirección IP privada con la IP pública de la instancia **NAT** para poder ser enrutado a través de Internet.

### **Persistencia de reglas de IPTables**

Para asegurar que las reglas de **iptables** persistan incluso después de reiniciar el sistema, instalamos el paquete **iptables-persistent** y ejecutamos los siguientes comandos:

sudo su

iptables-save > /etc/iptables/rules.v4

Esto guarda las reglas de **iptables** en un archivo de configuración que se recargará automáticamente al reiniciar la instancia.

### **Activar el reenvío de paquetes (IP Forwarding)**

Para permitir que las instancias en la **subred privada** puedan enviar tráfico a través de la instancia **NAT**, necesitamos activar el reenvío de paquetes (IP forwarding). Esto se hace editando el archivo de configuración **/etc/sysctl.conf** y descomentando la línea que habilita el reenvío de **IPv4**. La línea que debe estar descomentada es:

net.ipv4.ip\_forward=1

Una vez que se hace esta modificación, se ejecuta el siguiente comando para aplicar los cambios:

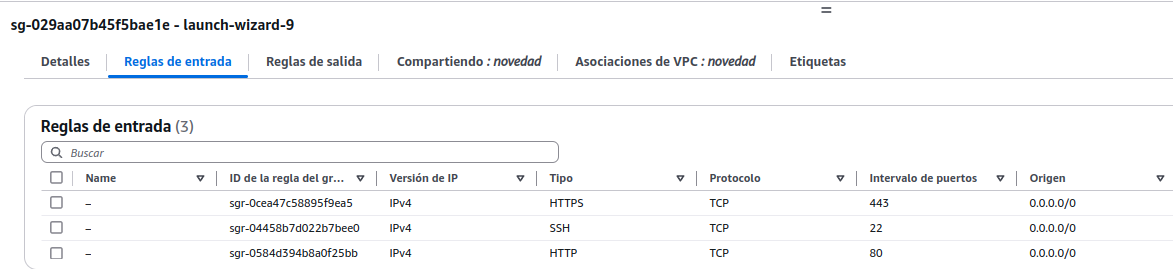
sudo sysctl -p

Esto asegura que el tráfico de red entre las instancias privadas y la instancia **NAT** sea correctamente enrutado.

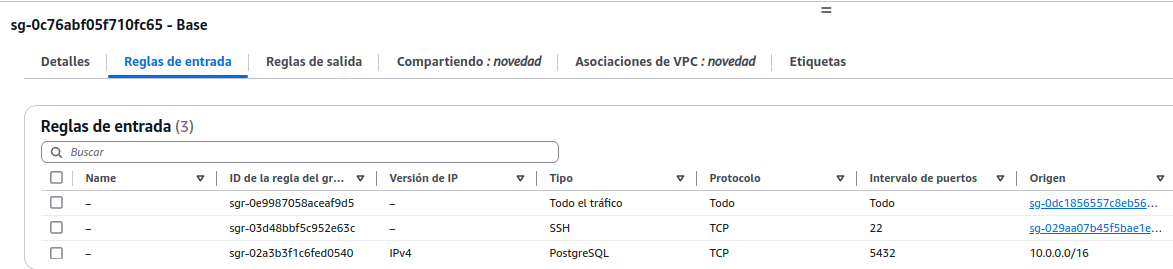
### **Grupos de Seguridad (Security Groups)**

Cada una de las instancias que forman parte de la infraestructura debe estar protegida mediante **grupos de seguridad** que controlan el tráfico entrante y saliente. En nuestro caso, cada instancia tiene sus reglas específicas:

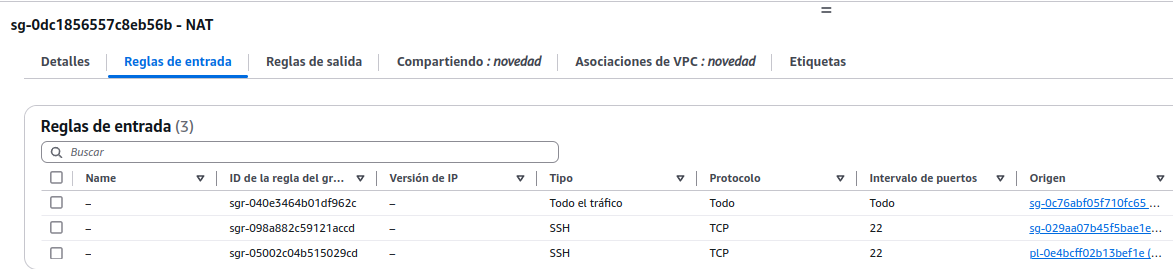
1. **Grupo de Seguridad para la Aplicación (hergutrucks)**:
   * Este grupo de seguridad define las reglas que permiten el tráfico a la aplicación, como acceso a puertos específicos (por ejemplo, el puerto 80 para HTTP o el 443 para HTTPS) para la interacción de los usuarios con la aplicación web.



1. **Grupo de Seguridad para PostgreSQL**:
   * Este grupo controla el acceso a la base de datos **PostgreSQL**. Solo las instancias que necesitan acceder a la base de datos deben tener permisos para conectarse a ella, mientras que el tráfico de otras fuentes es bloqueado.

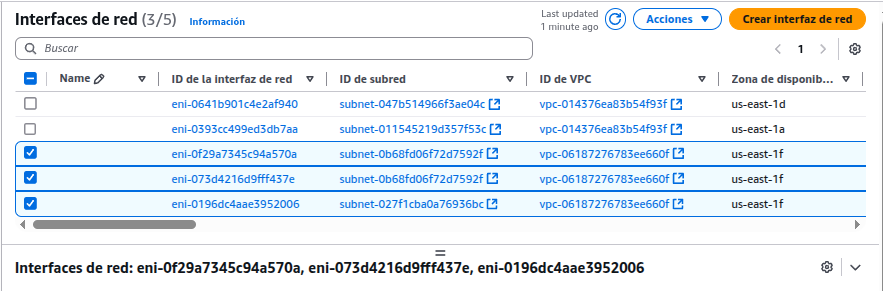


1. **Grupo de Seguridad para NAT**:
   * Este grupo de seguridad regula el tráfico hacia y desde la instancia **NAT**. Asegura que solo el tráfico permitido pase a través de ella, y garantiza la seguridad de la infraestructura.



### **Interfaces de Red**

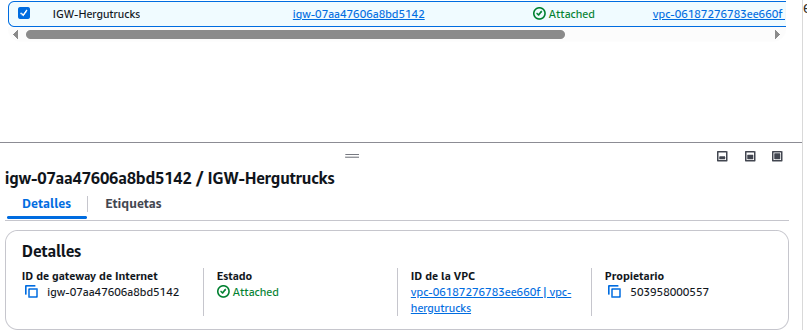
Para que las instancias puedan comunicarse entre sí y con el mundo exterior, tenemos configuradas varias interfaces de red en la **VPC (Virtual Private Cloud)**:



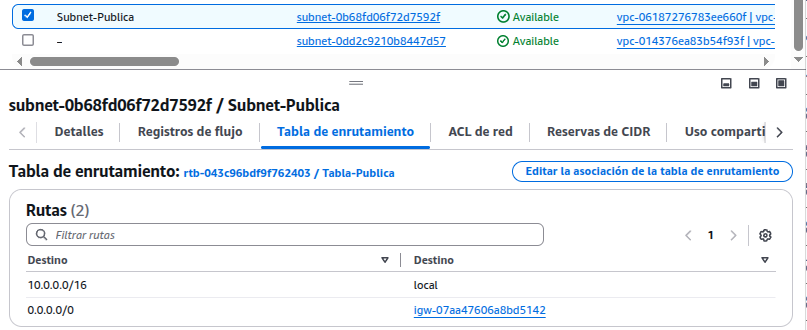
* **VPC**: Es la red virtual donde residen todas nuestras instancias (aplicación, base de datos, NAT, etc.). Al estar en una VPC, nuestras instancias pueden comunicarse de forma segura entre ellas.



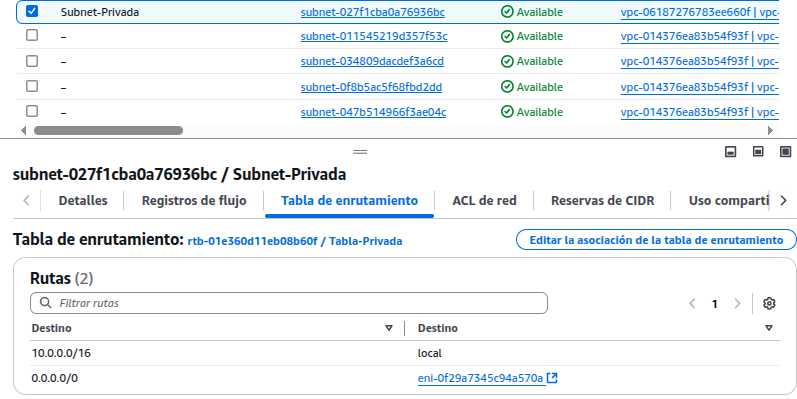
* **Gateway**: El gateway es el punto de salida para el tráfico hacia Internet. La instancia **NAT** está conectada a un gateway de la VPC para redirigir el tráfico de las instancias privadas hacia la red pública.



* **Subredes**:
  + **Subred pública**: Esta subred alberga recursos que necesitan acceso directo a Internet, como la instancia **NAT** y posiblemente la aplicación, dependiendo de la configuración.



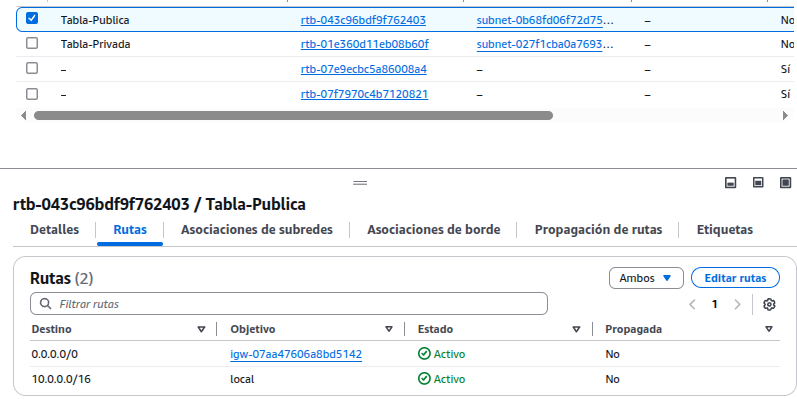
* + **Subred privada**: En esta subred residen las instancias que no necesitan acceso directo a Internet. Aquí es donde se encuentra **PostgreSQL**, aislado del acceso público por razones de seguridad.



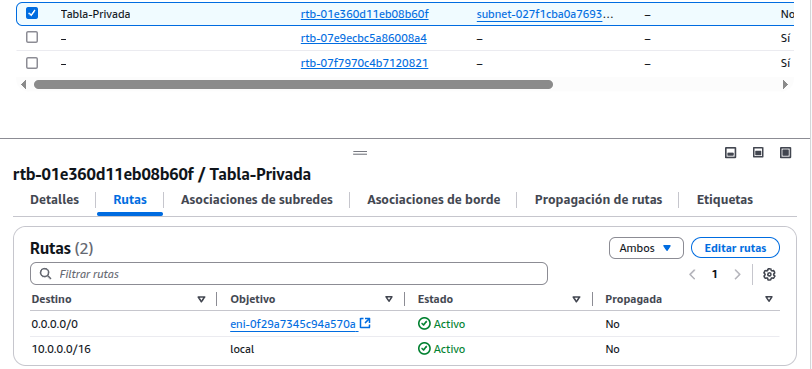
### **Tablas de Enrutamiento**

Las tablas de enrutamiento son esenciales para controlar cómo se enruta el tráfico dentro de la **VPC**. Existen dos tablas de enrutamiento principales en nuestra infraestructura:

1. **Tabla pública**: Controla el tráfico entre la subred pública y el resto de la red, incluyendo Internet. En esta tabla se configuran las rutas hacia el gateway para permitir que las instancias en la subred pública accedan a Internet.



1. **Tabla privada**: Gestiona el tráfico entre las instancias de la subred privada y la subred pública o hacia Internet a través de **NAT**. Esto asegura que las instancias privadas no estén directamente expuestas a Internet, pero puedan acceder a recursos externos a través de la instancia **NAT**.



Con esta infraestructura, tenemos una arquitectura segura, escalable y eficiente, donde cada componente tiene su rol específico, y todas las comunicaciones están cuidadosamente controladas y gestionadas.