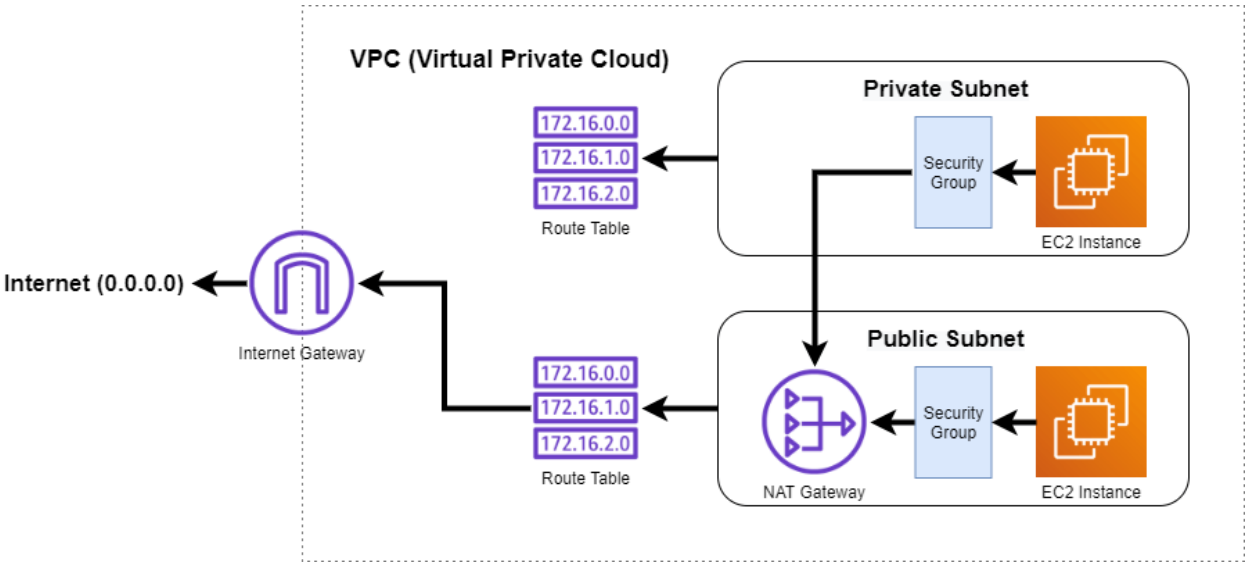
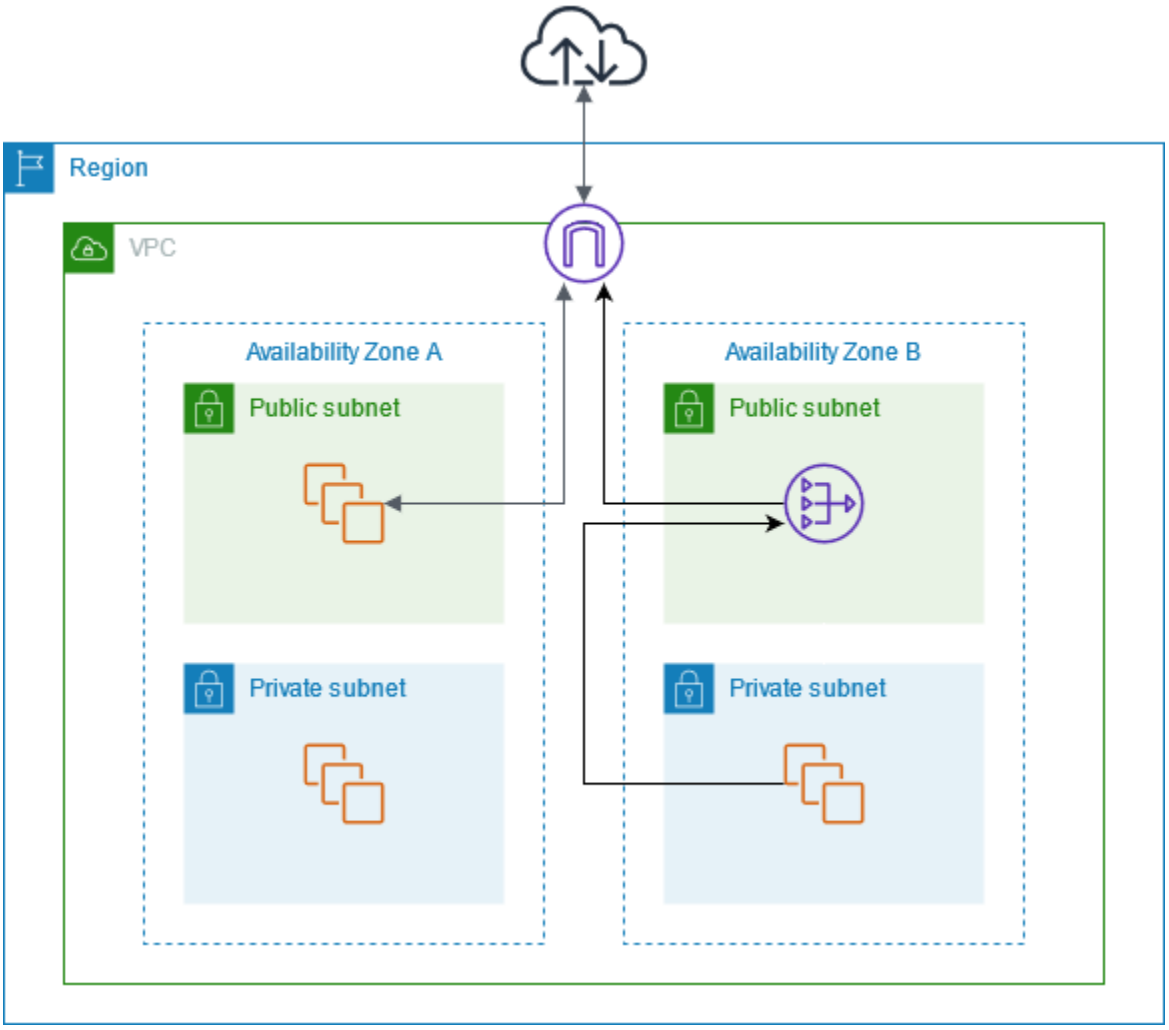
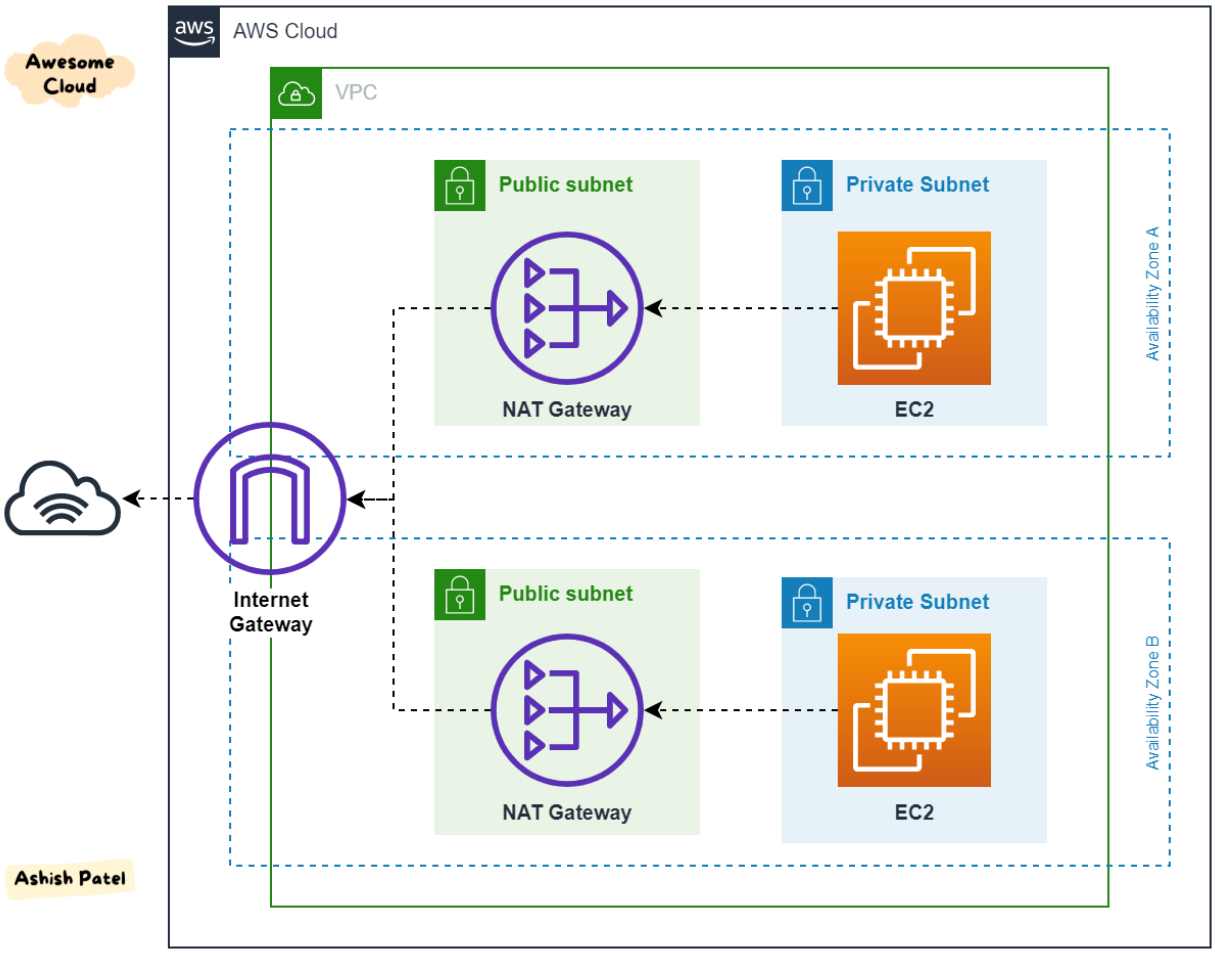
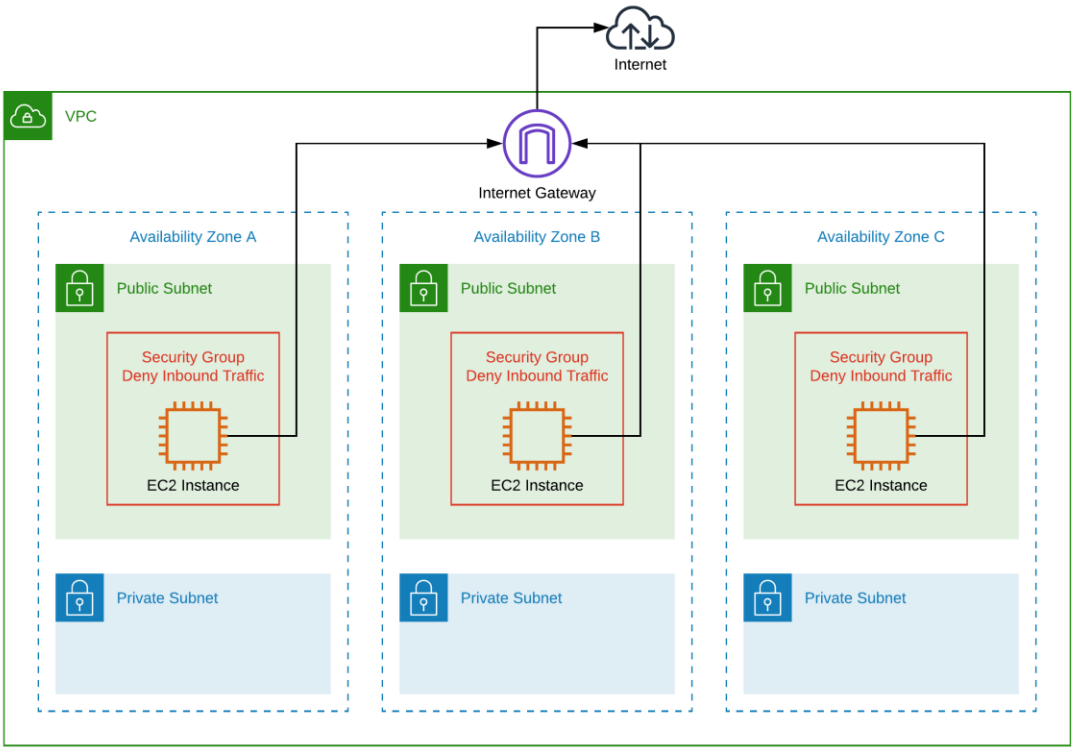
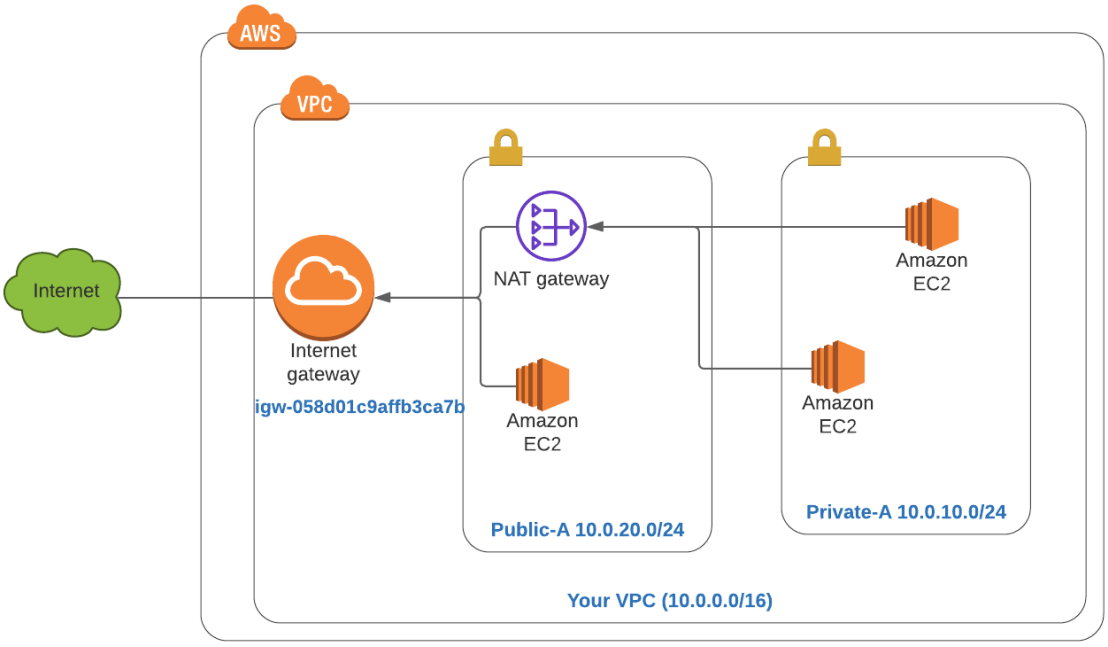
AWS NAT Gateway and NAT Instance And Internet Gateway

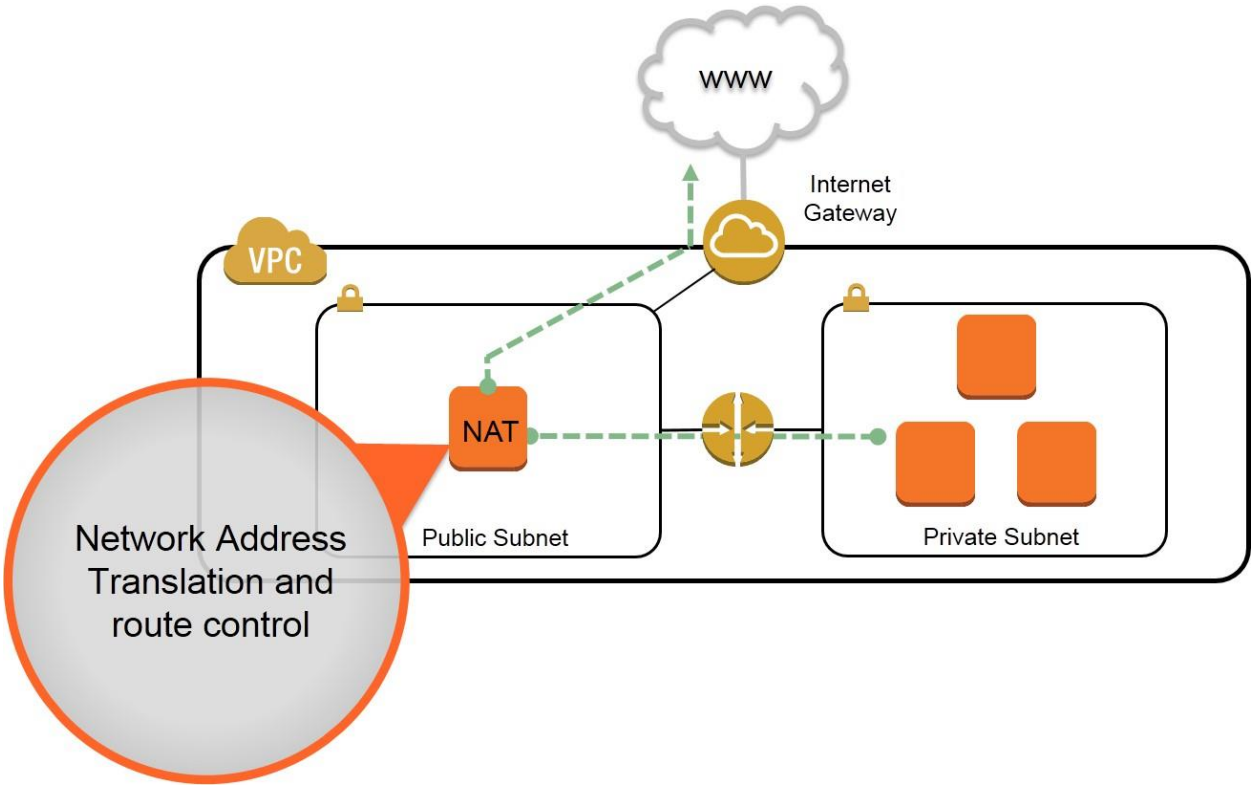


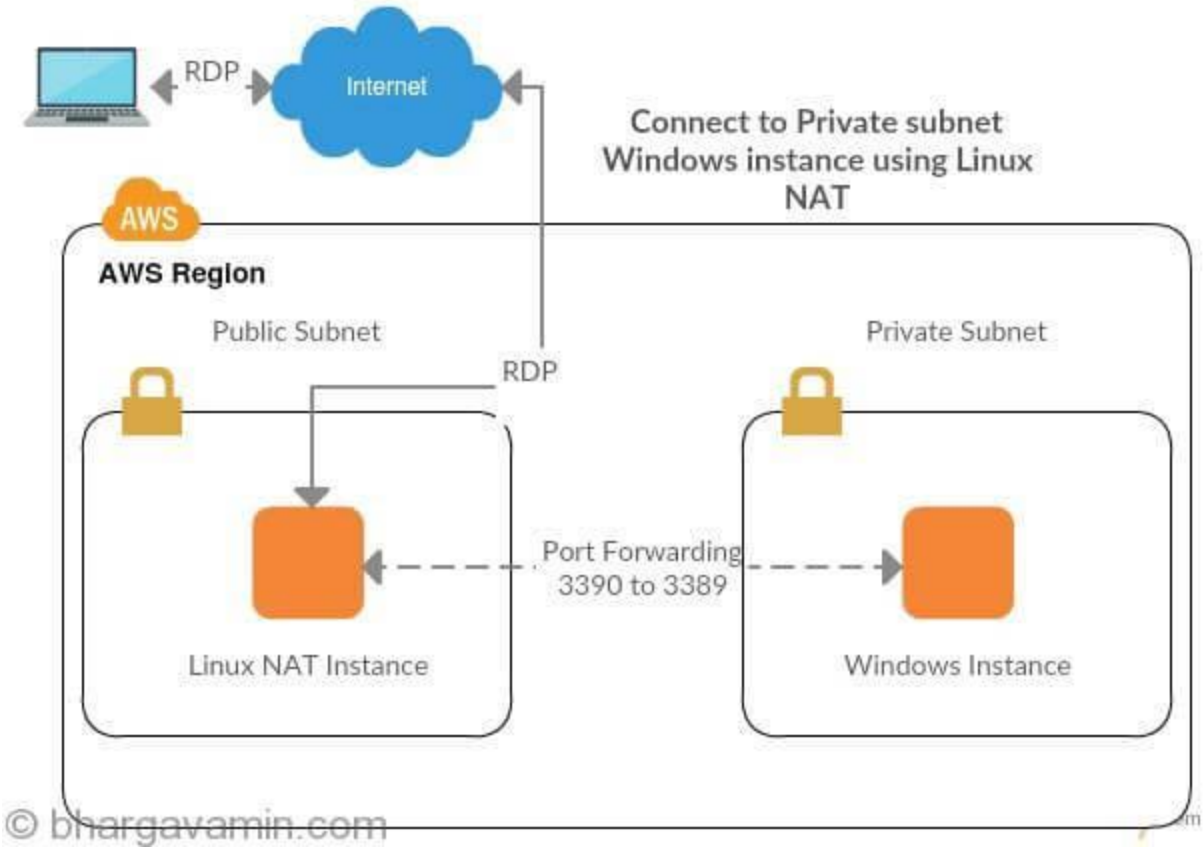

Region
VPC
Availability Zone A
Public subnet
Private subnet
Availability Zone B
Public subnet
Private subnet

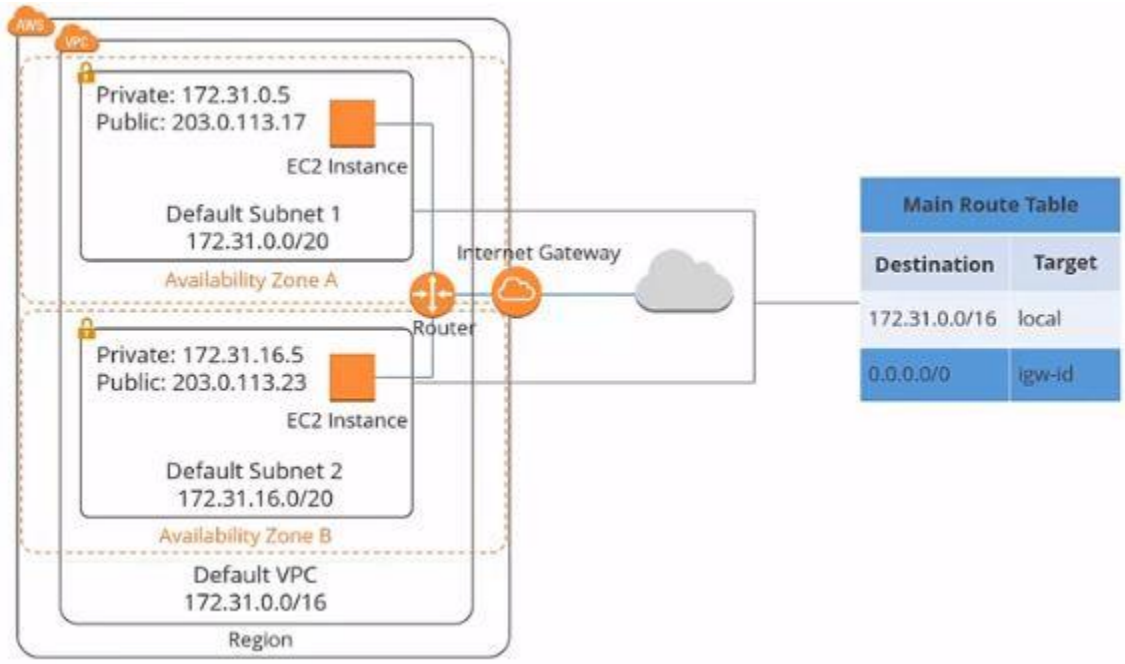

Awesome Cloud
AWS Cloud
VPC
Public subnet
Private Subnet
NAT Gateway
EC2
Availability Zone A
Internet Gateway
Public subnet
Private Subnet
NAT Gateway
EC2
Availability Zone B
Ashish Patel


Internet
VPC
Internet Gateway
Availability Zone A
Availability Zone B
Availability Zone C
Public Subnet
Public Subnet
Public Subnet
Security Group
Deny Inbound Traffic
Security Group
Deny Inbound Traffic
Security Group
Deny Inbound Traffic
EC2 Instance
EC2 Instance
EC2 Instance
Private Subnet
Private Subnet
Private Subnet


AWS
VPC
Internet
Internet
gateway
igw-058d01c9affb3ca7b
NAT gateway
Amazon
EC2
Amazon
EC2
Amazon
EC2
Public-A 10.0.20.0/24
Private-A 10.0.10.0/24
Your VPC (10.0.0.0/16)


www
Internet
Gateway
VPC
NAT
Public Subnet
Private Subnet
Network Address
Translation and
route control

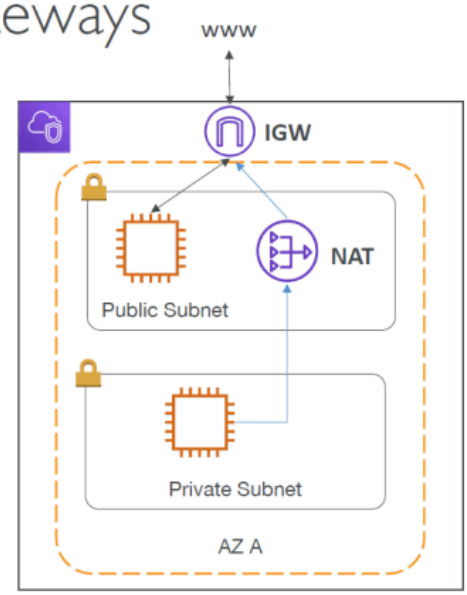

RDP
Internet
Connect to Private subnet
Windows instance using Linux
NAT
AWS
AWS Region
Public Subnet
Private Subnet
RDP
Port Forwarding
3390 to 3389
Linux NAT Instance
Windows Instance
© bhargavamin.com

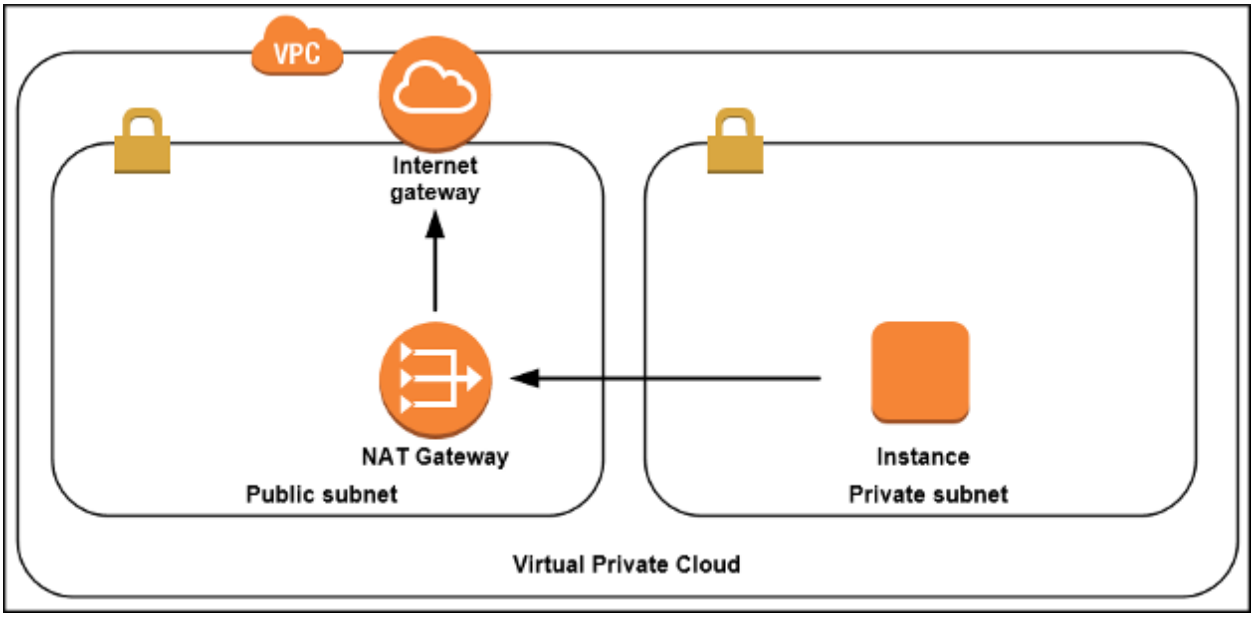

Private: 172.31.0.5
Public: 203.0.113.17
EC2 Instance
Default Subnet 1
172.31.0.0/20
Availability Zone A
Internet Gateway
Router
Private: 172.31.16.5
Public: 203.0.113.23
EC2 Instance
Default Subnet 2
172.31.16.0/20
Availability Zone B
Default VPC
172.31.0.0/16
Region
Main Route Table
Destination
Target
172.31.0.0/16
local
0.0.0.0/0
igw-id

Internet Gateway & NAT Gateways

- **Internet Gateways** helps our VPC instances connect with the internet
- Public Subnets have a route to the internet gateway.

- **NAT Gateways** (AWS-managed) & **NAT Instances** (self-managed) allow your instances in your **Private Subnets** to access the internet while remaining private





NAT Gateway Vs **NAT Instance**

- Are more scalable and can handle more bandwidth in comparison to NAT instances.
- Are created in Public Subnet to enable Private Subnets to communicate with internet.
- NAT gateway redundancy can be achieved inside Availability Zone.
- No association with Security groups required.
- No requirement of disabling Source/Destination checks.
- Starting with 5Gbps , can scale upto 45Gbps
- Preferred in comparison to NAT instances.

- NAT instances are just another EC2 instances capable of handling NAT.
- Instances are created in Public Subnet to enable Private Subnets to communicate with internet.
- Instances are not redundant.
- NAT instances are associated with Security groups just like any other EC2 instances.
- Since every EC2 instances does Source/Destination check so it has to be disabled for NAT instance .
- Limited by the line bandwidth of the instances.

	NAT Gateway	NAT Instance
Managed	Managed by AWS	Managed by you
Availability	Highly available within an AZ	Not highly available (would require scripting)
Bandwidth	Up to 45 Gbps	Depends on the bandwidth of the EC2 instance type selected
Maintenance	Managed by AWS	Managed by you
Performance	Optimized for NAT	Amazon Linux AMI configured to perform NAT
Public IP	Elastic IP that cannot be detached	Elastic IP that can be detached
Security Groups	Cannot associate with a Security Group	Can associate with a Security Group
Bastion Host	Not supported	Can be used as a bastion host