**VPC - Virtual private cloud**

VPC allows us to create an isolated network in the cloud. We can have complete control on our resources that are being launched in vpc. We can define our own VPC cidr block, Subnet range, custom nacls which also allows to deny traffic (black list ips).

**Route Table**

A route table contains a set of rules, called routes that are used to determine where network traffic is directed. Each route in a table specifies a destination CIDR and a target

Why public subnet

A public subnet is typically for resources that require ingress(Inbound) and/or egress(Outbound) to the public internet

If a subnet's traffic is routed to an Internet gateway, the subnet is known as a public subnet.

**What is public subnet?**

If a subnet has a route with the destination (0.0.0.0/0) and Internet Gateway as the target, the subnet is known as a public subnet

Public subnet Ex: A common use case for this is a DNS server, and a load balancer sitting in front of front-end webservers or web applications.

The new subnet will be deployed into the selected VPC, and into the selected Availability Zone.

**Private subnet**

If a subnet doesn't have a route to the Internet gateway, the subnet is known as a private subnet. Instances launched in a private subnet do not have publicly routable internet addresses either.

Both subnets have a route table associated with them. Instances on the public subnet route internet traffic through the internet gateway.

\*\*\*\*The private subnet routes internet traffic through the NAT instance.

Next you will need to setup the route table.

A route table contains a set of rules, called routes, that are used to determine where network traffic is directed. Each route in a table specifies a destination CIDR and a target

**Steps to create a VPC**

1)**Create a vpc**

Give a CIDR Block as 10.0.0.0/16

Everything leave as default

2) **Create an Internet Gateway**

Once the internet gateway has been created, It is dettached which means it is not attached to any vpc, attach the IGW to our VPC.

3) **Create a Subnet**

Define the range of a subnet as 10.0.7.0/24

Assocaite the subnet to any of the availability zone

As subnet by default get's associated to a route table, create your own route tables other then the main route table which was created while creation of vpc.

4) **Create Route Table**

Private Route Table

The route table i.e is created will have a route to local, hence it is considered as a private route label

Public Route Table

The route table which has route to the internet is identified as public route table, To have a route to internet, Associate Internet gateway, Ensure you've

**NACL's**

NACLs are stateless. NACL is better suited for a private subnet than a public one. (For public subnets, using security groups is recommended without NACLs.)

The VPC comes with a modifiable default network ACL and each subnet must be associated with a network ACL. If you do not explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL that allows all inbound and outbound traffic:

By default, a network ACL is not associated with a subnet until you explicitly associate it with one. Next you will associate a subnet with a network ACL.

Each instance launched in either subnet has it's own security group with inbound and outbound rules, to guarantee access is locked down to specific ports and protocols.

For example, private instances on the private subnet allow any outbound traffic, but only allow SSH access from the bastion host

In addition to security groups, the private subnet also has a network access control list (NACL) as an added measure of security.

**NAT Instance**

A NAT instance enables instances in the private subnet to initiate outbound traffic to the Internet. This scenario is common when you have a public-facing web application, while maintaining back-end servers that aren't publicly accessible.

A common example is a multi-tier website, with the web servers in a public subnet, and the database servers in a private subnet. You can set up security and routing allowing the web servers to communicate with the database servers. The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet cannot. The instances in the private subnet can access the Internet via the NAT instance in the public subnet

**Points to remember - vpc**

You cannot attach more than 1 internet gateway to a vpc

You can create 5 Elastic IP addresses per region

you can create 200 subnets per VPC

you can create 200 Route tables per VPC

You can create 5 Internet gateways per region

You can create 500 Security groups per vpc

EC2 ( previous class Lab)

**Try User Data on EC2**

#!/bin/bash

yum install httpd -y

yum update -y

service httpd start

chkconfig httpd on

echo "<html><h1>Hello !</h1></html>" > /var/www/html/index.html