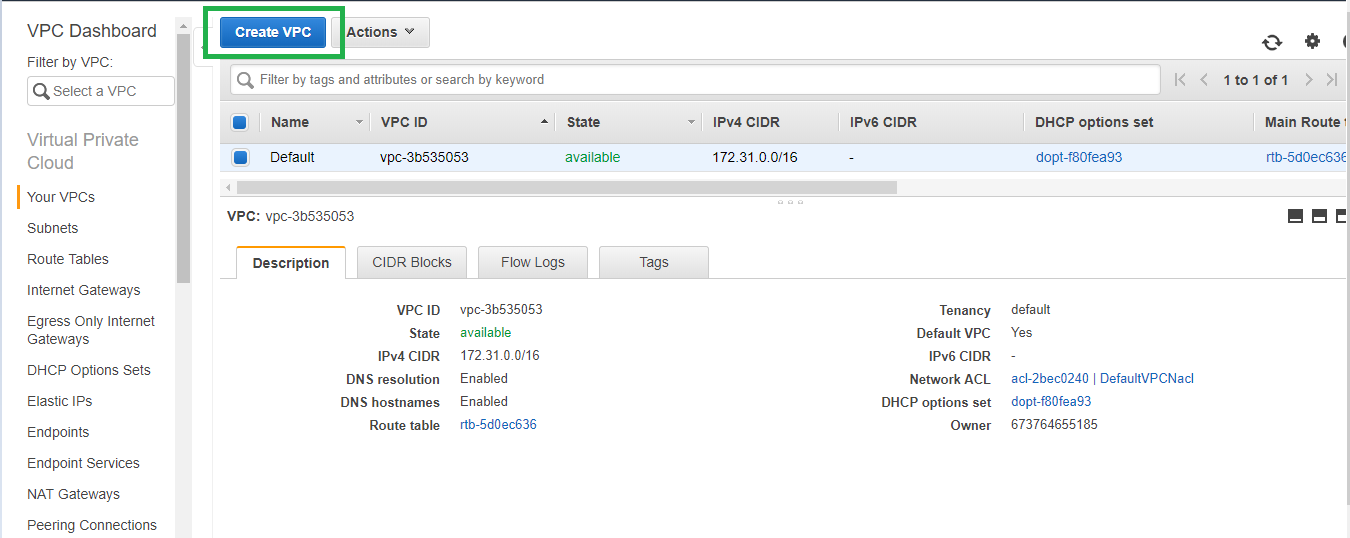
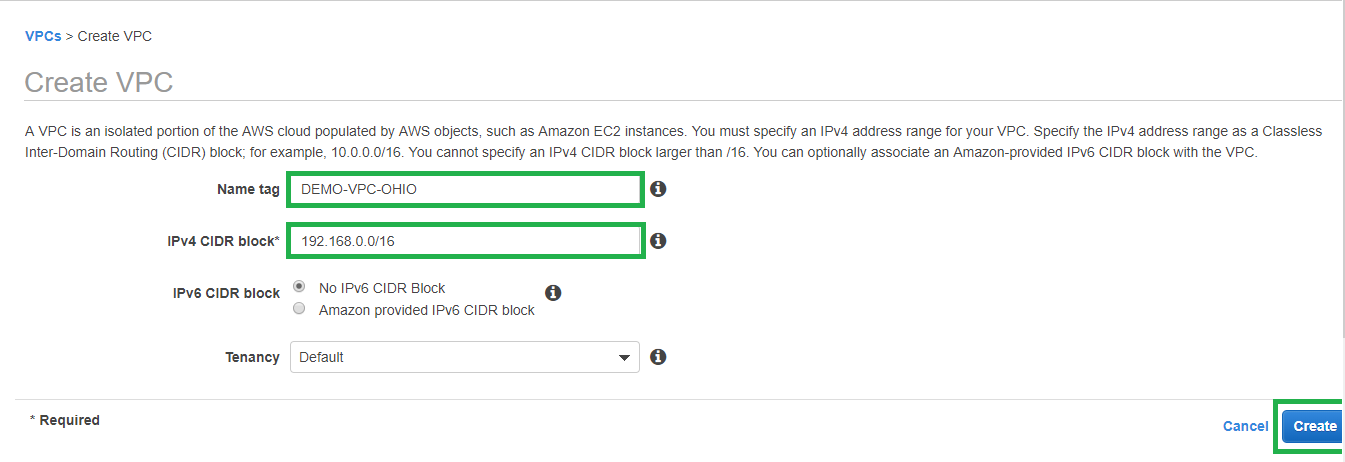
**Lab: VPC CREATION**

**Services Used: VPC**

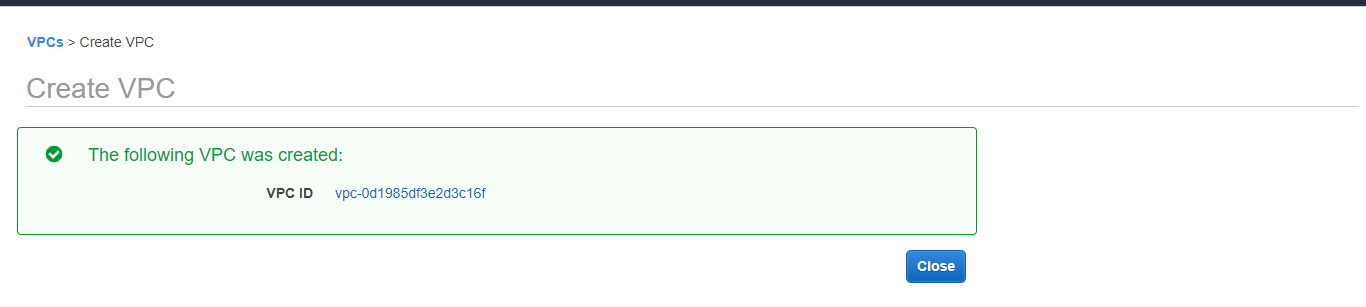
1. Go to VPC Service
2. VPC 🡪 Your VPCs 🡪 Create VPC.

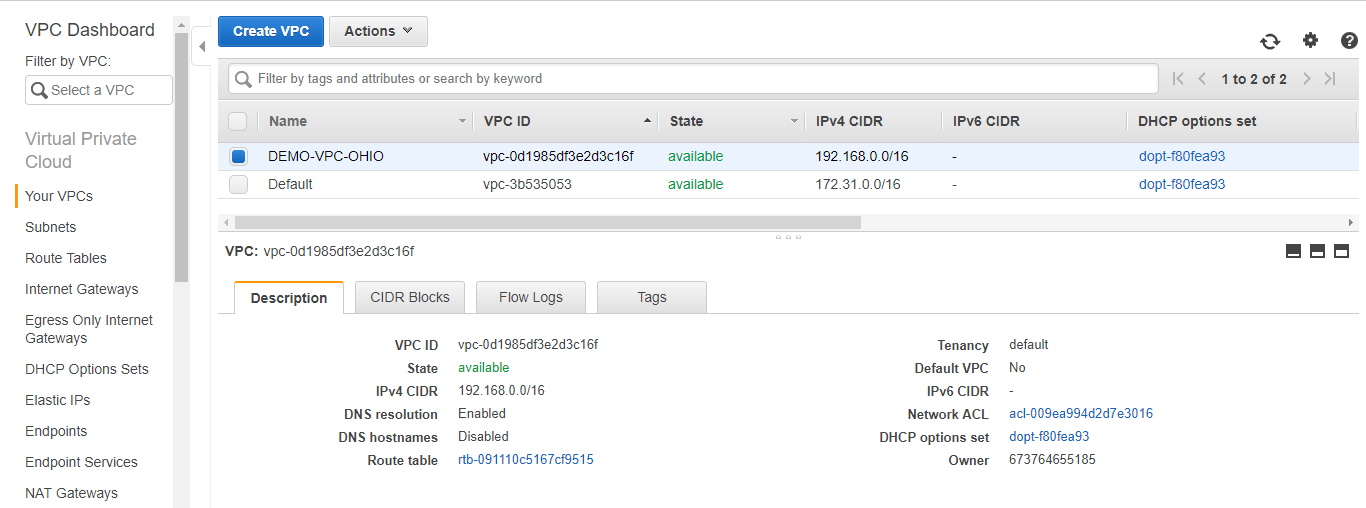


1. Provide Name for the VPC and provide a valid CIDR network that you have planned to use for the VPC, leave the remaining default and click create.

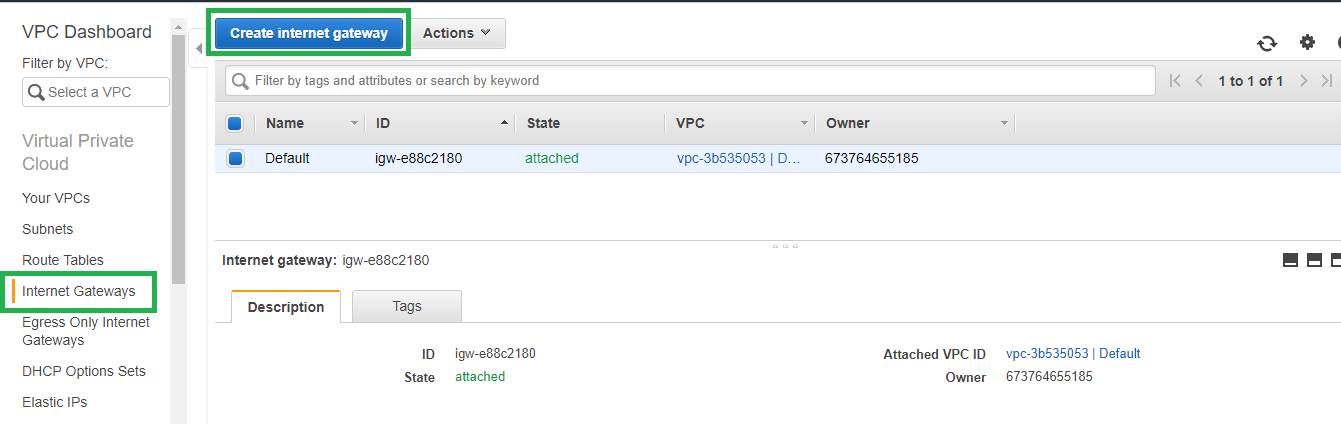


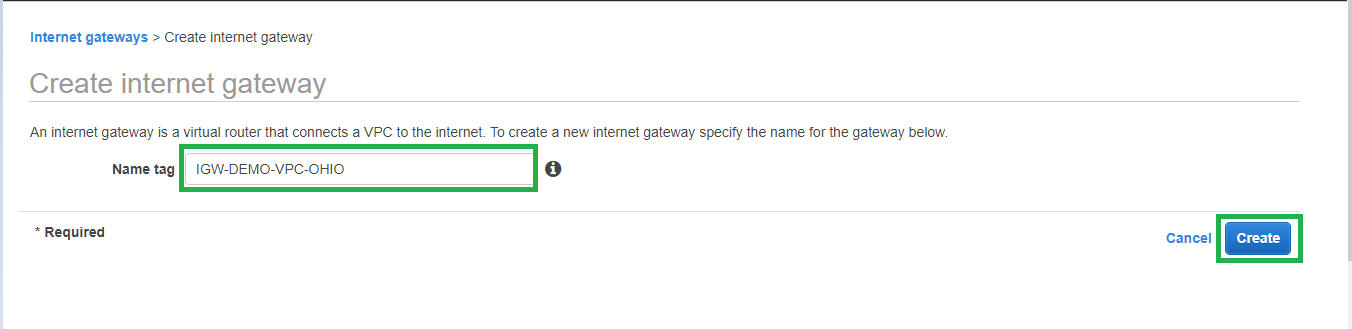
1. VPC is created now.

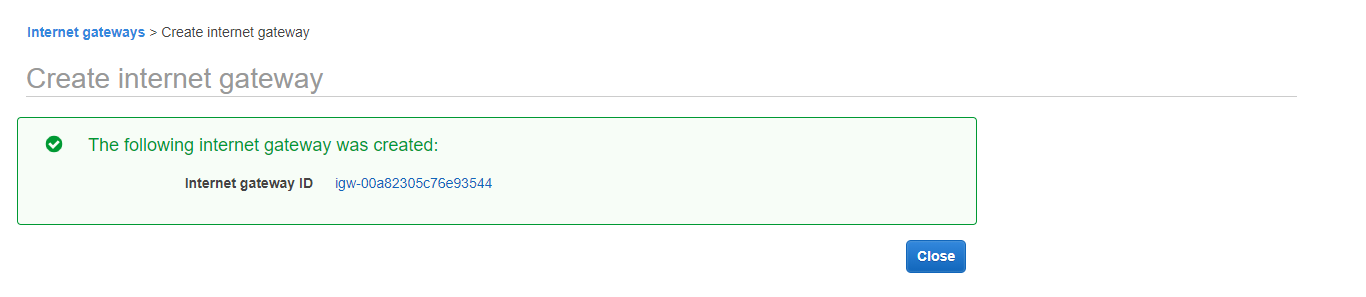


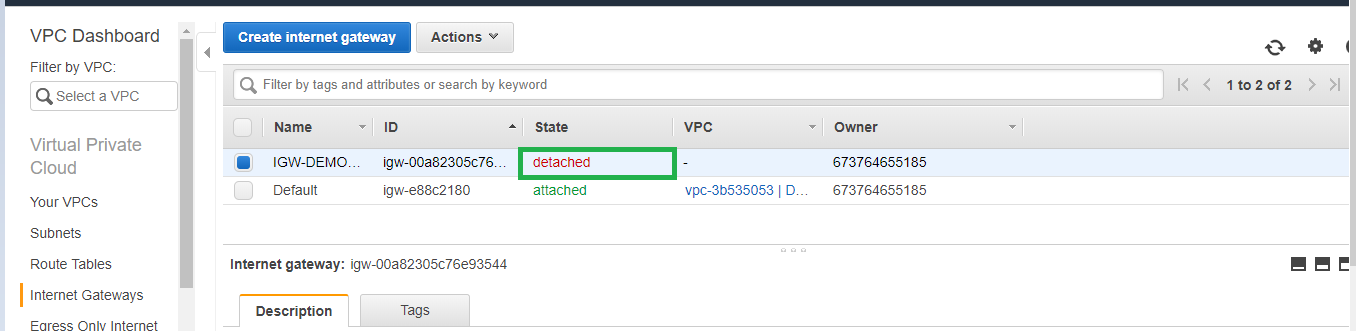


1. Create a new Internet gateway. Initial status will be detached.

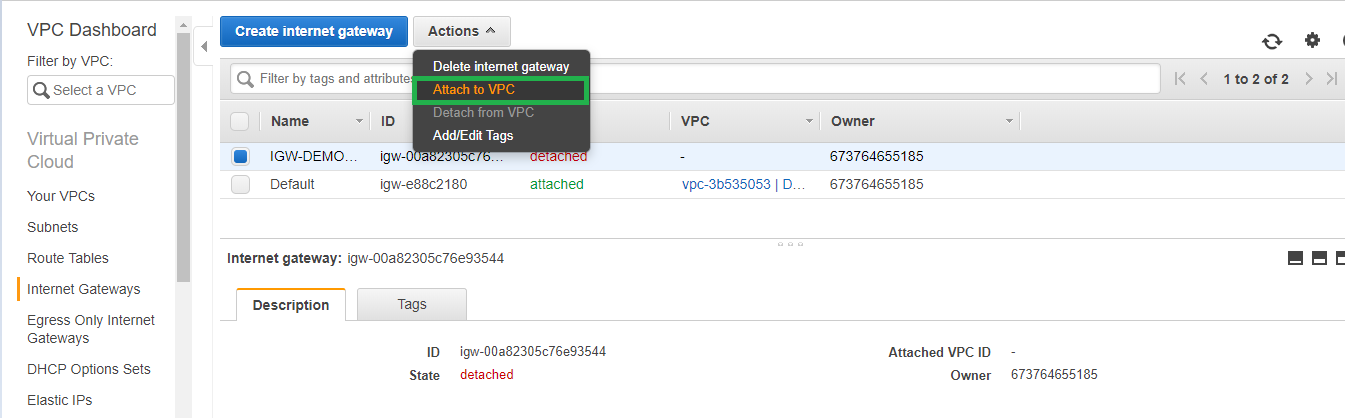


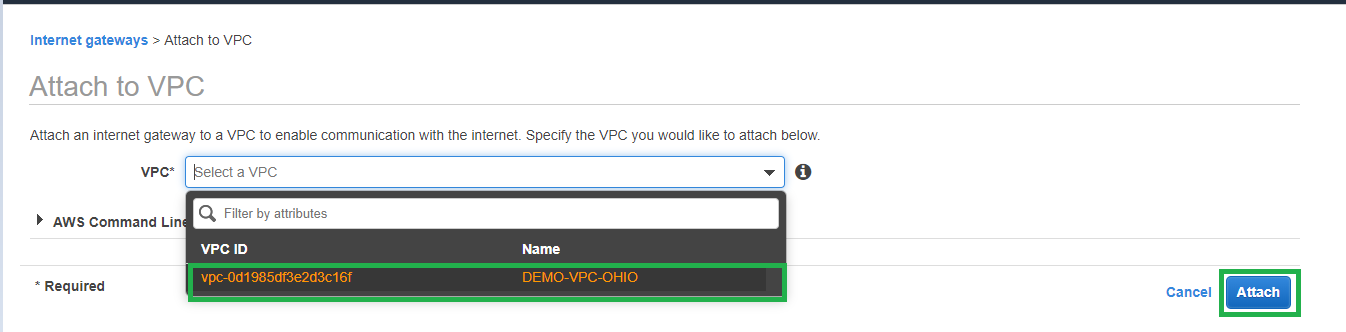




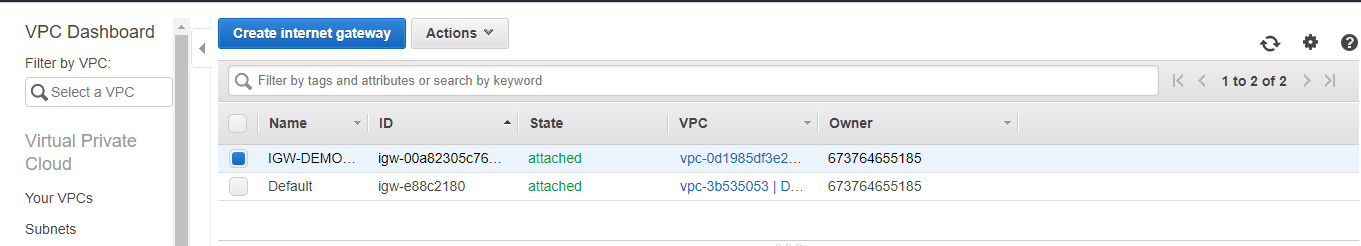


1. Attach the new Internet Gateway to the new VPC created.



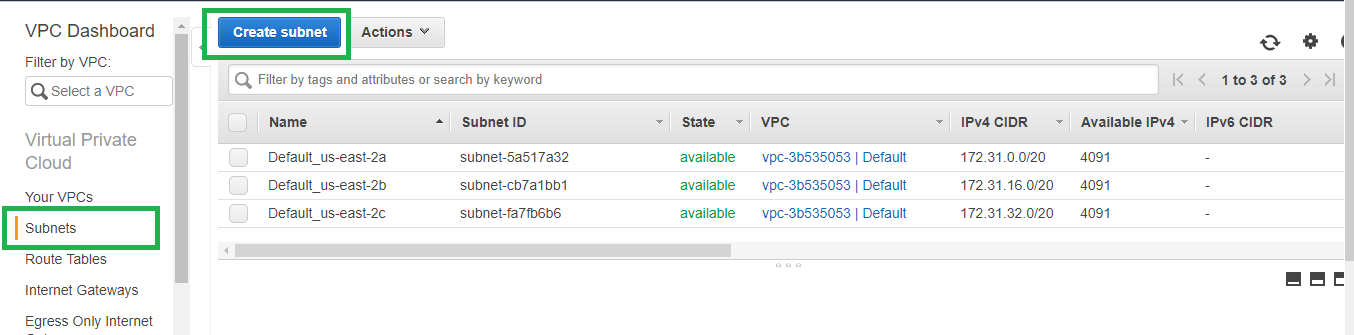


1. Now the Internet gateway status will be attached.



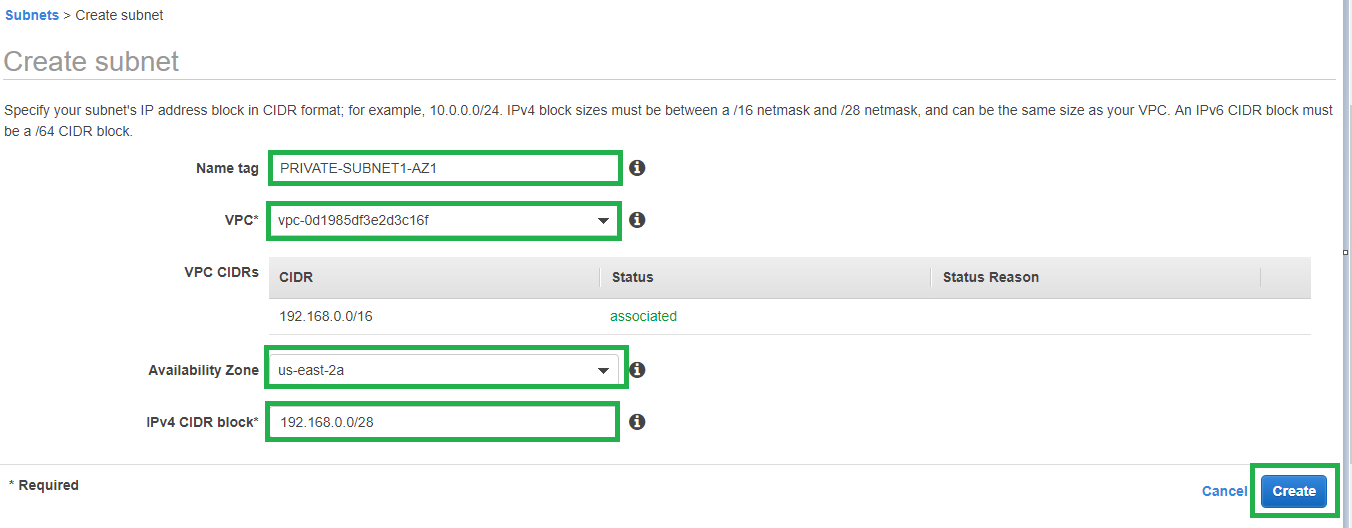
1. Create new Subnets for the VPC.

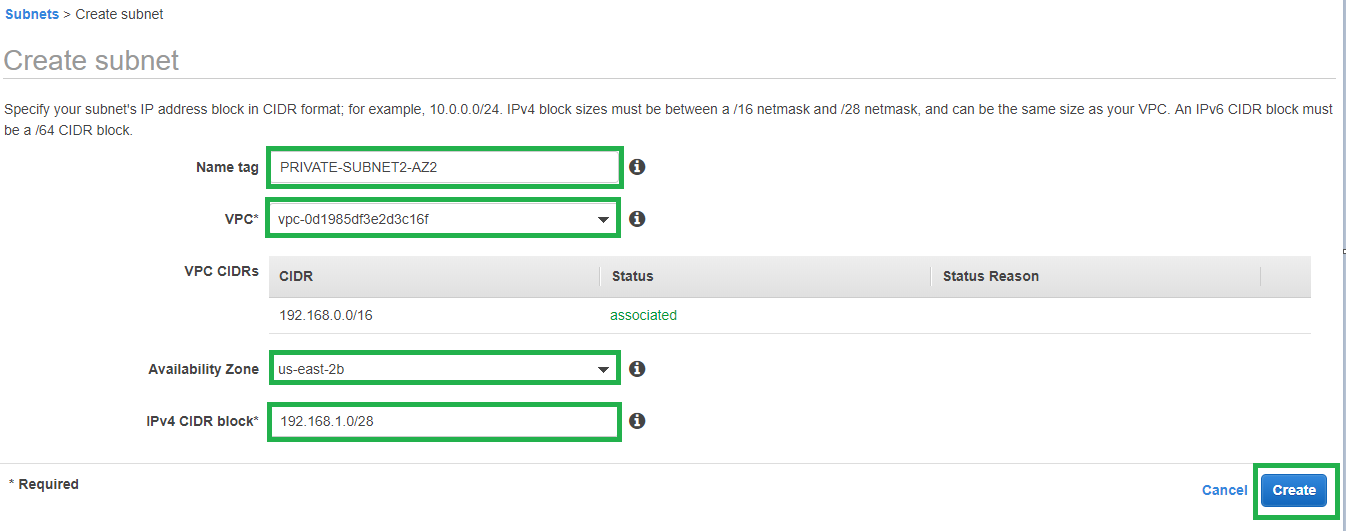
Subnets 🡪 Create subnet

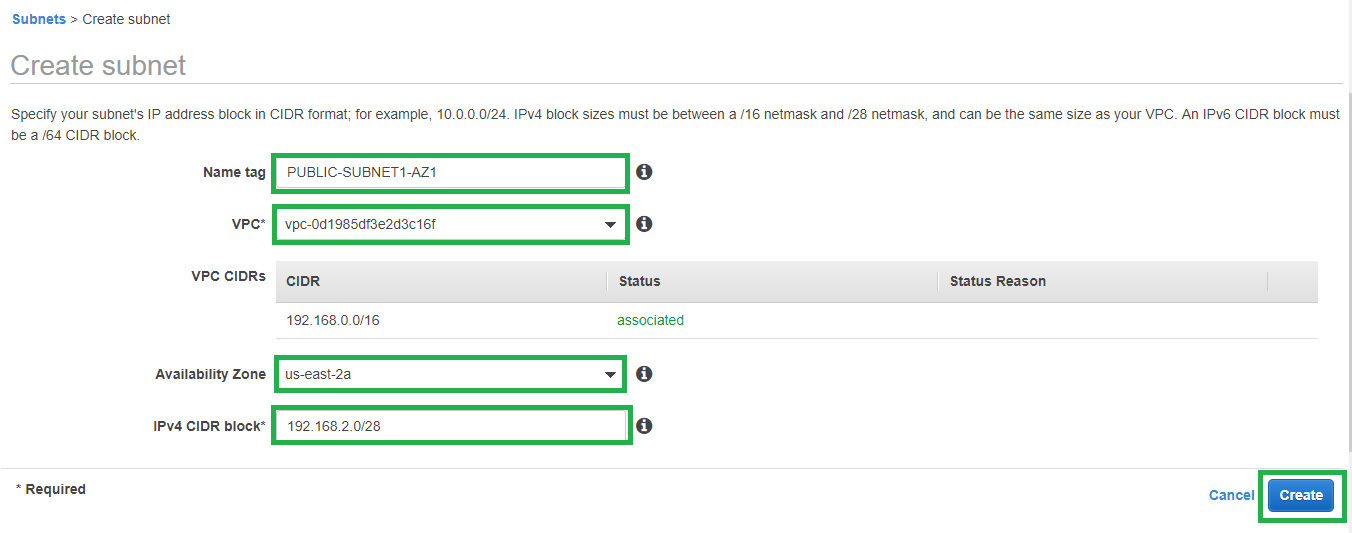


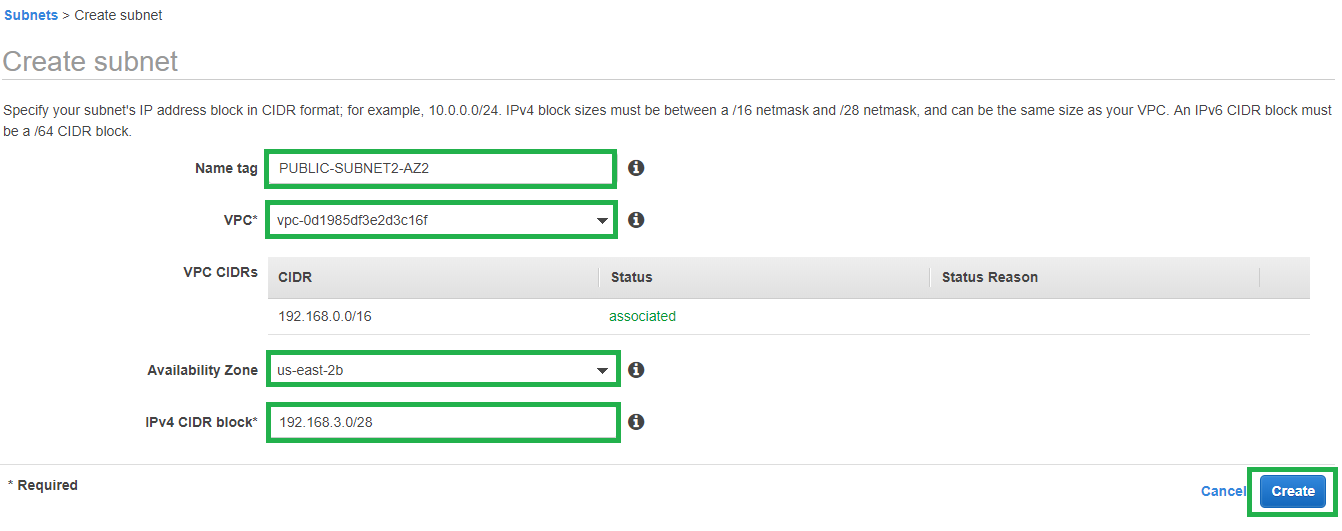
1. Provide Name for the subnet, select the New VPC that we created and select the Availability zone for the new subnet and provide Subnet’s CIDR block which should be within the VPC CIDR range.

In this Example we are creating 4 subnets 2 public and 2 private. So create all 4 subnets in the VPC. 1 private, 1 public in AZ 2a and 1 private, 1 public in AZ 2b

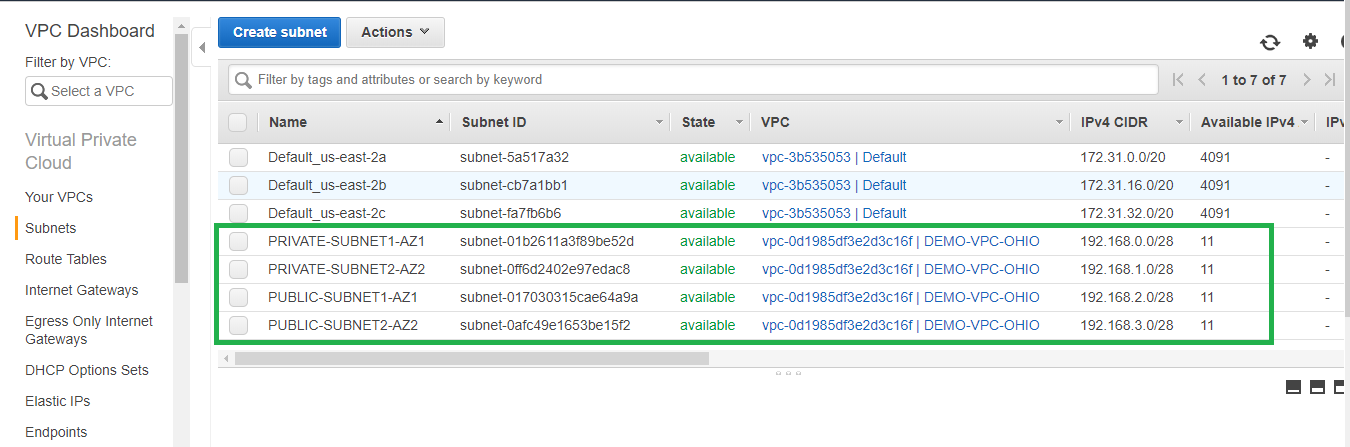




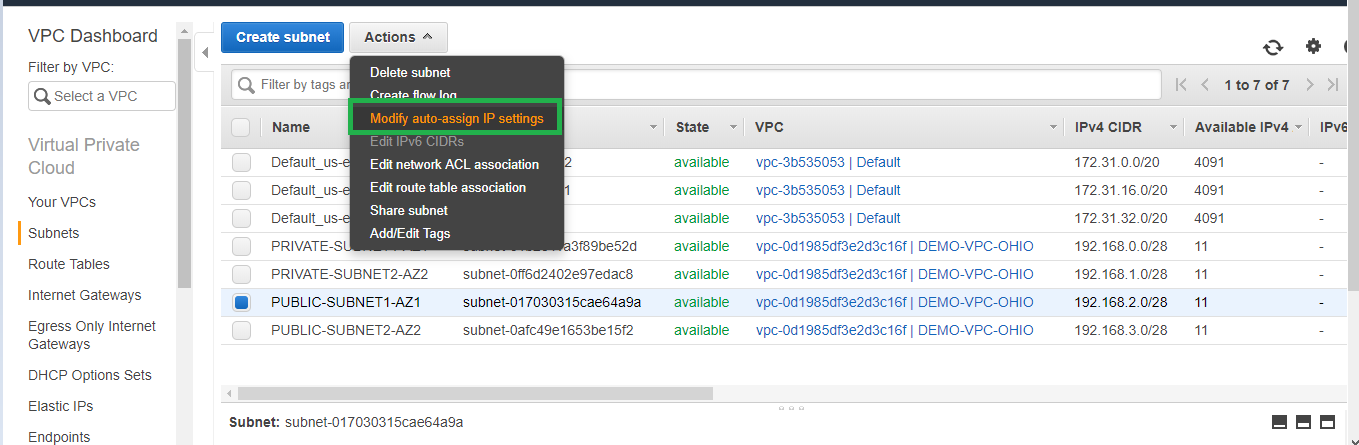


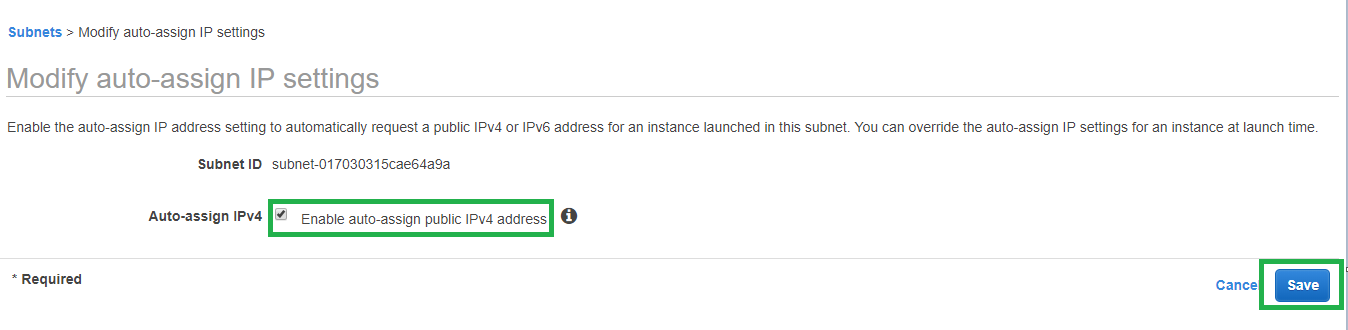


1. All 4 subnets are created in the new VPC.

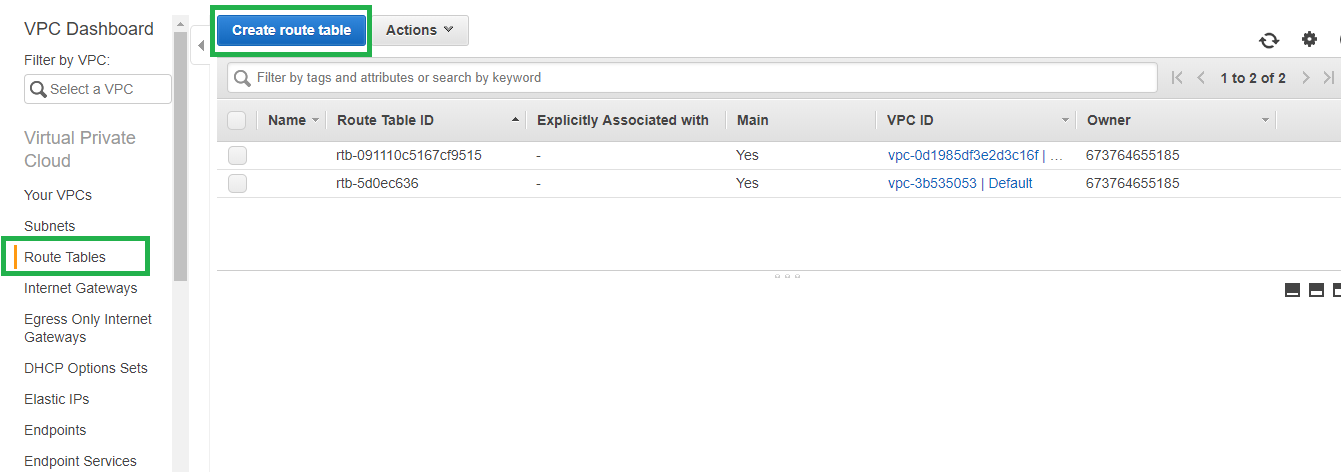


1. For the public subnets modify auto assign ip settings and enable.

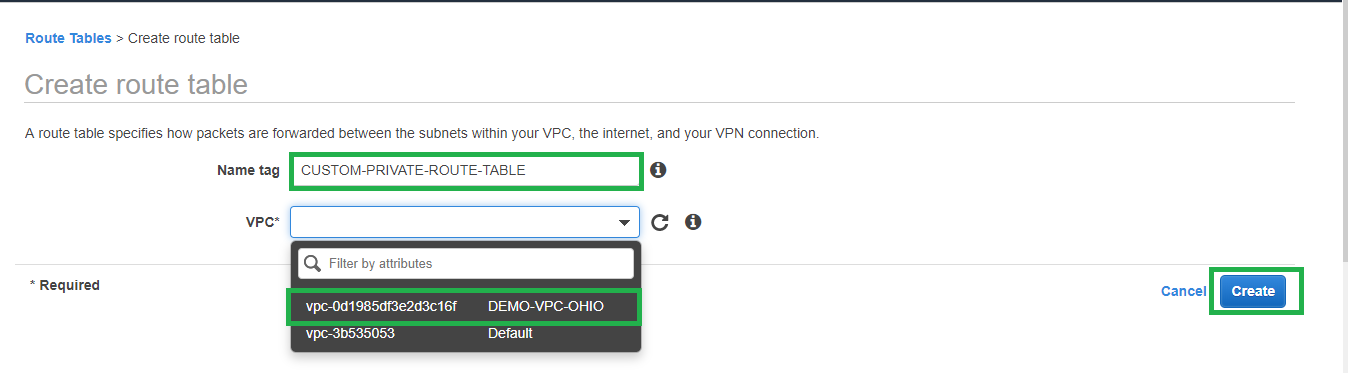


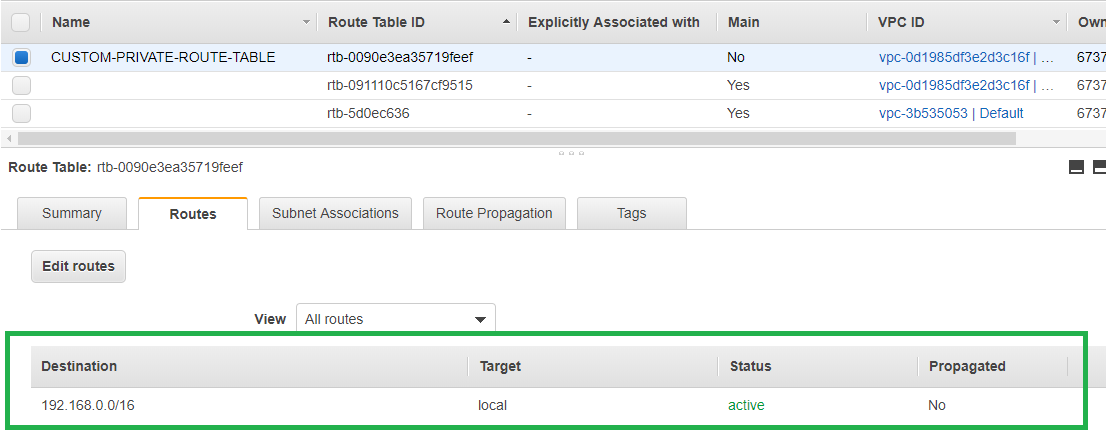


1. Create custom route tables for the private and public subnets.

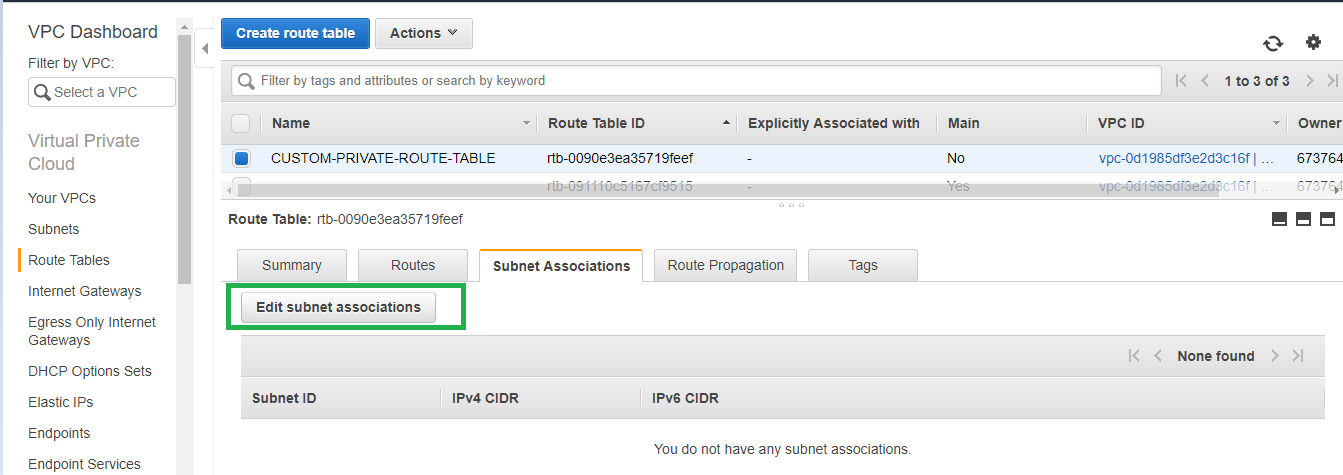


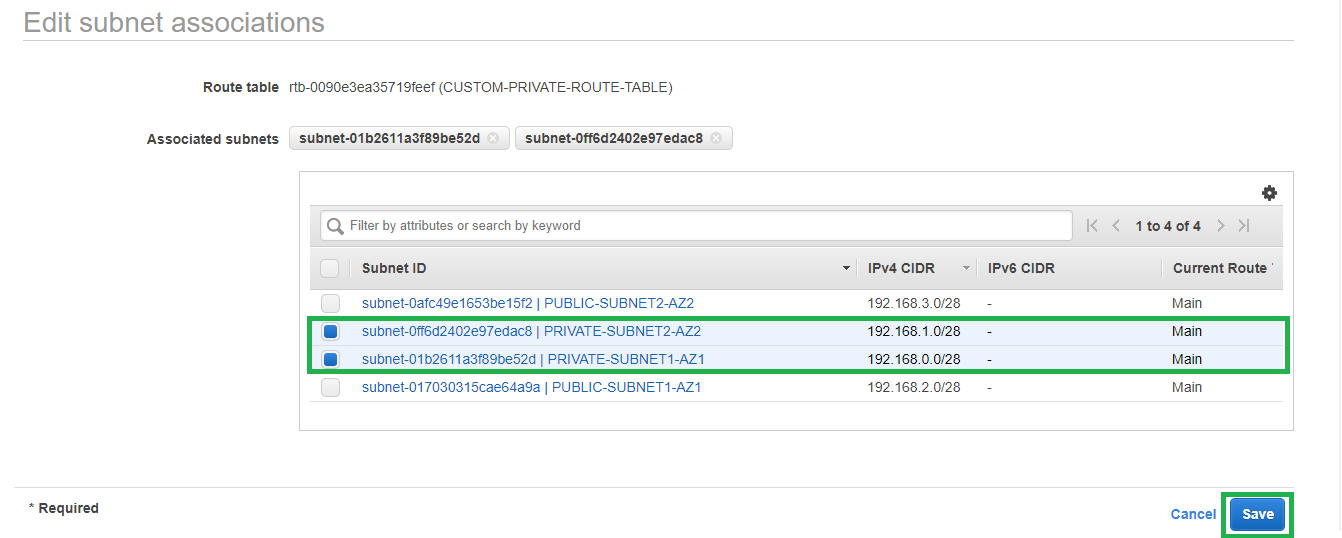
1. The private route table will only have local route table

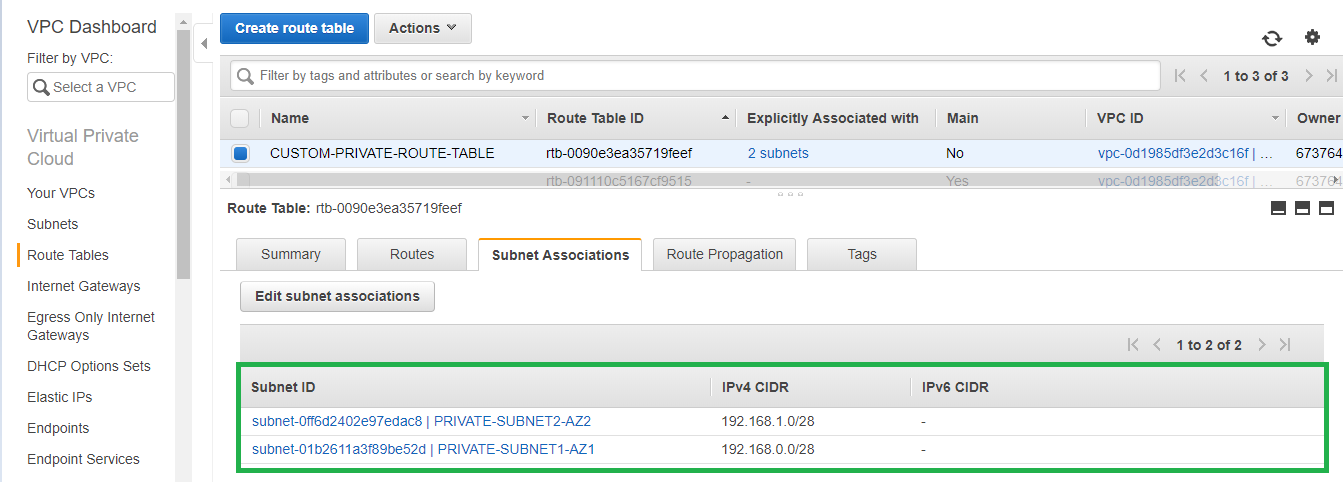




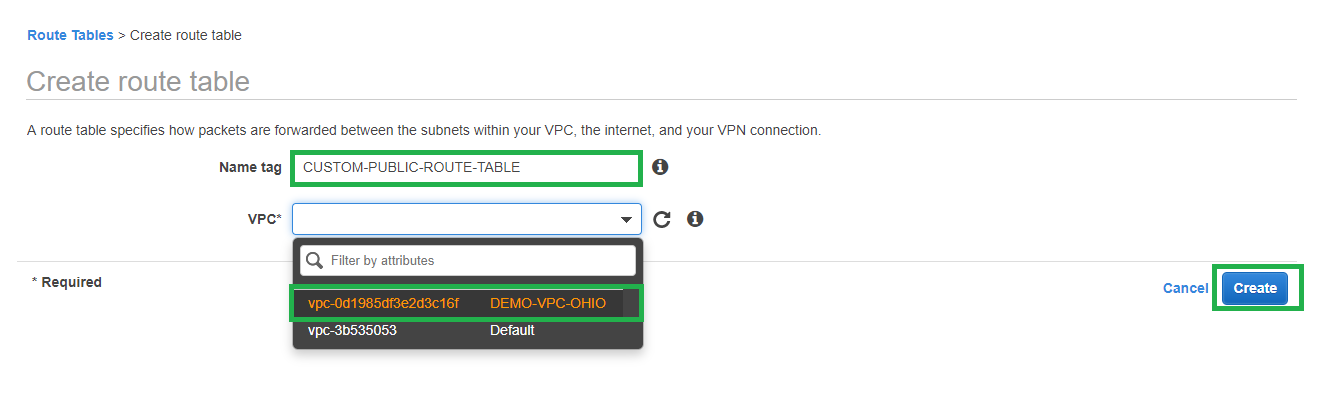
1. Associate the new custom private route table with the two private subnets created earlier.

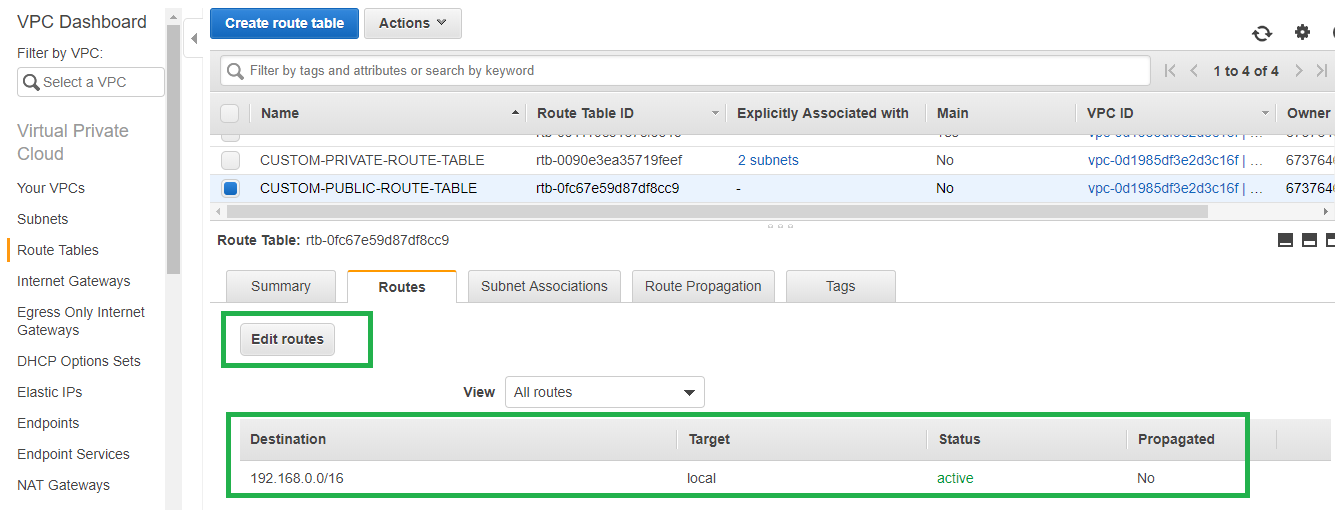




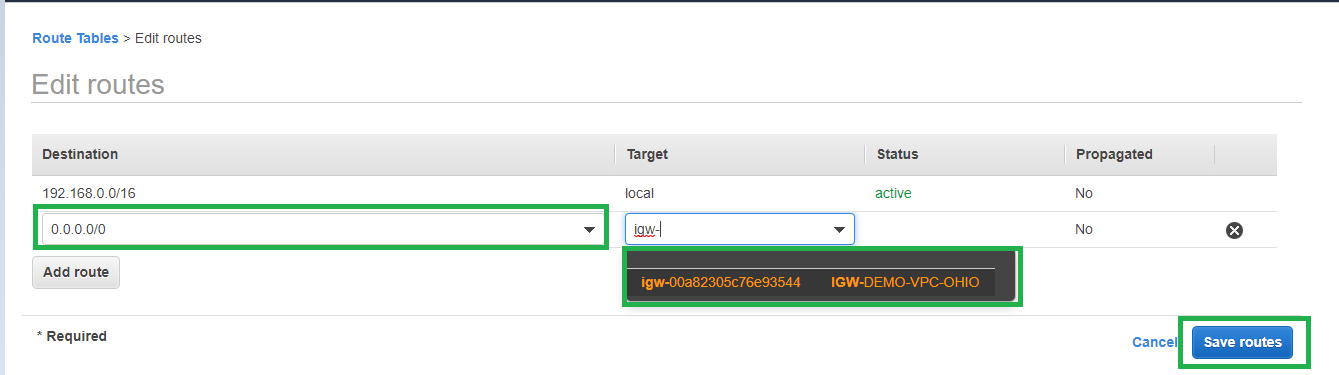


1. Create new Custom public Route table

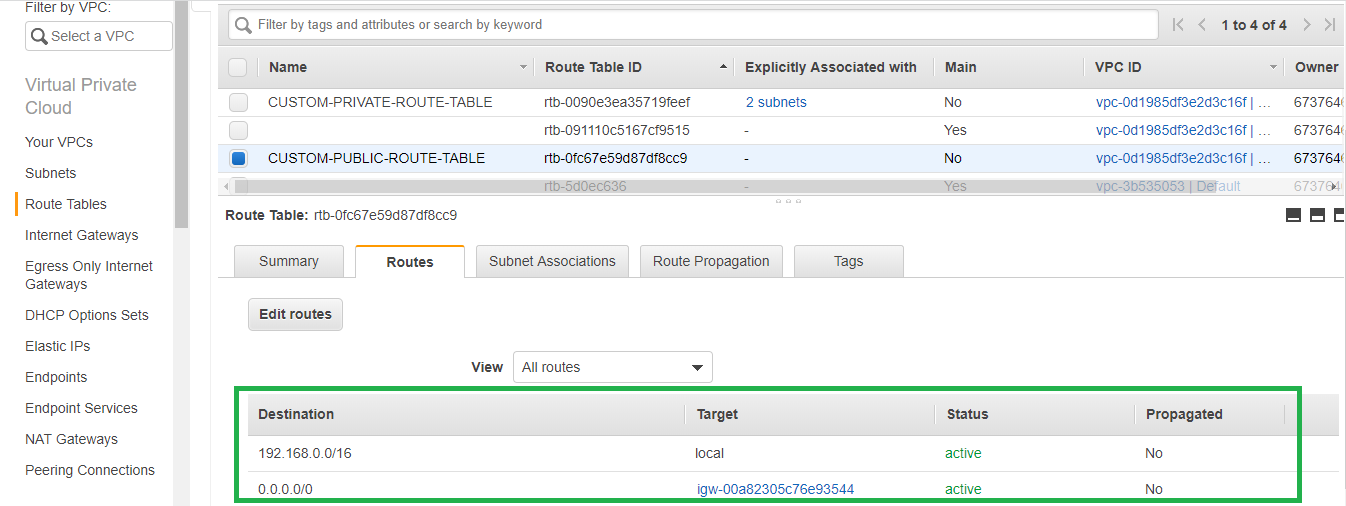


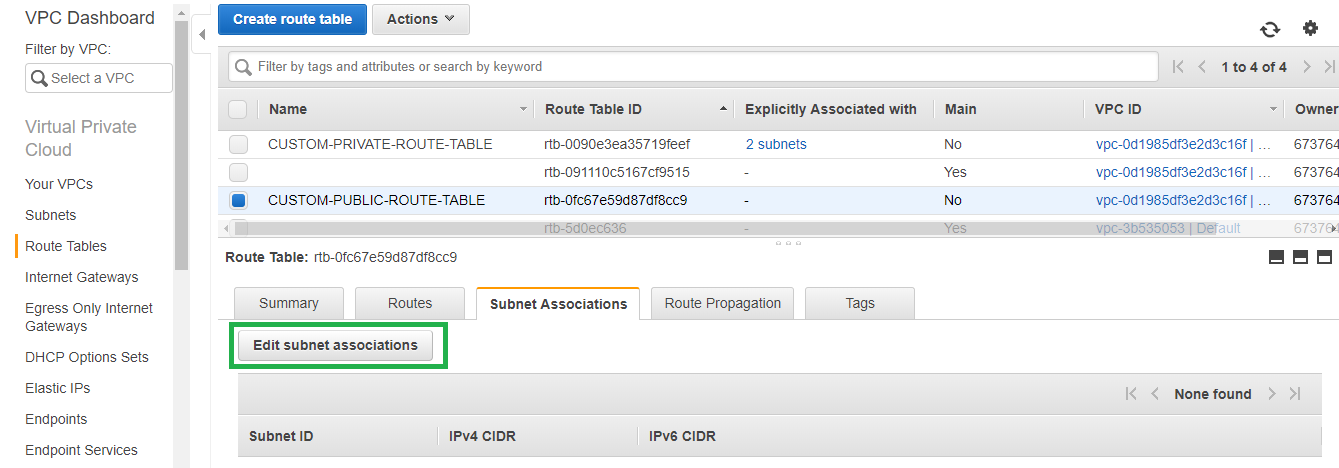


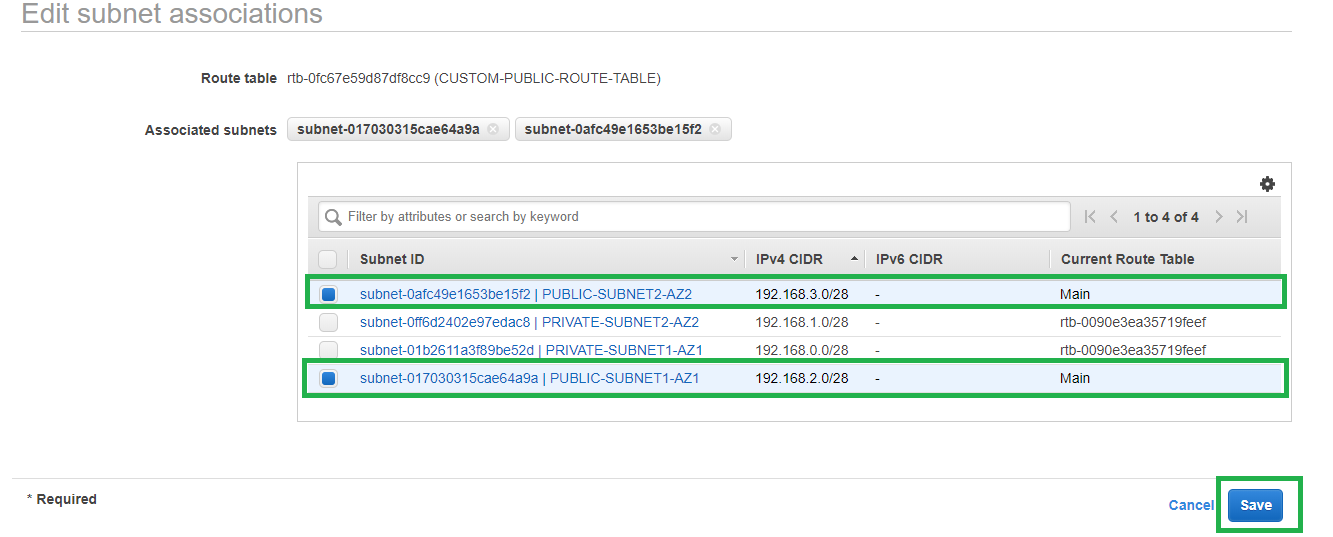
1. Edit the routes and add new route for Internet with the destination being 0.0.0.0/0 and target as Internet gateway. [Note: Only this route in the route table makes the associated subnet public. Without this route the subnet is private only]



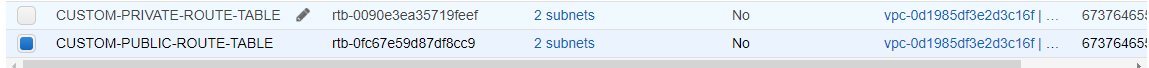
1. Associate the public subnets to the new custom public route table.



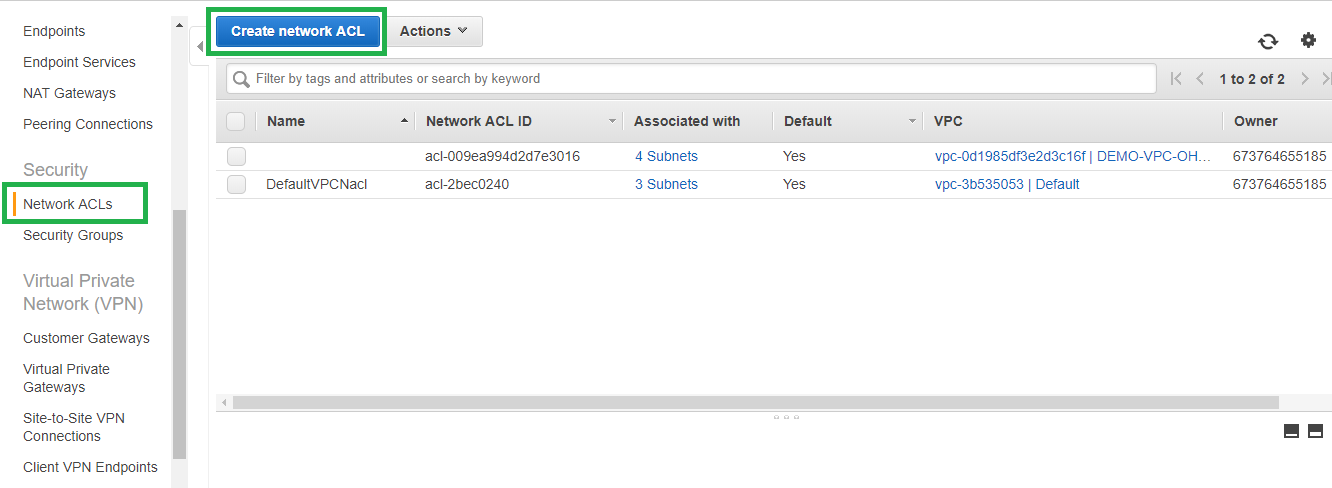




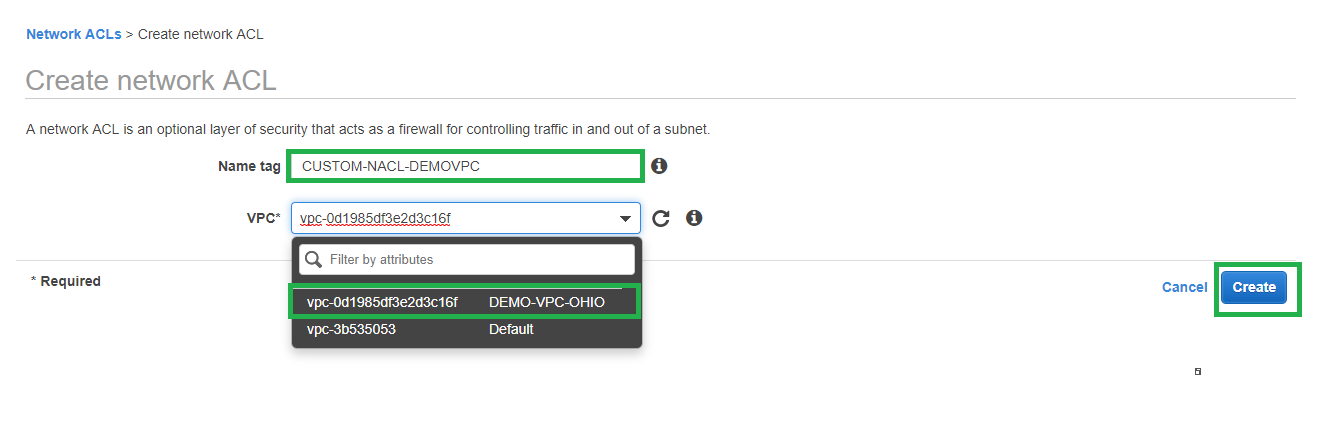
1. At this point we have created 1 New VPC with two private and public subnets in different Availability zones.



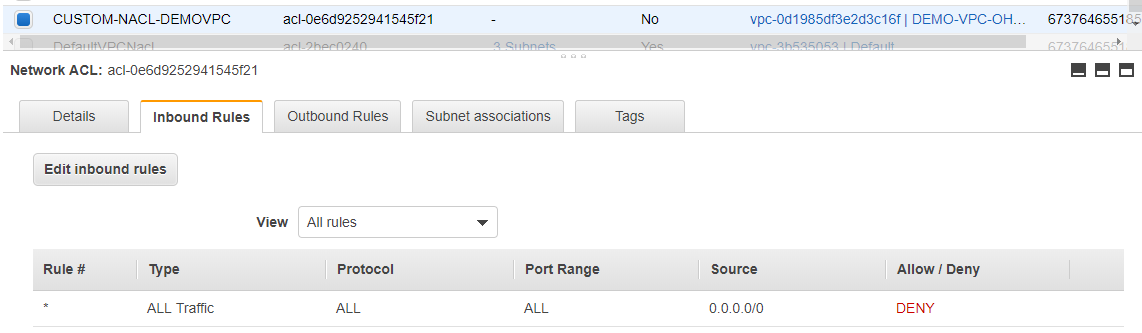
1. Create new Custom NACL for enhanced security for your VPC. [This can be skipped if you are using default NACL]

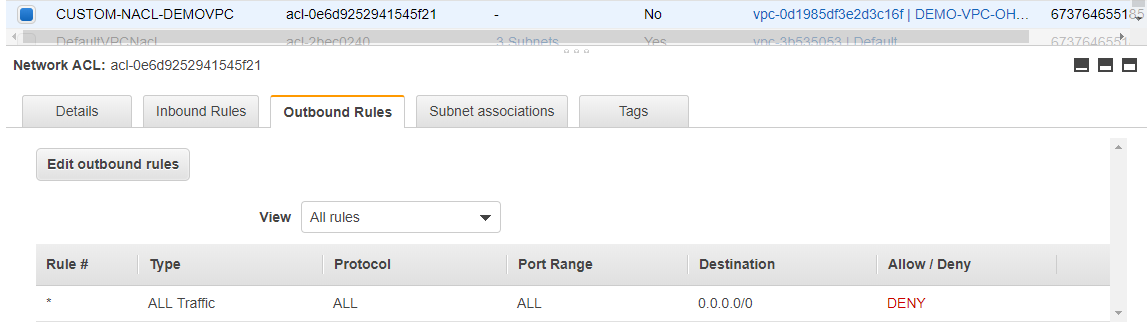


1. Create Network ACL and select the VPC

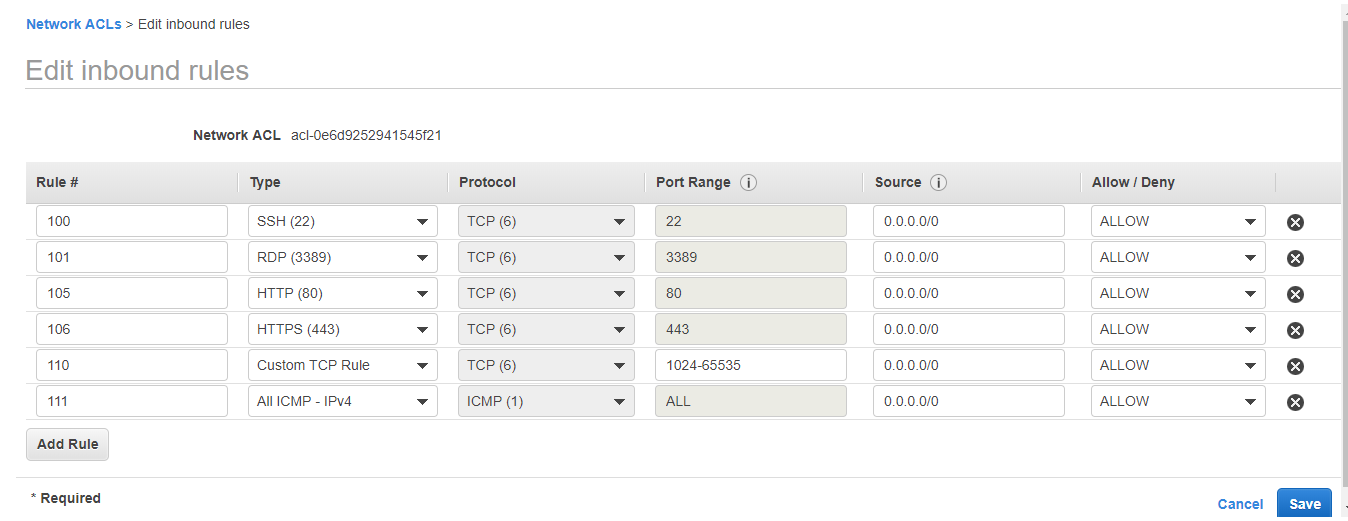


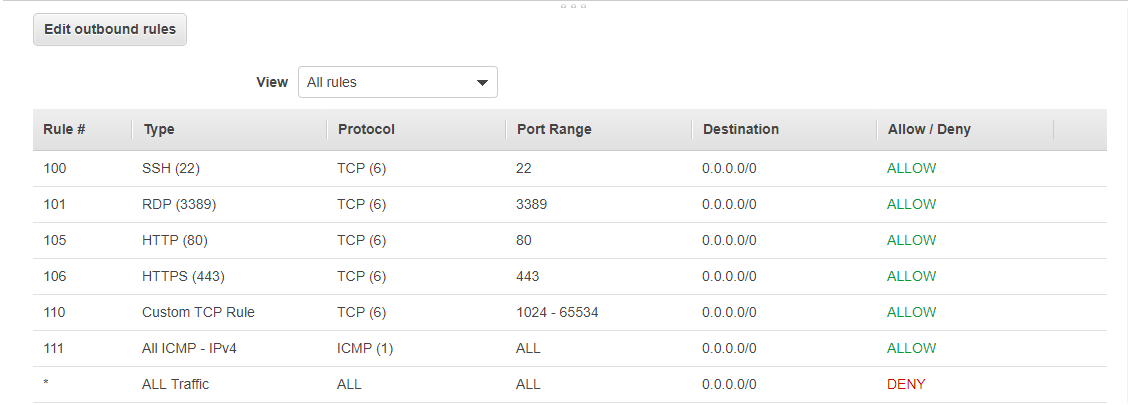
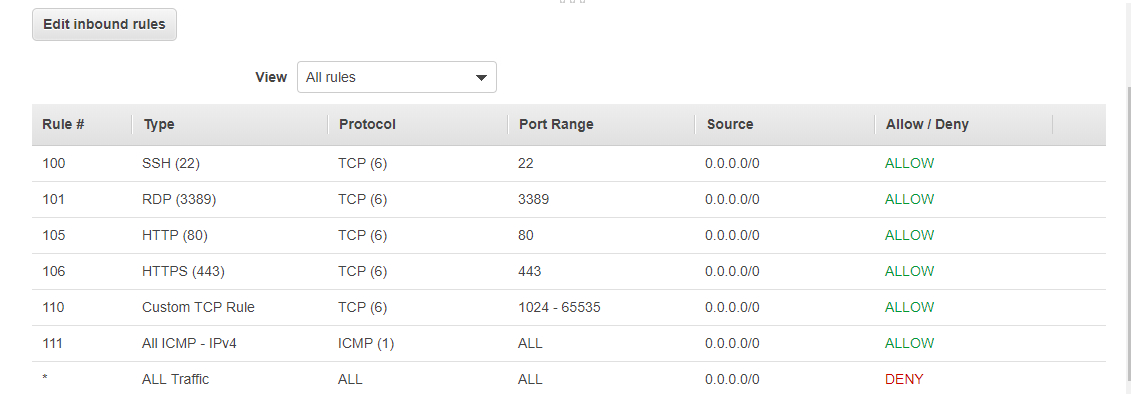
1. By default new NACLs deny all traffic inbound and outbound as seen below.

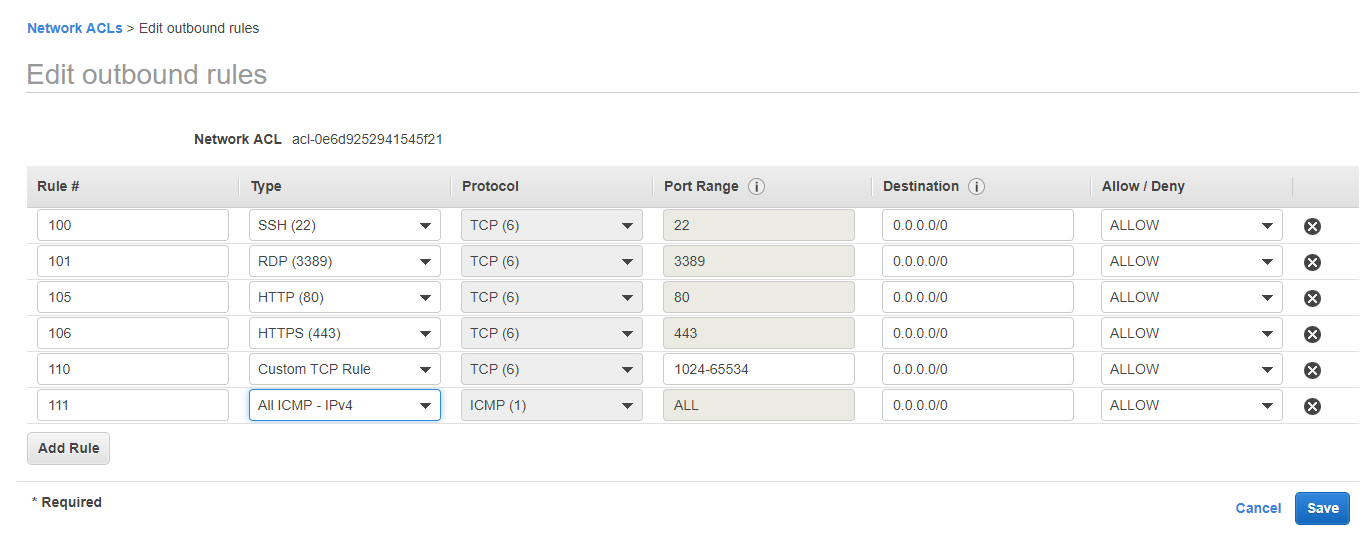


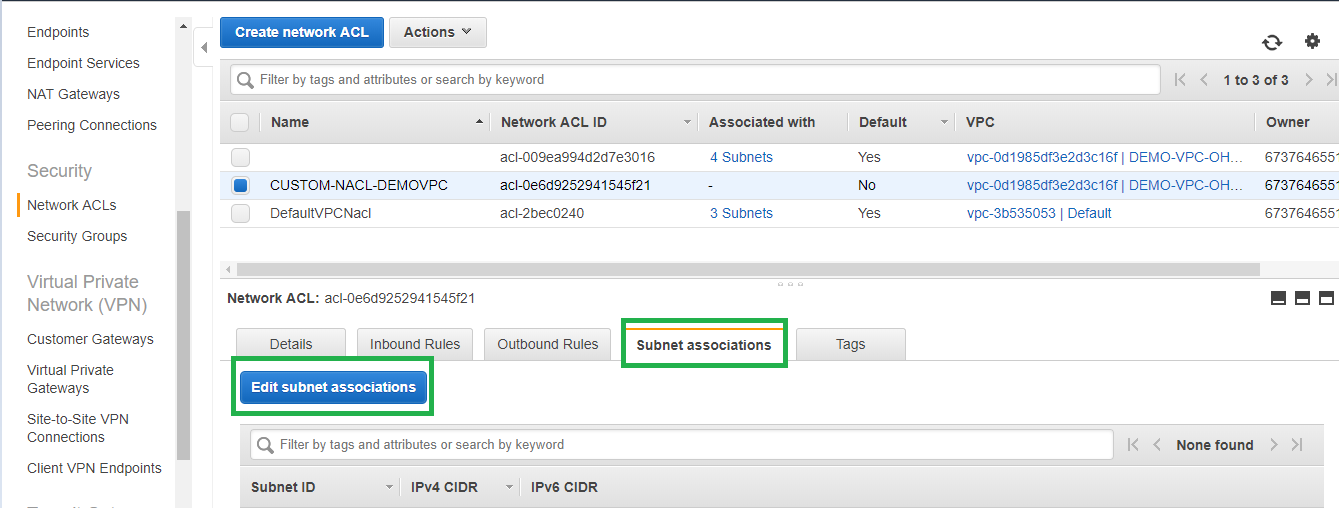


1. We need to allow traffic by adding custom rules as per our requirement. NACL being stateless requires both inbound, outbound rules to be defined with a priority. Ensure to use Ephemeral ports as NACL is stateless.

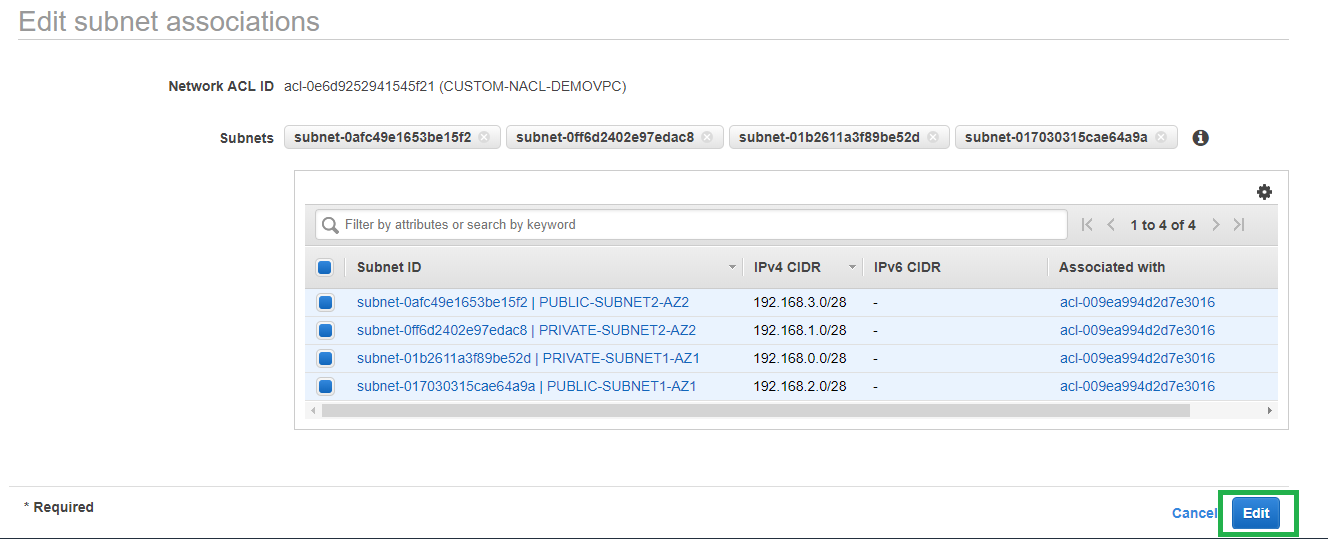




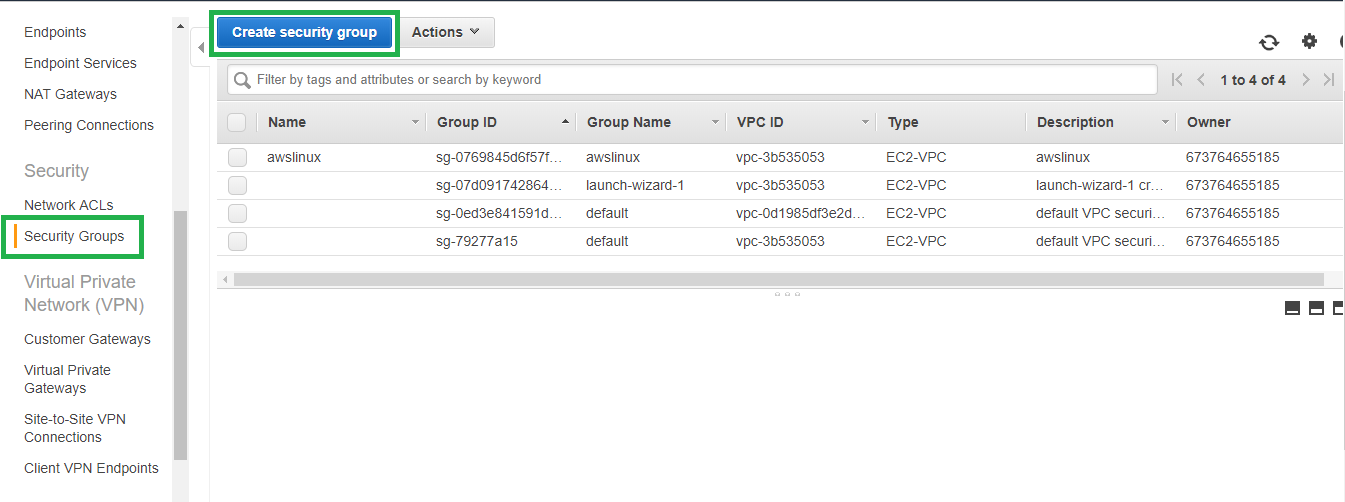


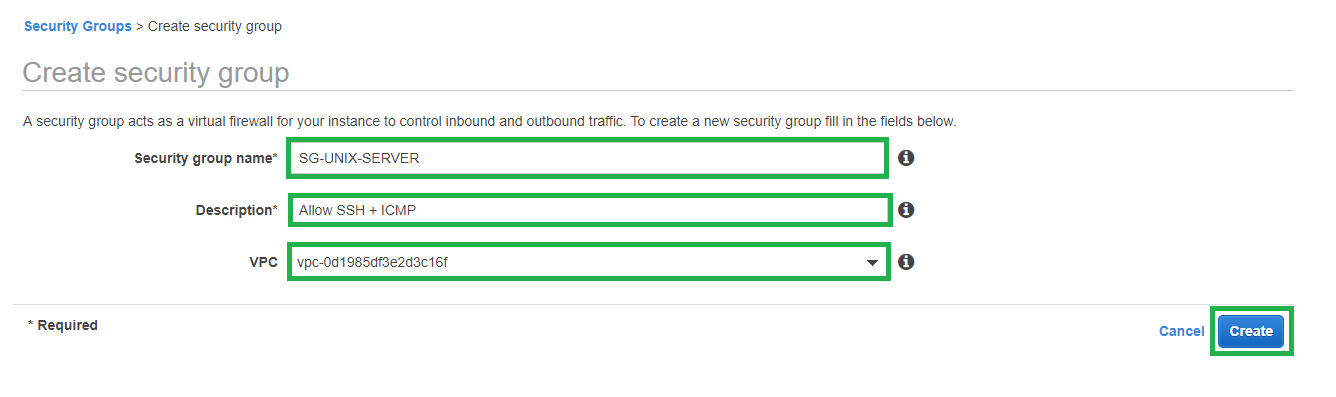


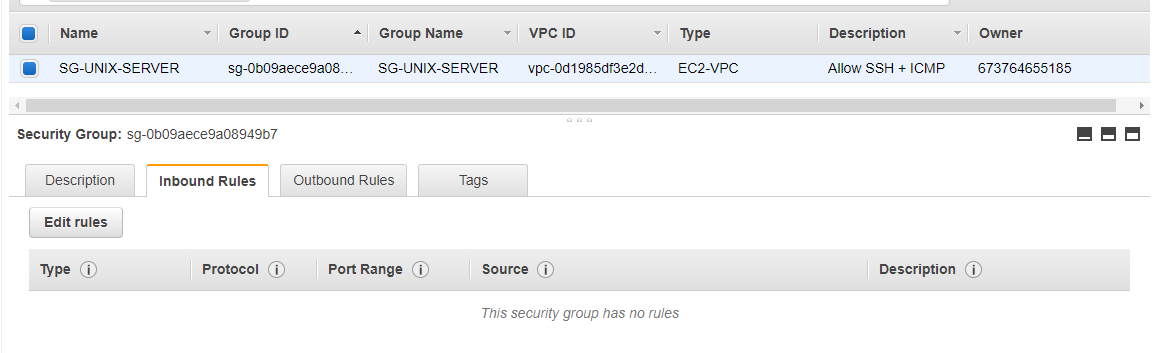
1. Associate the New NACL with our subnets, otherwise the subnets will be associated with default NACL.

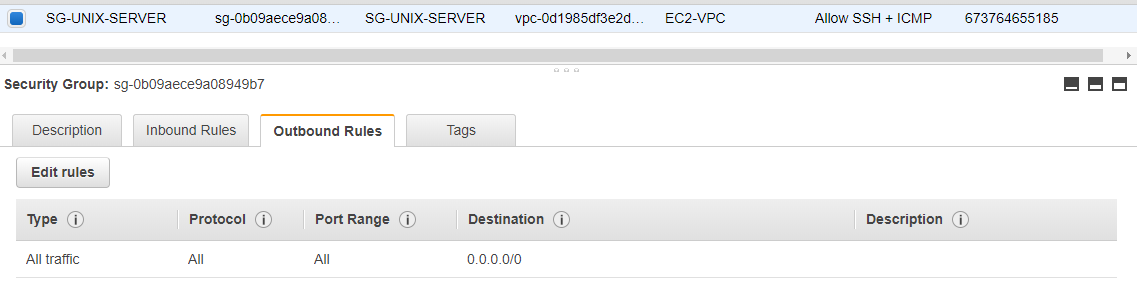


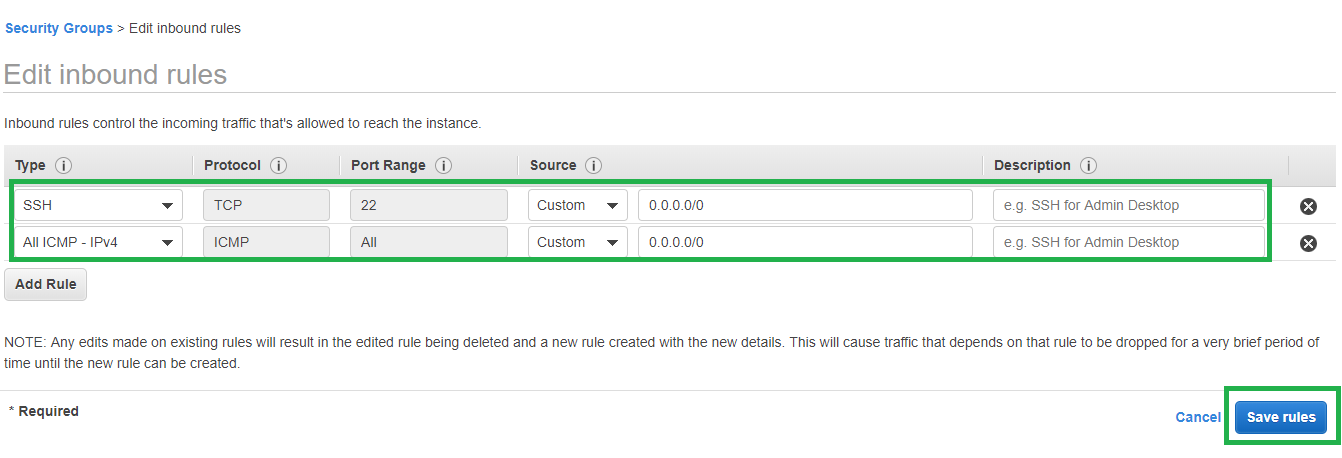
1. Create new Security Groups in the VPC that can be later used during instance creation.
2. In this example we are creating two security groups. One for UNIX allowing port Ssh [remote login] and icmp [for ping] & one for Windows allowing ports rdp [remote login] and icmp [for ping]. Note security groups are stateful.

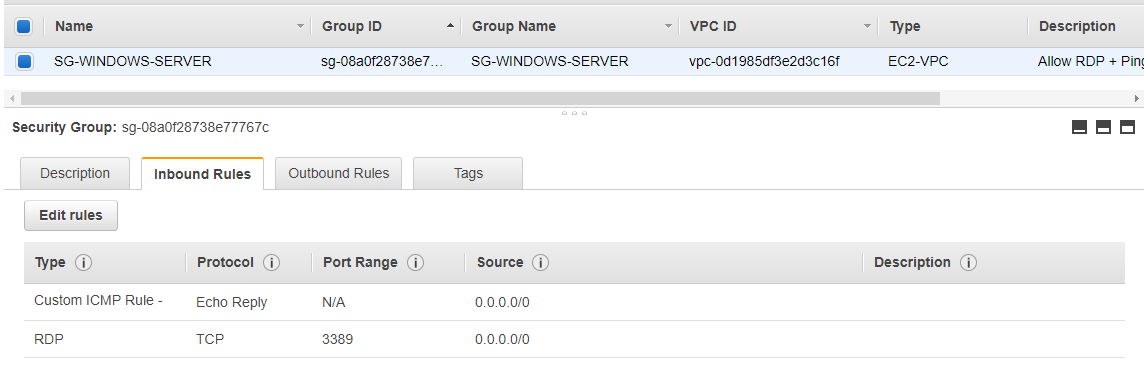












At this point our VPC is ready to be used. We can create new EC2 instances on the respective subnets. As nat gateway is not free version it has not been included in this demo. You can create Nat gateway in public subnet and modify private route table with destination 0.0.0.0/0 and target as nat gateway to allow outbound internet access for private instances. As an alternative demo a separate lab has been created for configuring NAT instance to provide internet access for private instances.