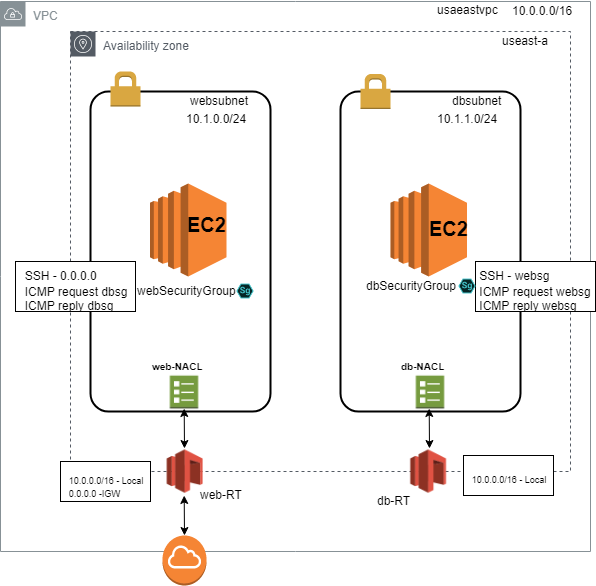
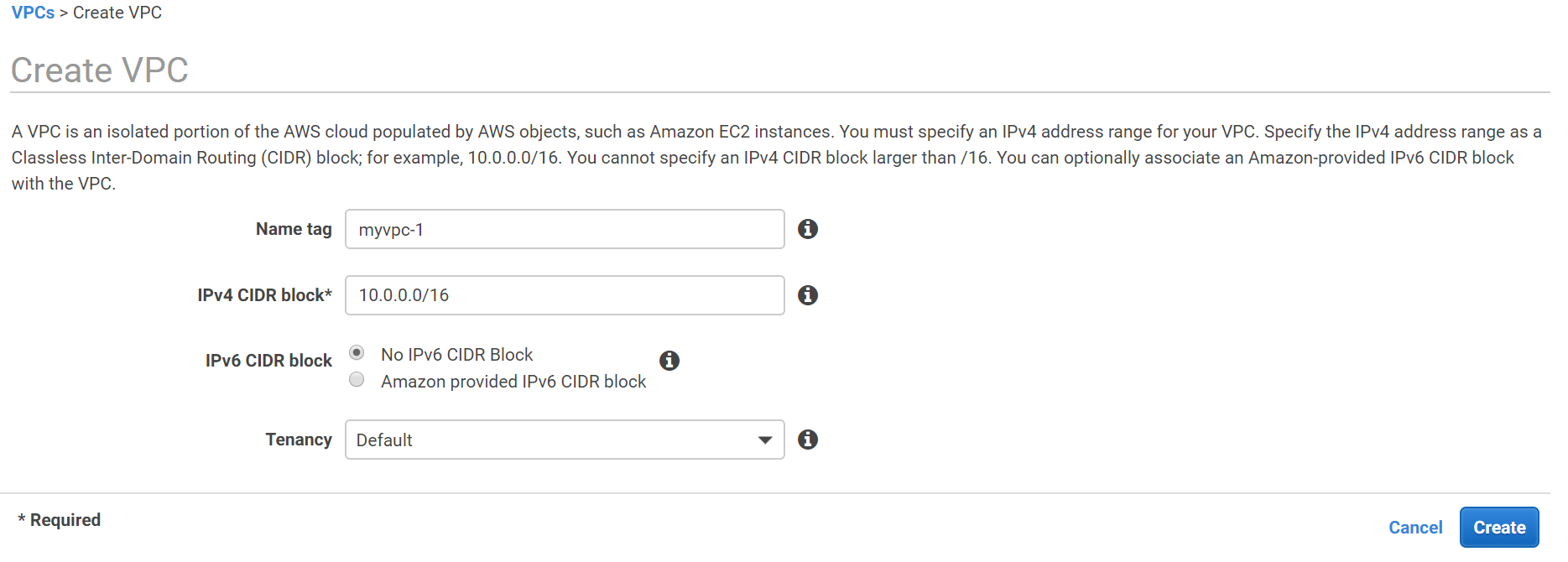
**Hands on LAB**

1. Create a custom VPC with two subnet one for each webserver and a database server. Configure NACL, Security Group and Routing table to ensure webserver can ping database server and vice versa.

****

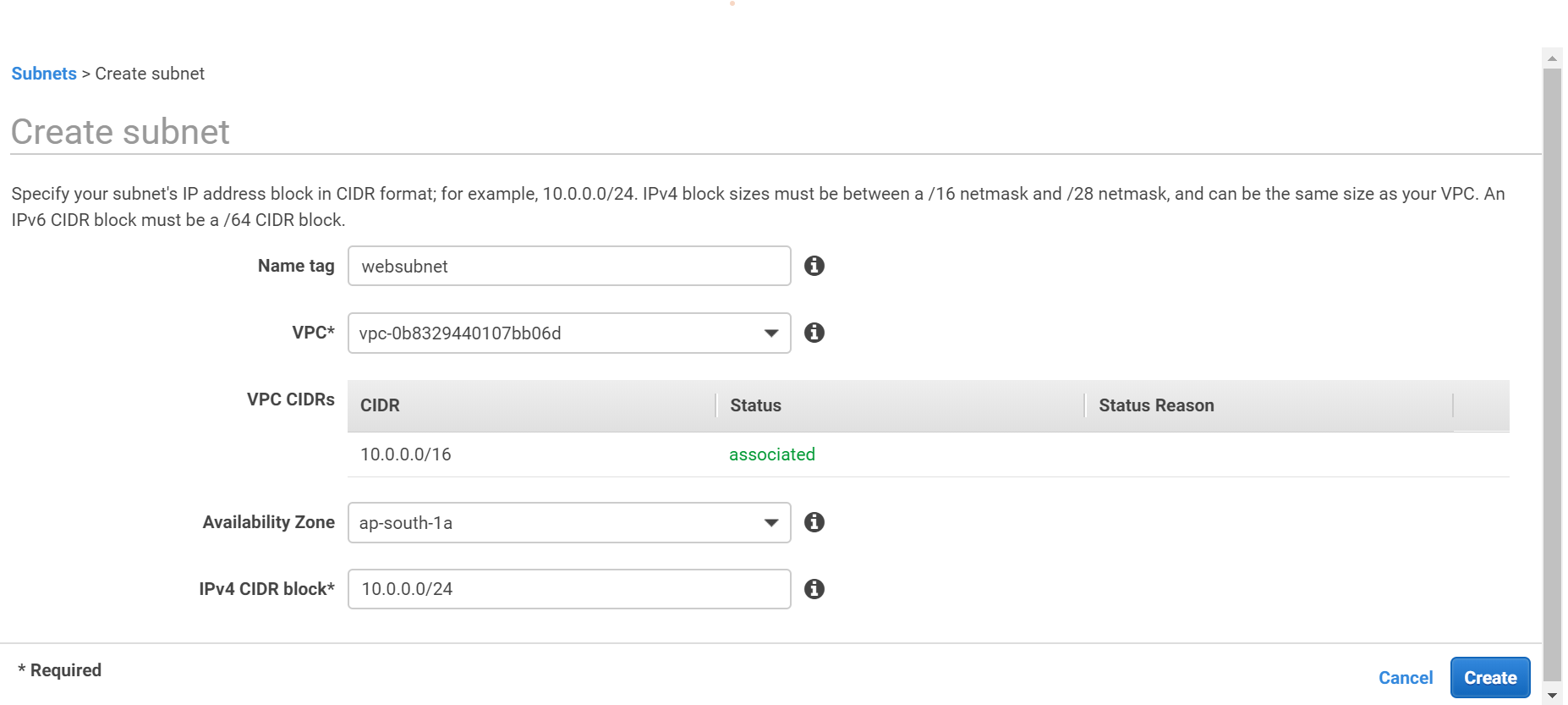
Things needs to be done

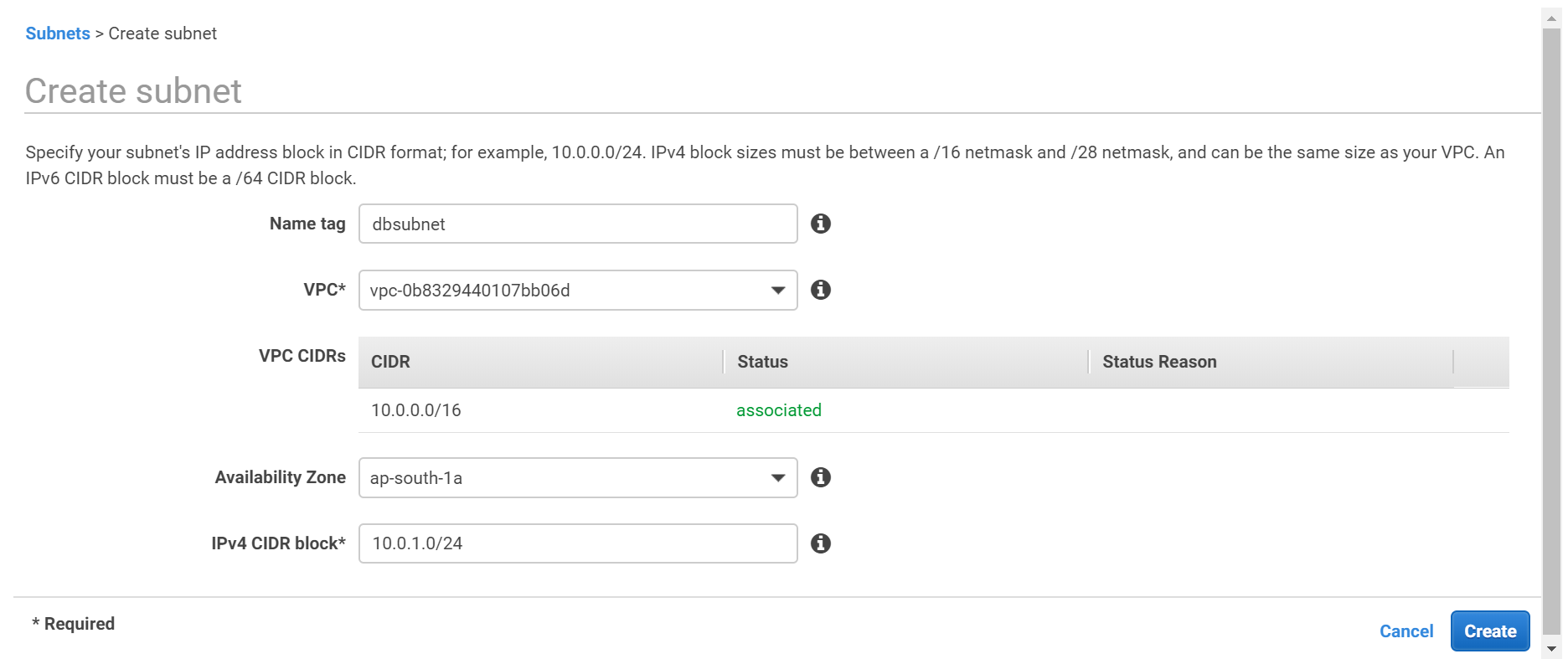
1. Create new VPC – CIDER block 10.0.0.0/16 = 65,531 IP address



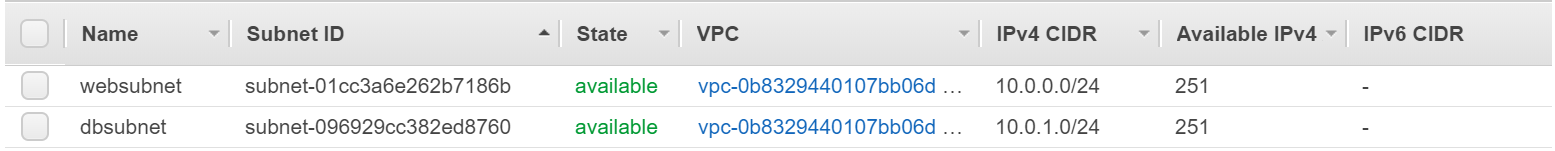
1. Create two subnets –public subnet websubnet (10.0.0.0/24) = 251 IP addresses

and a private subnet dbsubnet (10.0.1.0/24) = 251 IP addresses

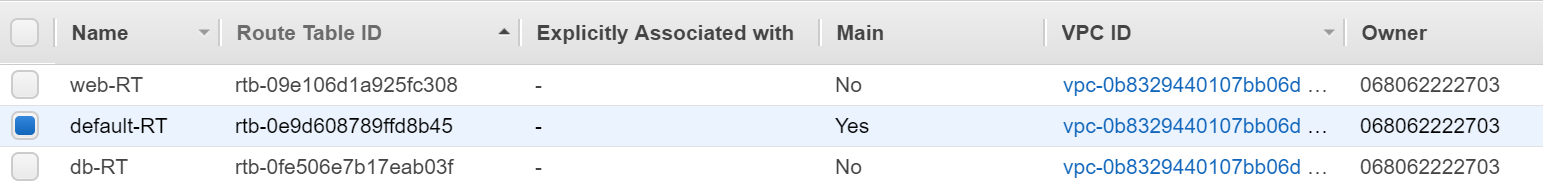




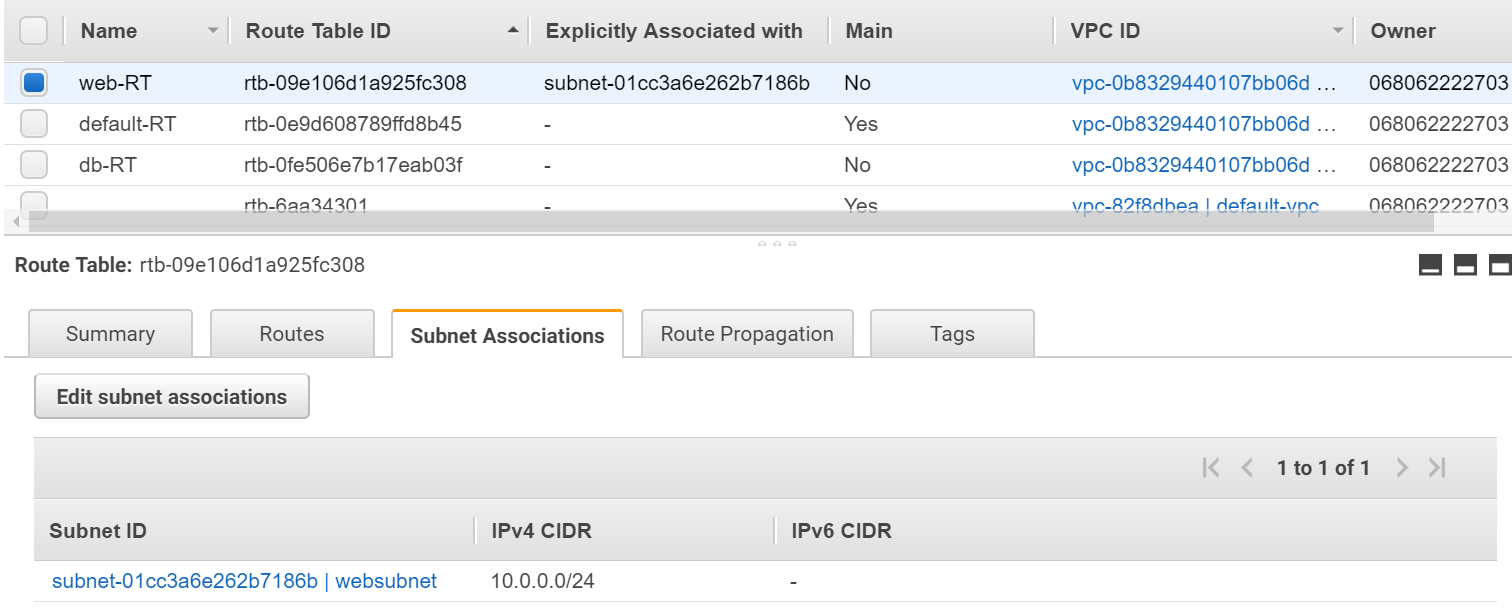
Subnet created

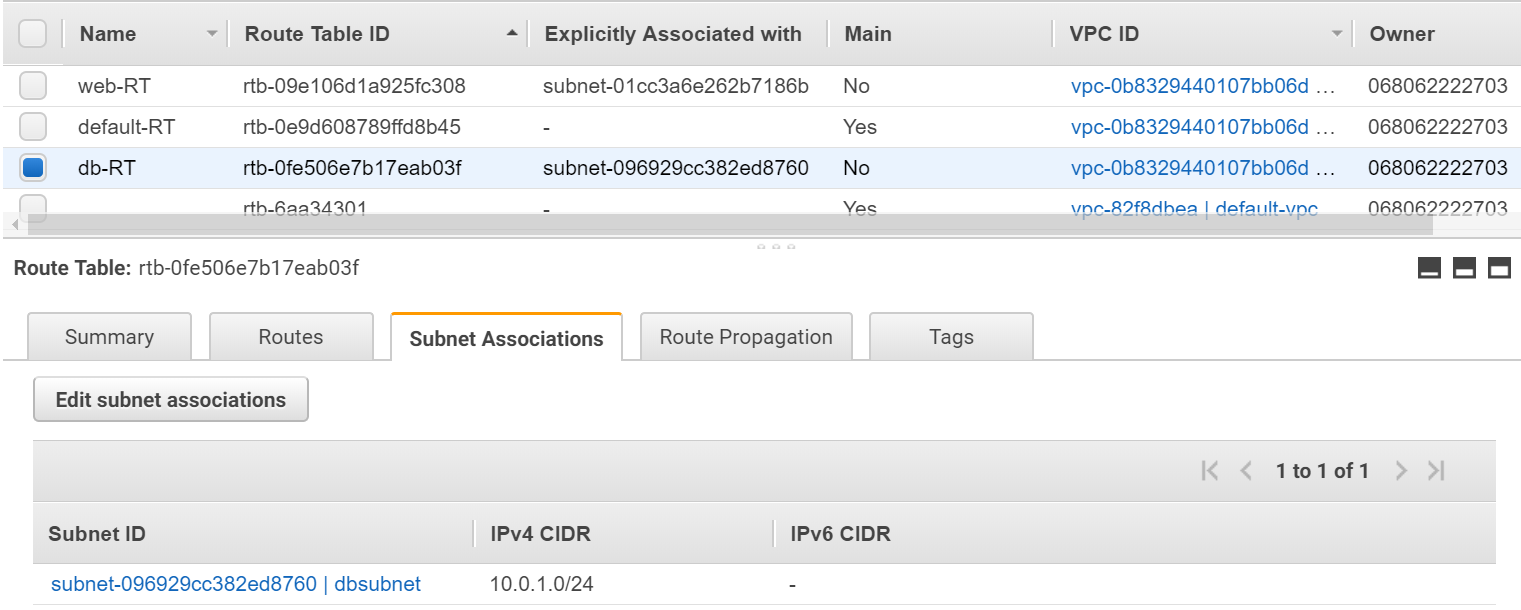


1. Create new Routing Tables **web-RT** and **db-RT**. Default-RT is created by default when VPC was created.

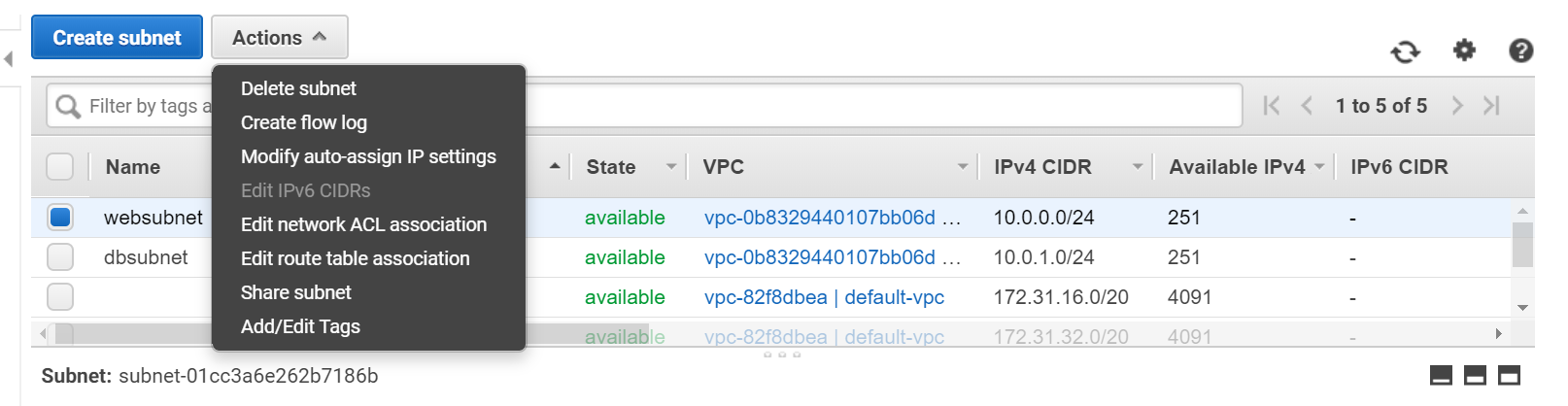


1. Associate web-RT to websubnet and db-RT with dbsubnet. Once associated websubnet and dbsubnet are no more associated with the default routing table.





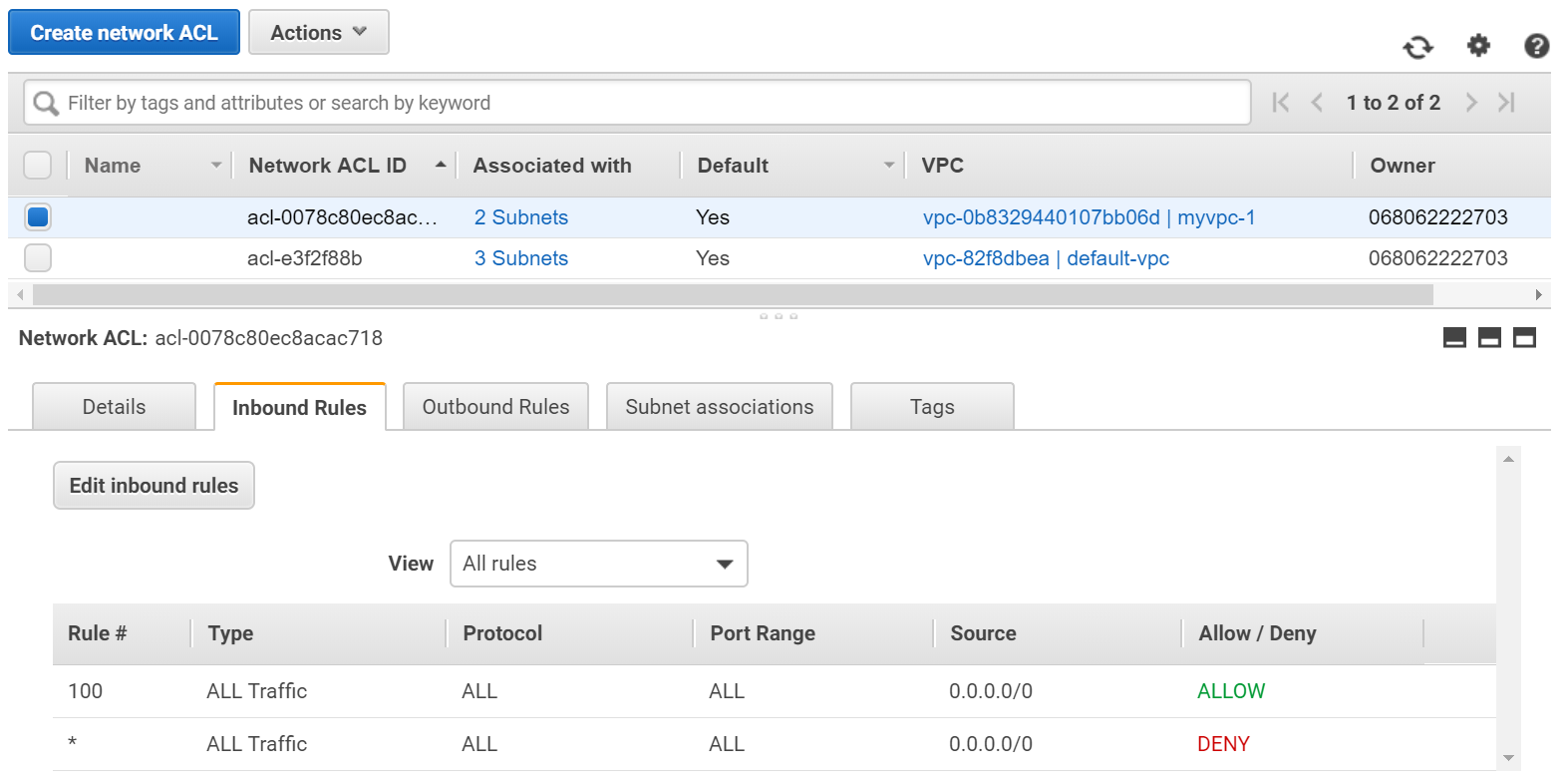
1. Modify auto assigned-IP setting for websubnet. Select websubnet and from action menu select Modify-auto-assign IP setting.



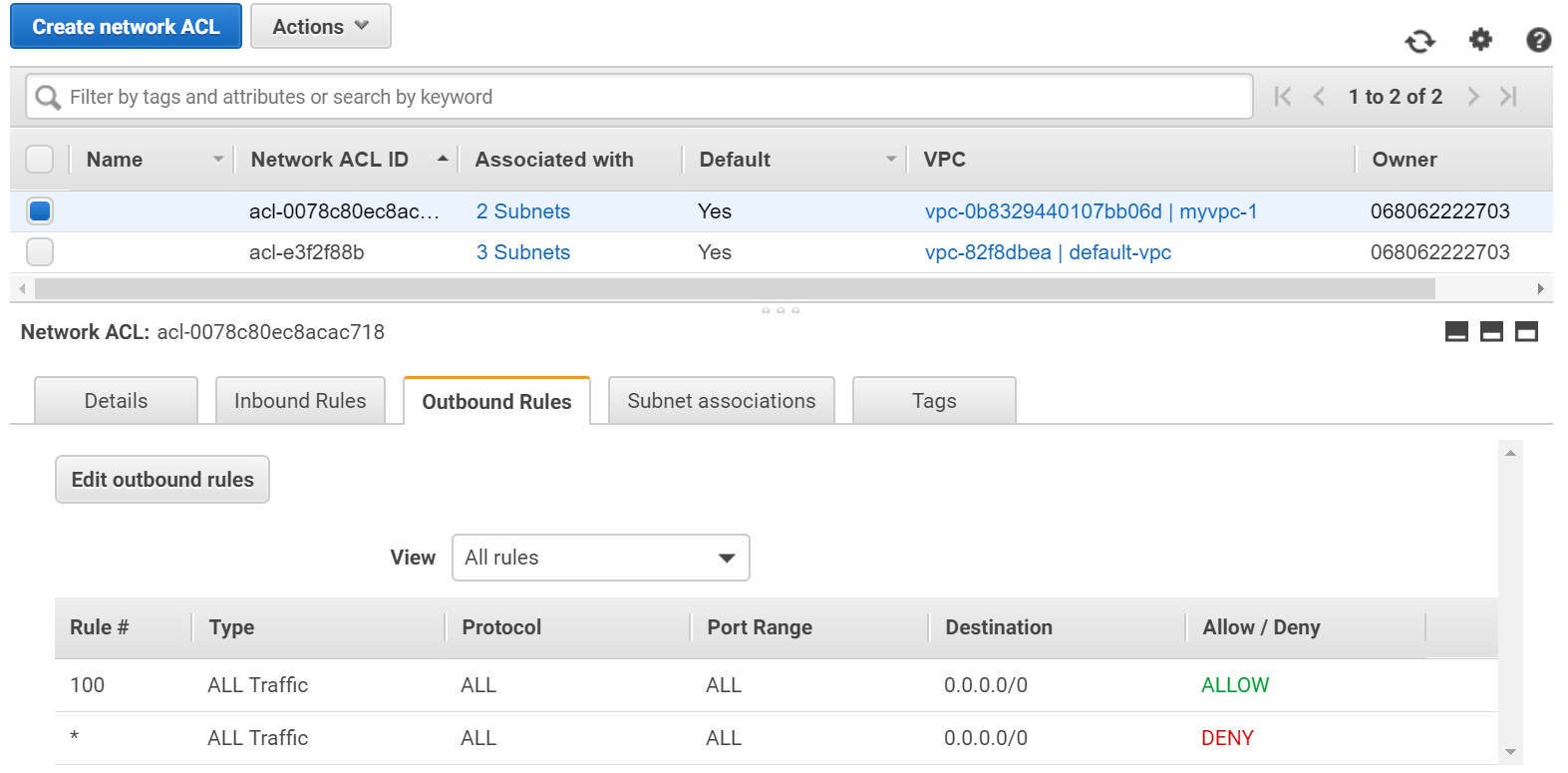


1. Default NACL allows all inbound and outbound traffic and associate to both the subnet.

**Inbound Rule – default NACL**

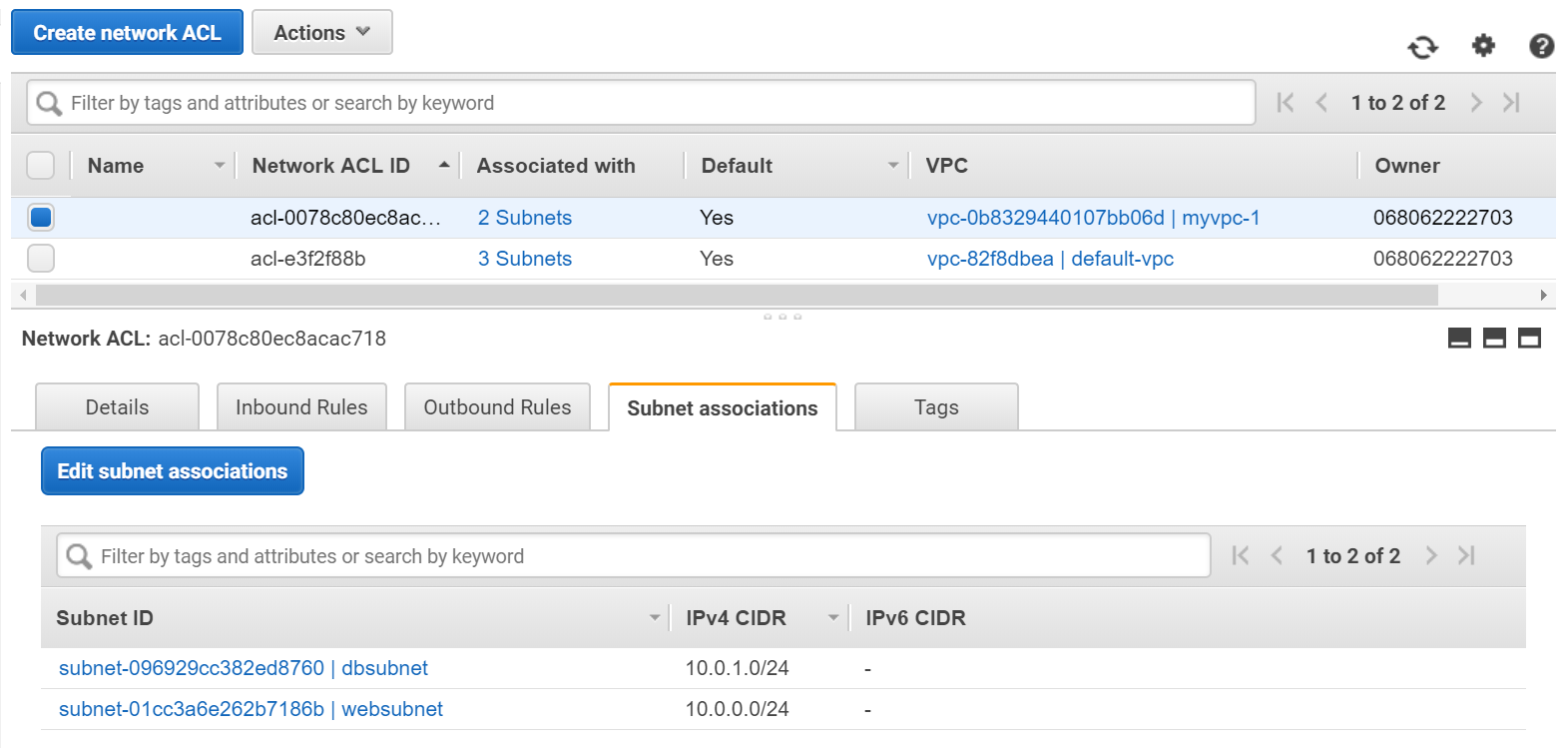


**Outbound Rule – default NACL**

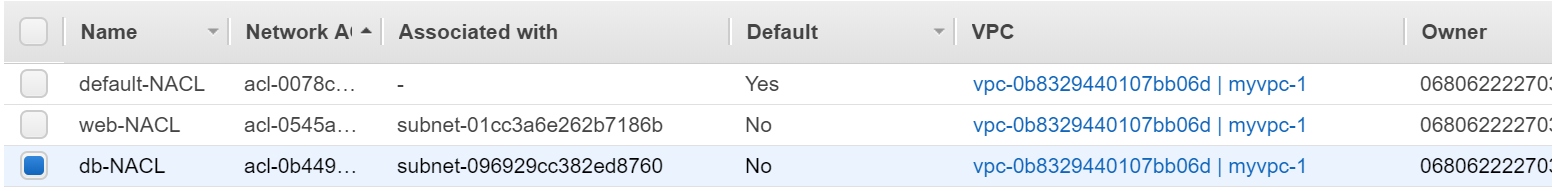


1. Create separate NACLs for websubnet and for dbsubnet.

**Subnet Association**

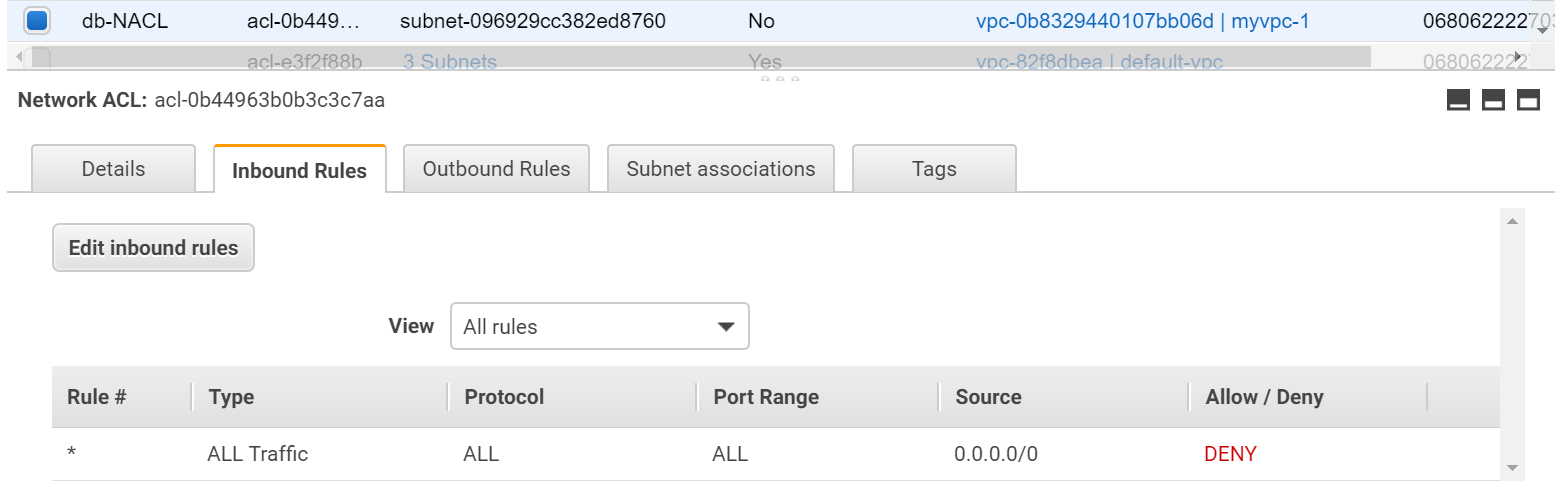


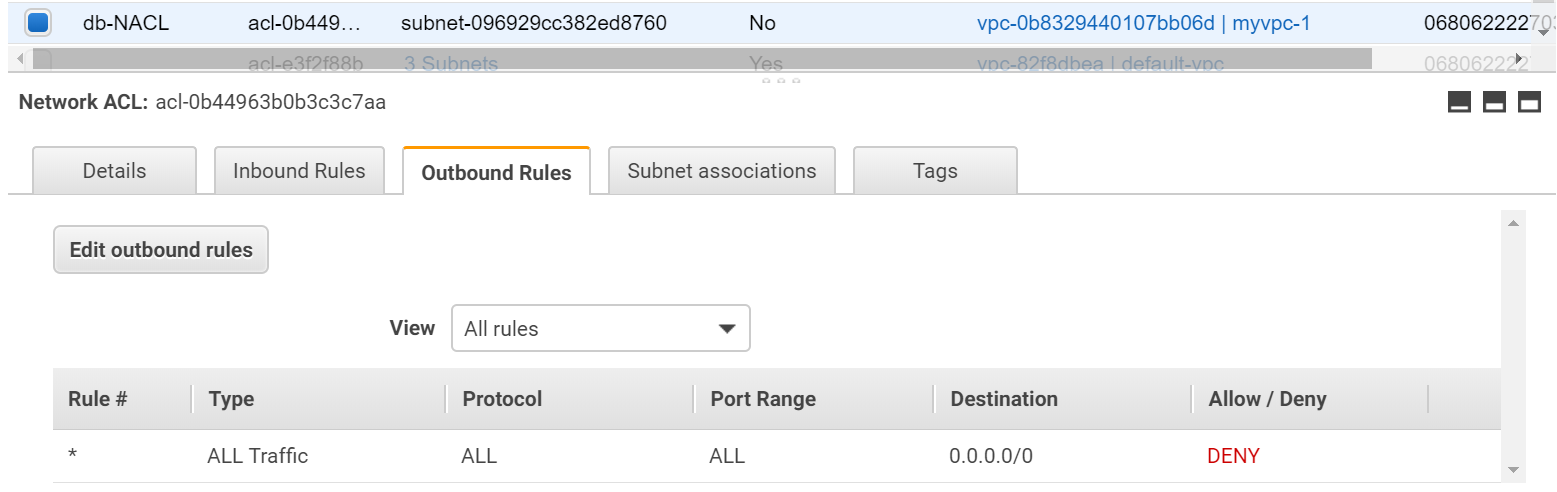
1. Create two new NACLs name them web-NACL & db-NACL and associate them with websubnet and dbsubnet respectively.



Note: this will automatically de-associate subnet from the default-NACL

By default, web-NACL and db-NACL block all inbound and outbound traffic to/from subnet.

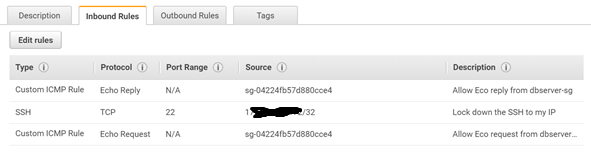




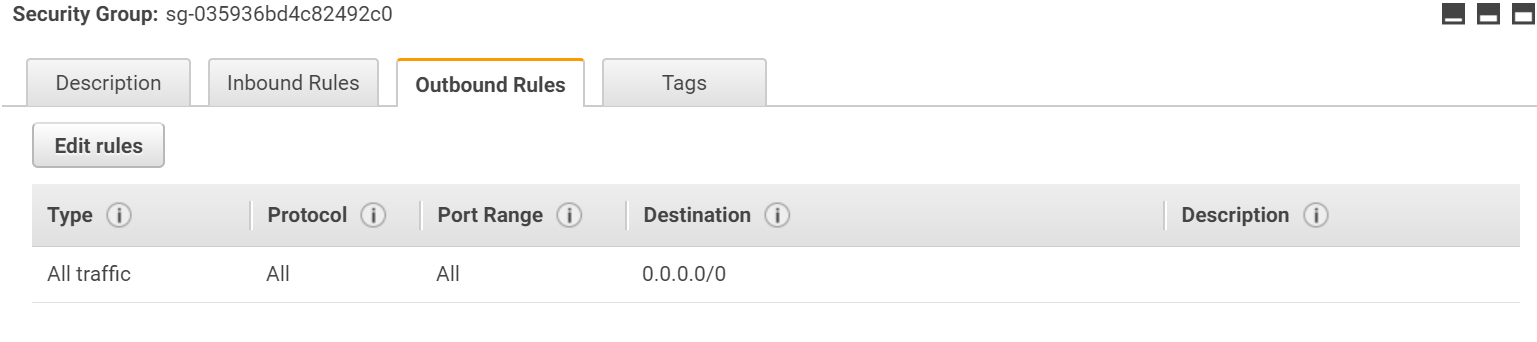
1. Create two new security group one for webservers and the other for dbservers.

Note: New security group by default blocks all the traffic (does not come with any allowed rule), default security group created with the VPC allows all traffic.

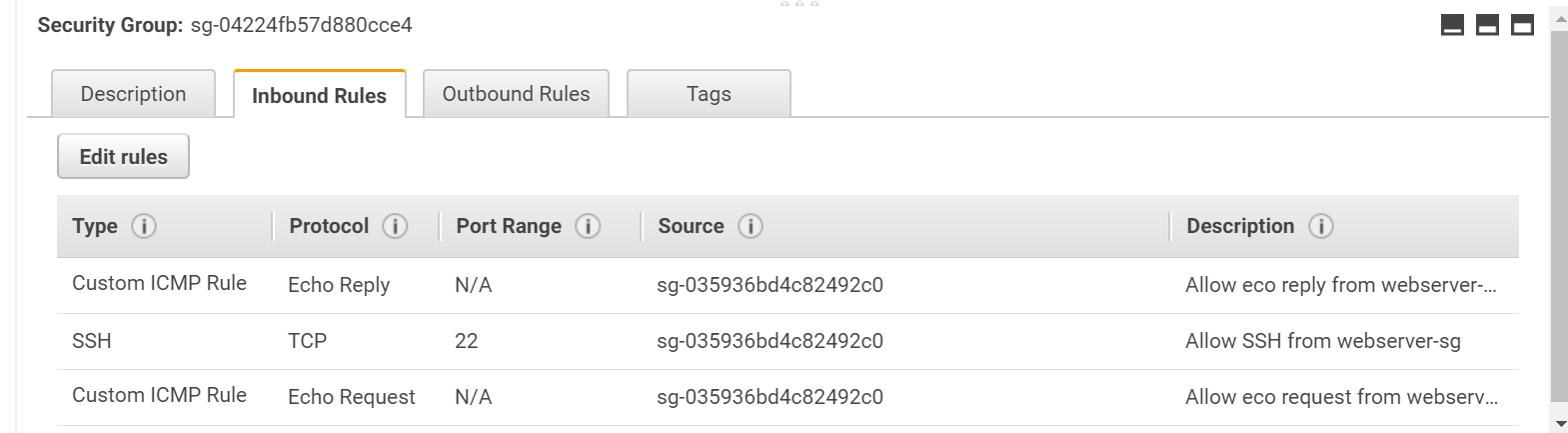
**Web-Security group – Inbound**

****

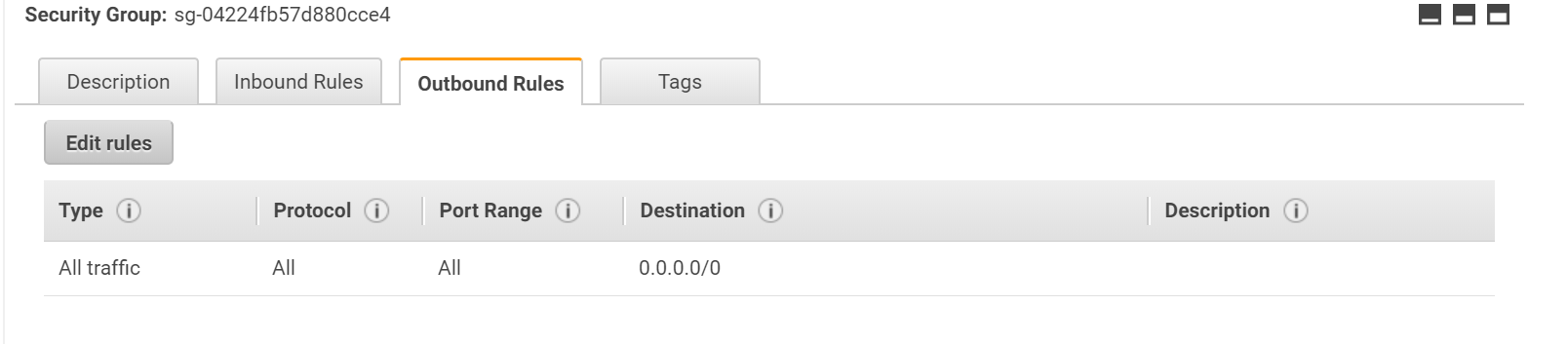
**Web-Security group – outbound**



**Db-Security group – Inbound**

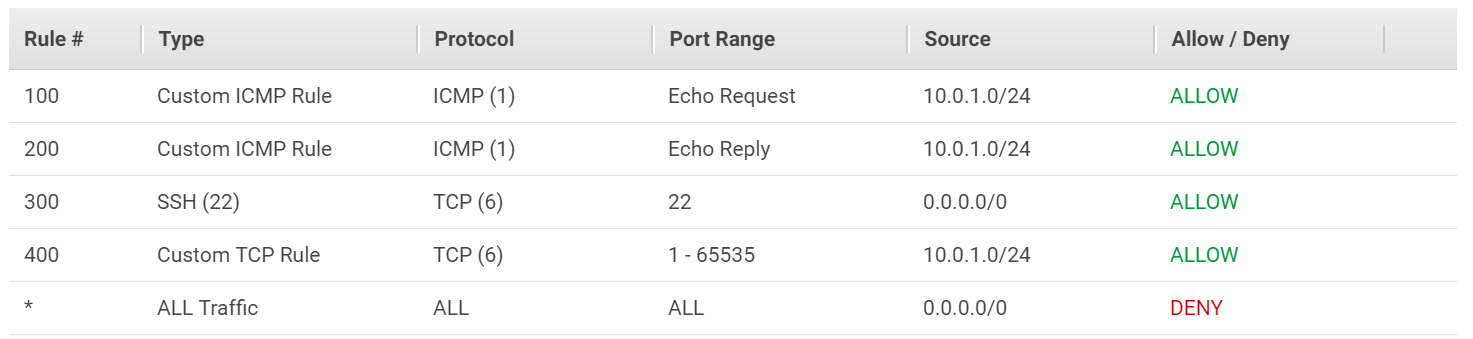


**Db-Security group – outbound**

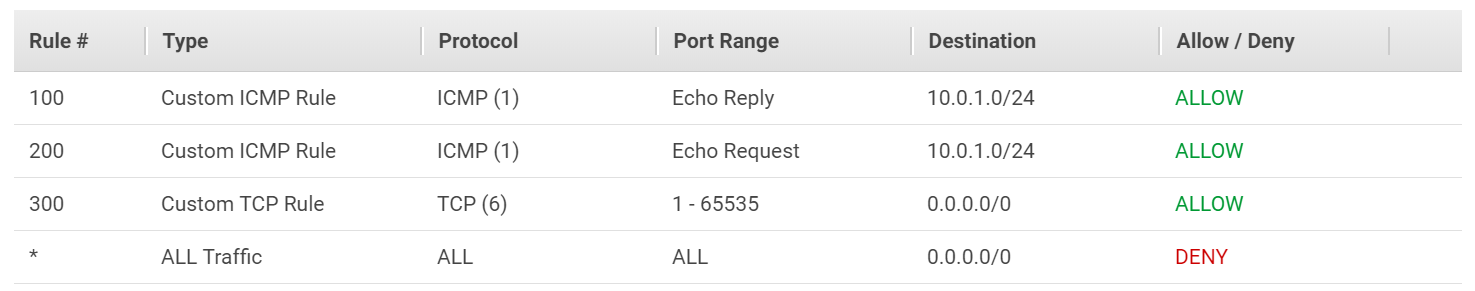


1. **NACLs to allow ICMP (ping) between websubnet and dbsubnet**

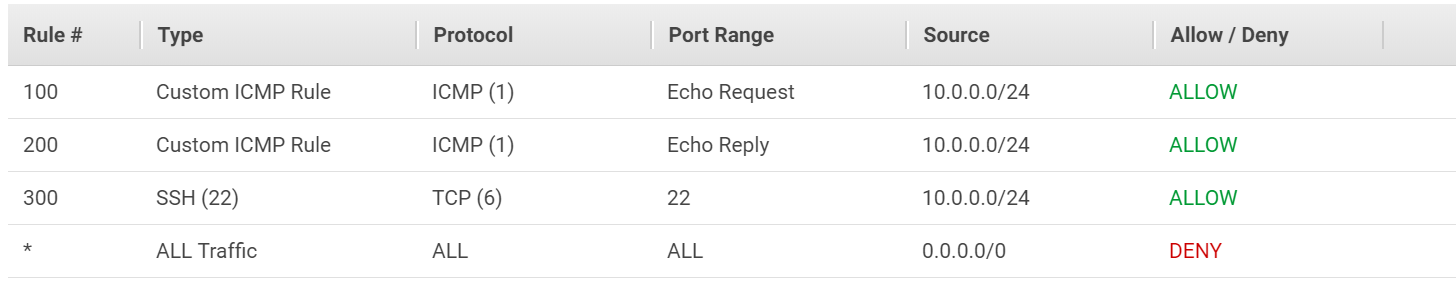
**Web-NACL inbound rule**



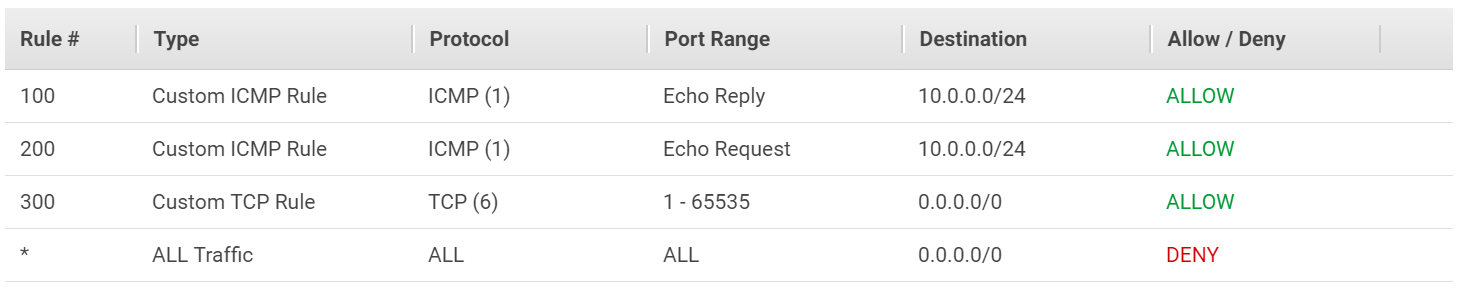
**Web-NACL outbound rule**



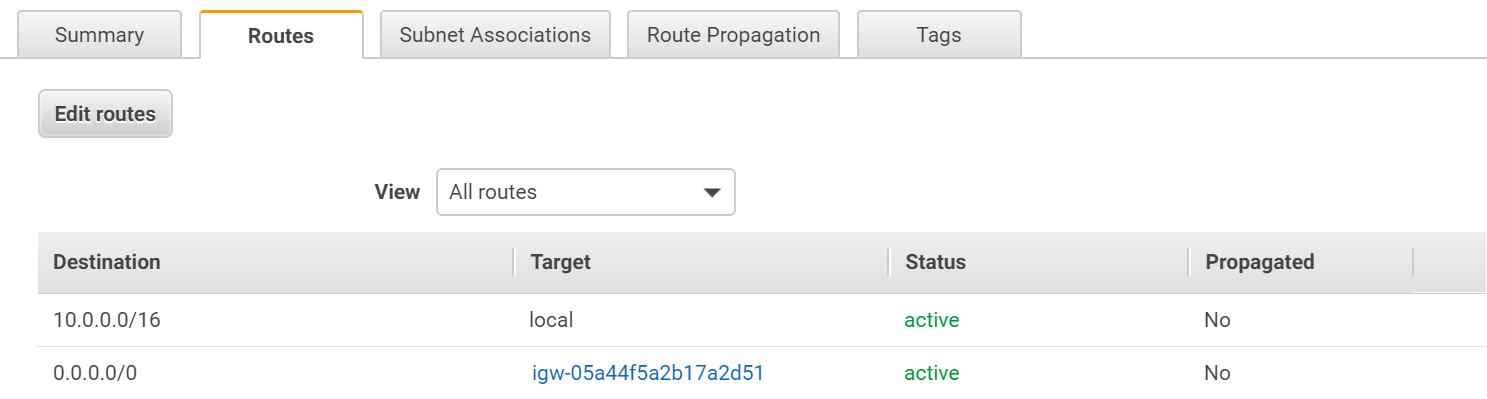
**Db-NACL inbound rule**



**Db-NACL outbound rule**



**Create an IGW (internet gateway) and associate it with Web-RT**



|  |
| --- |
| **Trouble shooting pointers** |
| For SSH to response back to instance TCP-IP port (1-65535) need to open. |
| SSH request goes over TCP-IP port 22 return back in (1-65535) port |
| One need an IGW to connect to internet to reach from internet. |