.....VPC.....

Select Mumbai region

Step 1: Create VPC   (MyVPC) - 10.0.0.0/16
Step 2: Create two subnets

subnet1 - 10.0.1.0/24 - WebSN (Public Subnet)
subnet2 - 10.0.2.0/24 - DbSN (Private Subnet)

Step 3: Enable public IP to subnet1

Step 4: Create Internet Gateway attach to VPC -- MyIGW
Step 5: Create Route table -- InternetRT
Step 6: Attach Route table to subnet1
Step 7: Attach Route table to Internet Gateway
Now, subnet1 is public.

++

Now, Lets launch webserver in public subnet.
Services ---Ec2 ---- Launch instance -- Step3 Network : MyVPC
                                          Subnet: 10.0.1.0/24

Additional Details -- User Data

```
#!/bin/bash
sudo su
yum update -y
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1> Welcome to the info-dell! </h1></html>' > /var/www/
html/index.html
```

Next -- Next -- Name Tag: WebServer   ---> Next -- Security
Group : WebSG01 , Description: WebSG01

ADD RULE

Type	Source
SSH	Anywhere
HTTP	Anywhere

Review and launch --- Launch -- Download keypair --> (webKP19.pem)
Launch-- View Instance

++

Lets Launch Database Server in Private SUbnet.

Services ---Ec2 ---- Launch instance -- Step3 Network : MyVPC
Subnet: 10.0.2.0/24

Name Tag: DbServer -- ---> Next -- Security Group : DbSG01 ,
Description: DbSG01

Change Type   from SSH to MYSQL/Aurora

Type	Source	
MYSQL/Aurora	Custom	10.0.1.0/24

(MySQL Port is open to entire subnet)
Review and launch -- Launch --> Create new keypair --> (test.pem)
launch instances --- View instances

++

Now, web server can pull data from database server.

++

DBA wants to create some files. Wants to perform maintenance activity.
Can he connect?
As DB Server is not having public IP and it is not having internect connectivity, DBA cannot connect.

For this, we need to create Bastion-host-host server/ Jump server in public subnet
It is noting but normal EC2 Machine

Services -- EC2 -- Luanch -- Amazon Linux ---> select VPC , Select subnet

Name: Bastion-host-hostServer
Security Group: Bastion-host-hostSG01
Description: Bastion-host-hostSG01

(SSH port -- should be open to myself)

Type	Source
SSH	My IP

Review and launch -- launch -- Create new keypair ---test.pem

View Instances

++

Now, Only I can connect to Bastion-host-host server through SSH

From the Bastion-host-host server, I should able to jump into Dbserver.

That means, DbServer SSH port should be open to Bastion-host-host server.

Goto Dbserver security group - DbSG01 (new tab)
Select DbSG -- Inbound --Edit
Add Rule

Type Source
SSH Custom 10.0.1.144/32 (Private IP of Bastion-host-host server)

Save.

Now, Lets test can we connect to DB server

In EC2 Dashboard -- select Bastion-host-host server -- connect
copy user@public_ip

Open putty
Host Name - user@public_ip
Provide PPK file -- Connect!
$ sudo su
# yum update -y

From Bastion-host-host-- we need to jump to dbserver

Now, to connect to DBserver, we need to enter the details to DBserver in Bastion-host-host server.

Select DbServer --- connect

Copy the entire ssh command.

As we are connecting from linux to linux .pem file is required.

Enter the ssh command in putty.
eg:
ssh -i "test.pem" ec2-user@10.0.2.249

Note: To connect the .pem file need to be present in present working

directory.

Now, we need to copy test.pem file in Bastion-host-host server.
It is there in our windows machine.

We will use FileZilla or WINSCP to transfer the file from windows to linux

In google search for "FileZilla" "WinSCP"

https://filezilla-project.org/download.php?platform=osx

https://winscp.net/eng/index.php

download and run.

Open FileZilla or WINSCP
We will connect to Bastion-host-host server using FileZilla or Winscp
host name: user@ipaddress
advanced ---Authentication --- private key file - select the ppk file -- open -- ok - login

Now, drag and drop the .pem file to Bastion-host-host server.

In Putty
ls   (We should able to see the file)

Now connect to Dbserver by running the SSH command
ssh -i "DbKP7.pem" ec2-user@10.0.2.106

You are now connected to DBserver!!!

Now, In DB server, lets execute the following commands
$ sudo su
#

Now I want to upgrade the latest version of MYSQL database

Command to upgrade MYSQL database
yum install mysql -y

not successfull.
We cannot install, As we are not having internet connection to private subnet.

TO get internet connection, we create NAT server. (Network Address Translator)

The purpose of NAT is to provide internet to private subnet.
We need to create NAT in public subnet.

In VPC Dashboard

NAT Gateways --> Create NAT Gateway (myNAT)
subnet: 10.0.1.0/24
Create new EIP ---> Create a NAT Gateway -- Close
NAT needs 2 min approx to get created.
Name it as NAT

++

What is Elastic IP ?
It is similar to Static IP
When we stop and start the EC2 Machines, public IP will change.

If you stop and start the machine, we you want the same public IP, then we create Elastic IP
Elastic IP is nothing but static public IP

Why do we need Elastic IP to NAT?
If incase NAT is down, entire private subnet will not get internet.
Then we restart the NAT again, then it acquire new public IP
When NAT acquire new public IP, there could be connection issue.
So we need Elastic IP to NAT

++

NAT is a closed box. It does not have any ports concept.
So, No one can connect to NAT.

We cannot connect NAT to private Subnet.
So, we create RouteTable.
One end of RouteTable , I connect to NAT.
Another end of RouteTable, I Connect to private subnet.

Instead of creating new RouteTable, we can use default RouteTable which was created, when we created VPC

Lets change the name of default RouteTable to NatRT
Select NatRT -- Subnet Associations -- Edit subnet Associations -- select private subnet-- save

Select NatRT -- Routes -- Edit Routes --Add Route -- Target: NAT Gateway (Select NAT)
Destination- 0.0.0.0/0 -- Save routes -- close

Now, lets test are we able to get internet to our DBServer.

Run the same command in putty again

```
# yum install mysql -y
```

It Works!!

++

Network ACL (NACL)

Security group will provide security at instance level

NACL will provide security at subnet level.

Creating NACL

Select Network ACL ---- We have two default NACL
One for default VPC
One for MyVPC
(So, whenever we create new VPC, by default NACL is created automatically)

We will create a new NACL and attach to public subnet

++

Create Network ACL -- Name Tag: PublicNACL
VPC: MyVPC
Create
Subnet Associations -- Edit subnet associations --select public subnet
Edit

++

Now, try to access the webser
We cannot get the webpage !!! No

We need to open ports at NACL
Inbound rules ---- Edit inbound rules --Add rule

Rule#	Type	Source	
100	SSH	183.83.39.215/32	(My laptop IP,we can get it from Bastion-host-host-host security group)
200	HTTP	0.0.0.0/0	(HTTP open to all)

Save.

Now, try to access the webser
We cannot get the webpage !!! No

We need to know about statefull and stateless

Lets select webSecurity group -- Inbound tab -- edit

Did we add ports in outbound tab?

In security group, when we open inbound port, by default outbound port is open to all.
This status is called statefull.

So, we have opened HTTP incoming, by default outbound port is open to all.
Hence, we are able to access webserver.

This status is called statefull.

++

For NACL , The case is different.
We need to open outbound port to NACL explicitly.
So, NACL is stateless

Select NACL -- Outbound Rules --- Edit Outbound Rules --- Add Rule

Rule	Type	Destination
100	SSH	183.83.39.215/32 (MY IP)
200	HTTP	0.0.0.0/0

Save

Now, can we able to access webserver
No!!!

Ephemeral ports

Total Range of ports : 0 to 65535
Range 1024 - 65535 are the range of ephemeral ports

search in google "ephemeral ports in AWS" , we can see the range

Assume in public subnet, we have 100 webservers
All are connected to load balancer.
If hacker blocks any http port on 1 webserver
Will it be a problem?
No!!
As load balancer will send the request to other servers.

If hacker blocks any http port on NACL level (subnet level)
Entire website is down.

To avoid this problem, AWS is providing range of ports (1024 - 65535)

We need to open this range in NACL level,
So when hacker blocks a particular port (HTTP), AWS uses a random port from the range.
AWS will replace the random as HTTP port.

So that website will never godown.

Note: Ephemeral ports are mandatory at NACL level

++

Select -- PublicNACL --- Inbound -- Edit inboud rules -- Add rule

Rule	Type	port range
300	Custom TCP Rule	1024-65535

Save.

Now, can we able to access webserver?
No!!

NACL are stateless. We need to open ports in outbound level also.

Select -- PublicNACL --- Outbound -- Edit outboud rules -- Add rule

Rule	Type	port range
300	Custom TCP Rule	1024-65535

Save.

Now, can we able to access webserver?
Yes!!

++

WHat is the use of NACL?

Select our NACL -- inbound rules

Rule	Type	
200	HTTP	we have opened to all.

Add Rule

Rule#	Type	Allow/ Deny
201	HTTP	Deny

Save.

Similarly

Select our NACL -- outbound rules

Rule	Type

200 HTTP we have opened to all.

Add Rule Type Allow/ Deny
201 HTTP Deny

Save.

Now, Are we able to access webserver?
Yes!!!
Conclusion, Lowest rule# will have highest priority.

Now, in inbound rules
Rule# -- 201 change to 199.
Save.

goto outboud rules
Rule# -- 201 change to 199.
Save.

Now, Lowest rule# is 199 which is deny.
so, we cannot access the webserver.
No!!

Usecase:

++

Hacker is continuous accessing the webserver.
We want to block his IP, but other customers should be able to
access the webserver.

How can we do it.
Lets Assume, I am the hacker
Now, in inbound rules , change the source

Rule# Source
199 183.83.38.112/32 (My laptop IP)

Save.

(Network team will give us incoming request IP address)

Similarly in outboud rules also

Rule# Source
199 106.217.195.229/32 (My laptop IP)

Save.

Now, Are we able to access webserver
No! (As it is blocked to my machine)

But, others can able to access the webserver.

Imp Usecase: By using NACL, we can block specific IP address

Now,
Lets delete Rule# 199 from inbound and outbound level.
Save.

Now, Are we able to access webserver
Yes!!!

NACL is not recommended to use for private subnet.

++

Deletion process

Step 1: Delete NAT
Step 2: Delete all Ec2 Machines
Step 3: Delete VPC
Step 4: Release Elastic IP