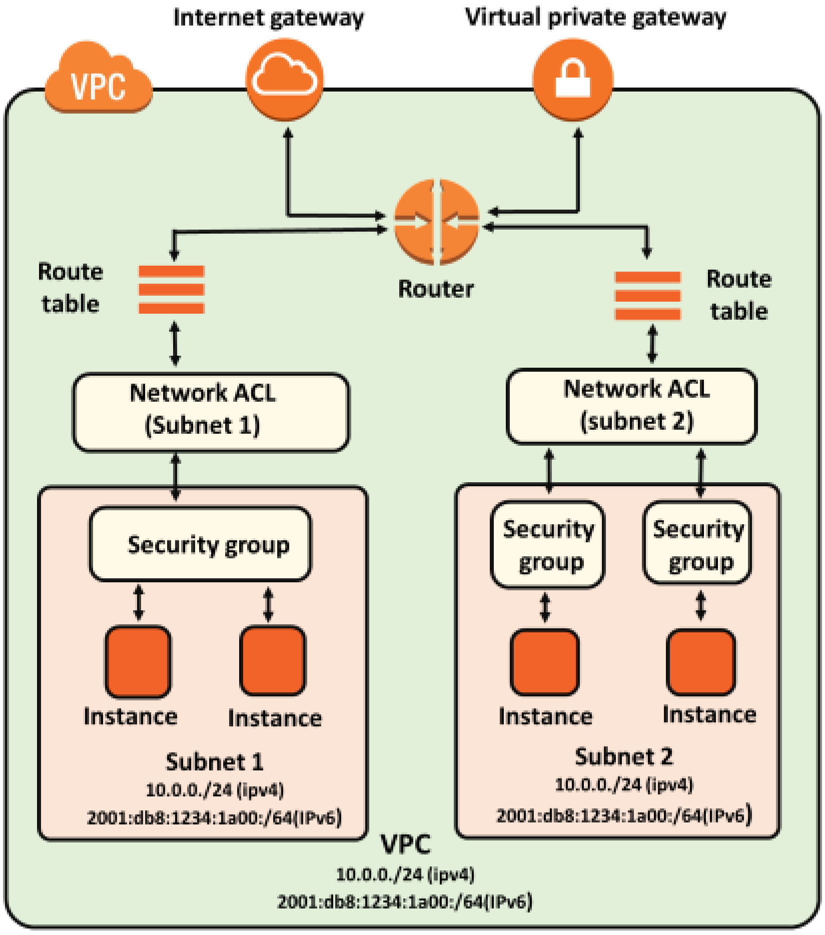
Lab 5:

Lab Scenario 1:

Apply Network ACL on Subnet 1 only and Test its working.



Lab Activities for Scenario 1

Task 1: Create a Custom VPC in an Availability Zone at one region and Create its all-necessary components such as Subnet, IGW and Route Table.

Task 2: Launch a window server free tier t2.micro in the public subnet only and allow all traffic

Task 3: Create a custom Network ACL and attach the subnet of default NACL.

Task 4: First, set the inbound rules in NACL such as 100 for RDP.

Task 5: Also set the outbounds rules in NACL such as 100 for HTTP and 200 for HTTPs.

Task 6: Check the Connection of server using RDP (Error will be there while connection)

Task 7: Go to Custom VPC NACL and Change the outbound rules as 250 custom TCP and open the port range 1024 to 65535 and Save.

Task 8: Connect again the RDP.

Task 9: Check the internet connectivity using CMD or Browser.

Task 10: If not connected to internet then also make the changes in the Inbound rules of the NACL

Task 11: Take the snapshots of all performed tasks and Merge with snaps of Lab scenario 2.

Video Link:

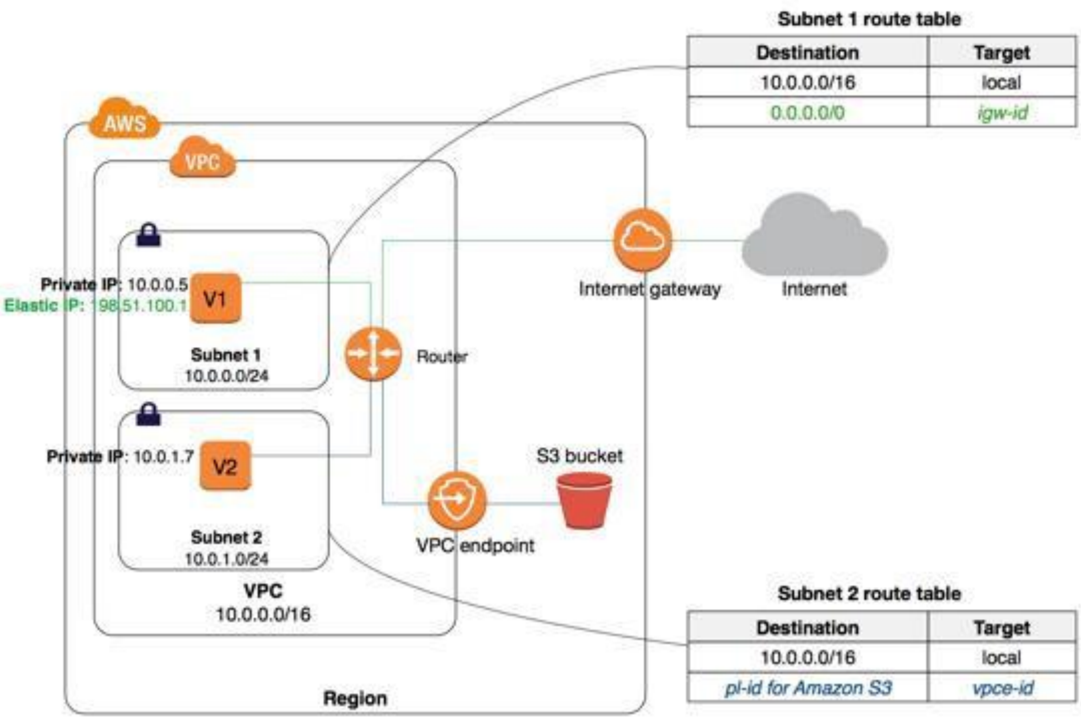
https://www.youtube.com/watch?v=IznTIXBIKl0&ab_channel=ITProGuide

Web URL:

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

https://www.javatpoint.com/aws-nacl-vs-security-group

Lab Scenario 2 (Access AWS Resource Using VPC EndPoints)



Subnet 1 route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Subnet 2 route table

Destination	Target
10.0.0.0/16	local
pl-id for Amazon S3	vpce-id

In this lab activity, you will create a VPC endpoint and an S3 bucket to illustrate the benefits available for our cloud implementations. VPC endpoints can be used instead of NAT gateways to provide access to AWS resources. Many customers have legitimate privacy and security concerns about sending and receiving data across the public internet. VPC endpoints for S3 can alleviate these challenges by using the private IP address of an instance to access S3 with no exposure to the public internet**.**

Lab Activities:

Task 1: Create VPC by creating 2 subnets in it (one private and one public). (Other components IGW, Route Tables will also be there)

Task 2: Launch two EC2 Linux server in the subnet one for one. (The SSH rule will be anywhere)

Task 3: Create a VPC Endpoint and associate it in private subnet.

Task 4. Select the S3 Service.

Task 5. Verify VPC Endpoint Access to S3

Task 6. Check the route table to make sure you see a route using the VPC endPoint to S3.

Task 7. To verify, SSH into the public instance.

Task 8. SSH into the private instance.

Task 9. Check the accessibility of the AWS resources privately and confirm that the S3 buckets is in our environment.

Task 10: Take the snapshots of all performed tasks and merge with Lab scenario 1 snapshots. Then create a doc/pdf of your enrolment number_lab05(Ex: E18CSE072_Lab05) and upload the file on LMS.

Web Link:

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

https://aws.amazon.com/premiumsupport/knowledge-center/create-vpc-endpoint/

https://networking.workshop.aws/lab4/lab4-vpcendp.html

YouTube video Link:

https://aws.amazon.com/premiumsupport/knowledge-center/create-vpc-endpoint/