AWS VPC Peering Connections

Purpose:

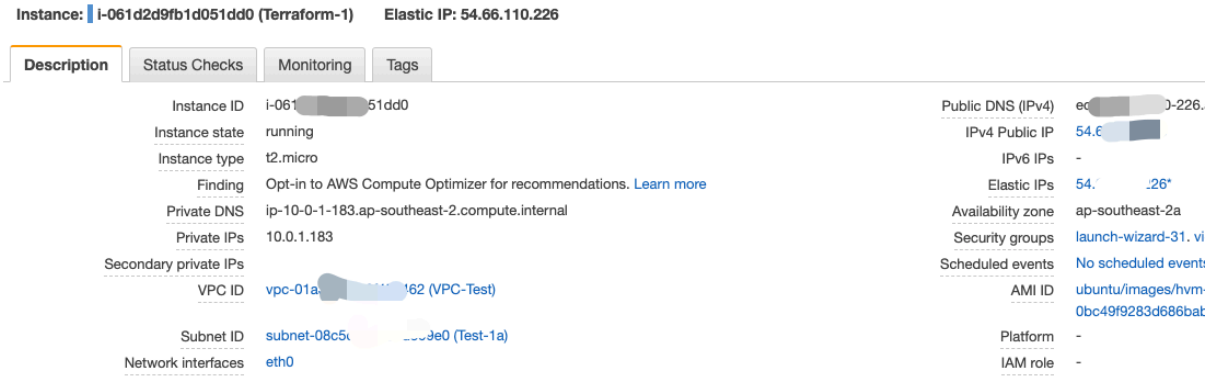
Cost-effective, no single point of failure or bandwidth bottleneck, more secure (No DDoS, common exploits, without traffic going through public internet) inter-region VPC Peering connection.

Assumption:

Having 2 VPCs within Sydney (Asia Pacific (Sydney) ap-southeast-2) and Singapore (Asia Pacific (Singapore)ap-southeast-1) respectively.

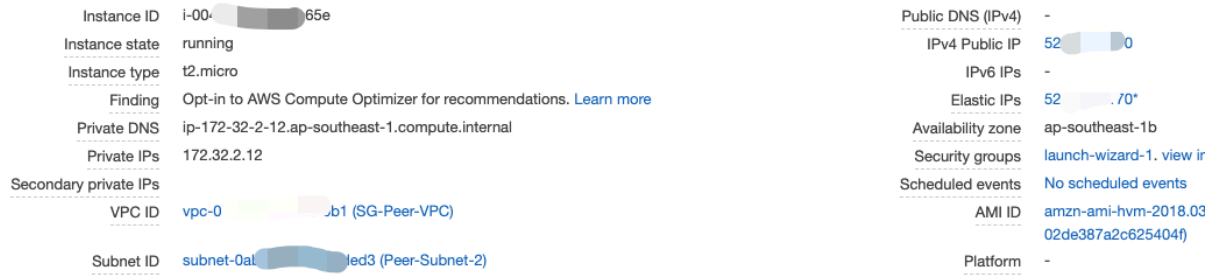
Subnet configuration in Sydney region:

We have an EC2 instance running in this subnet with private IP 10.0.1.183

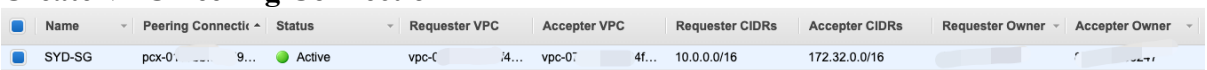


Subnet configuration in Sydney region:

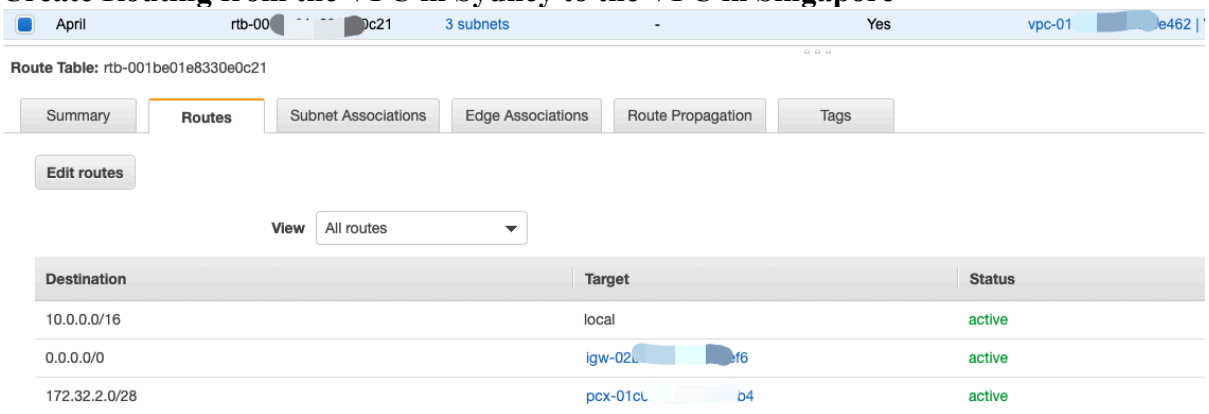
We have an EC2 instance running in this subnet with private IP 172.32.2.12



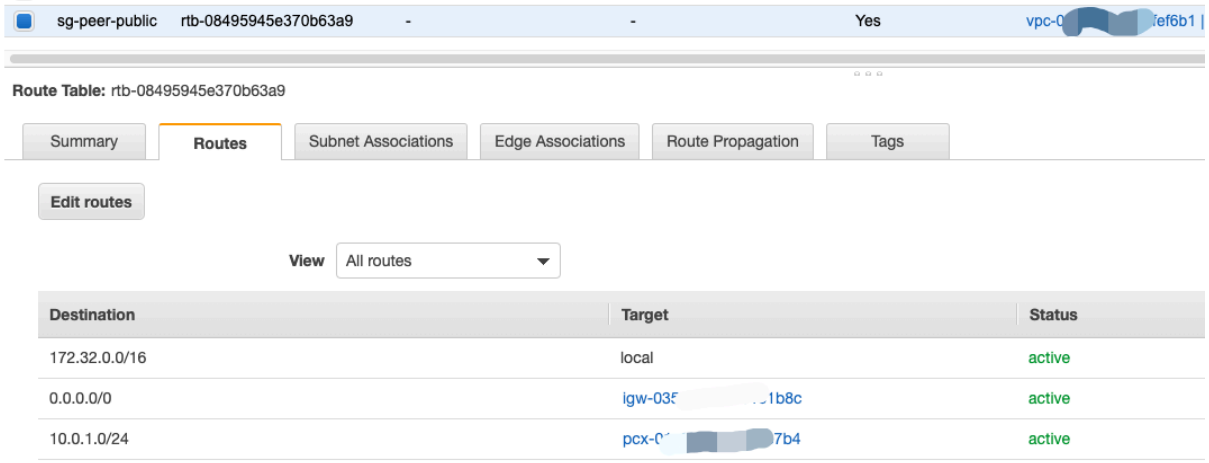
Create VPC Peering Connection



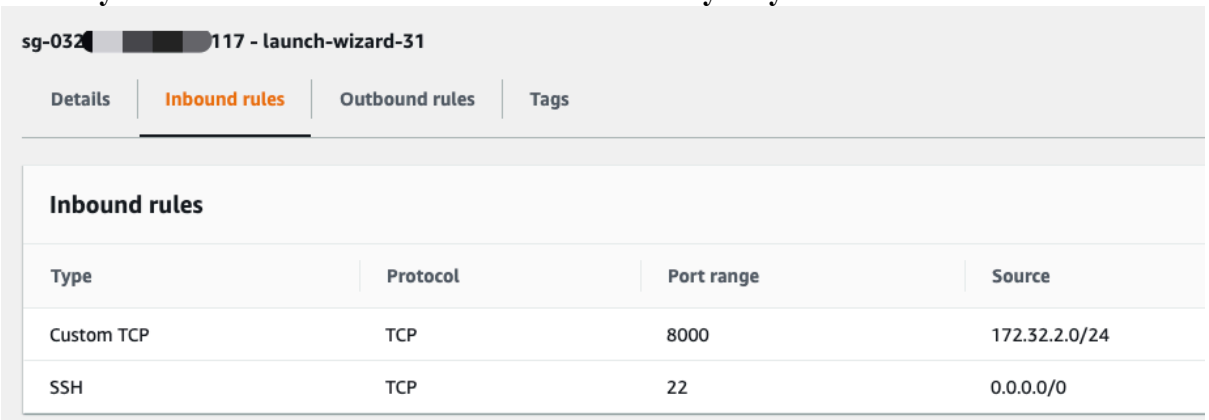
Create Routing from the VPC in Sydney to the VPC in Singapore



Create Routing from the VPC in Singapore to the VPC in Sydney



Security Inbound rule for the EC2 instance in the Sydney VPC



Only allow traffic from the 172.32.2.0/24 subnet in peering VPC in Singapore region

Listen to port 8000 in Sydney EC2 instance

```
root@ip-10-0-1-183:/home/ubuntu# nc -l -p 8000
nice
```

Connection from Singapore EC2 instance to the Sydney EC2 instance through private network. (Must use private IP as destination IP here)

```
[root@ip-172-32-2-12 ec2-user]# nc -vv 10.0.1.183 8000
Connection to 10.0.1.183 8000 port [tcp/irdmi] succeeded!
nice
```