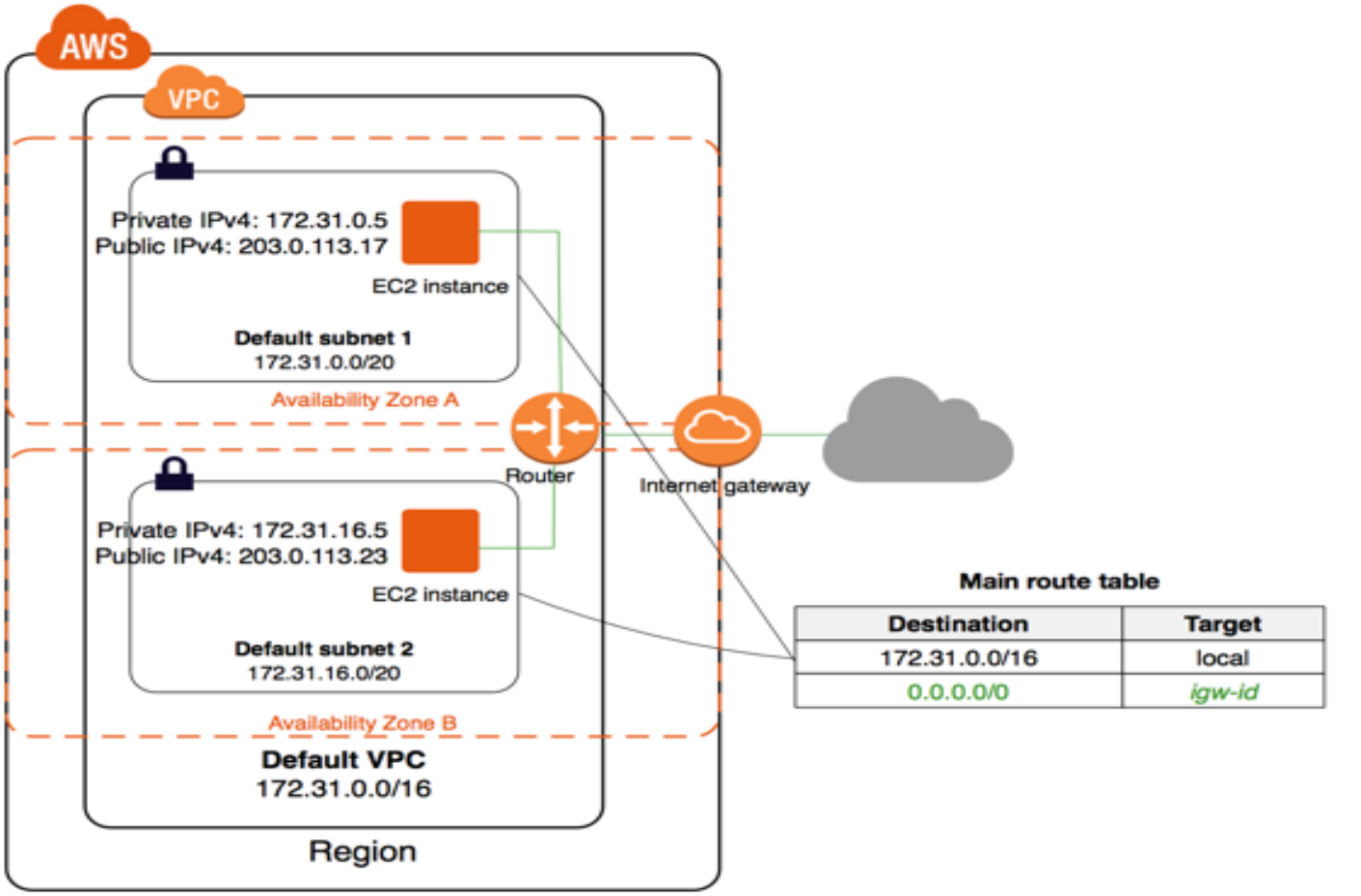
VPC (Virtual Private Cloud)

AWS VPC

- **What is AWS VPC?**
  - Amazon Virtual Private Cloud (VPC) is a service that allows users to create a virtual dedicated network for resources.
- **Security Groups:**
  - **Default Security Groups:-**
    - Inbound rule - Allows all inbound traffic
    - Outbound rule - Allows all outbound traffic
  - **Custom Security Groups:- (by default)**
    - Inbound rule - Allows no inbound traffic
    - Outbound rule - Allows all outbound traffic
- **Network ACLs (access control list):**
  - **Default Network ACL:-**
    - Inbound rule - Allows all inbound traffic
    - Outbound rule - Allows all outbound traffic
  - **Custom Network ACL:- (by default)**
    - Inbound rule - Denies all inbound traffic
    - Outbound rule - Denies all outbound traffic

AWS VPC


AWS
VPC
Private IPv4: 172.31.0.5
Public IPv4: 203.0.113.17
EC2 instance
Default subnet 1
172.31.0.0/20
Availability Zone A
Router
Internet gateway
Private IPv4: 172.31.16.5
Public IPv4: 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

Components of VPC

- **Subnets**
  - The subnet is a core component of the VPC.
  - Resources will reside inside the Subnet only.
  - Subnets are the logical division of the IP Address.
  - One Subnet should not overlap another subnet.
  - A subnet can be private or public.
  - Resources in **Public Subnet** will have internet access.
  - Resources in the **Private Subnet** will not have internet access.
  - If private subnet resources want internet accessibility, then we will need a NAT gateway or NAT instance in a public subnet.

Components of VPC

- **Route Tables**
  - Route tables will decide where the network traffic will be directed.
  - One Subnet can connect to one route table at a time.
  - But one Route table can connect to multiple subnets.
  - If the route table is connected to the Internet Gateway and that route table is associated with the subnet, then that subnet will be considered as a Public Subnet.
  - The private subnet is not associated with the route table which is connected to the Internet gateway.

Components of VPC

- **NAT Devices**
  - NAT stands for **Network Address Translation.**
  - It allows resources in the Private subnet to connect to the internet if required.
- **NAT Instance**
  - It is an EC2 Instance.
  - It will be deployed in the Public Subnet.
  - NAT Instance allows you to initiate IPv4 Outbound traffic to the internet.
  - It will not allow the instance to receive inbound traffic from the internet.

Components of VPC

- **NAT Gateway**
  - Nat Gateway is Managed by AWS.
  - NAT will be using the elastic IP address.
  - You will be charged for NAT gateway on a per hour basis and data processing rates.
  - NAT is not for IPv6 traffic.
  - NAT gateway allows you to initiate IPv4 Outbound traffic to the internet.
  - It will not allow the instance to receive inbound traffic from the internet.

Components of VPC

- **DHCP Options Set:**
  - DHCP stands for Dynamic Host Configuration Protocol.
  - It is the standard for passing the various configuration information to hosts over the TCP/IP Network.
  - DHCP contains information such as domain name, domain name server.
  - All this information will be contained in Configuration parameters.
  - DHCP will be created automatically while creating VPC.

Components of VPC

- **PrivateLink**
  - **PrivateLink** is a technology that will allow you to access services privately without internet connectivity and it will use the private IP Addresses.
- **Endpoints**
  - It allows you to create connections between your VPC and supported AWS services.
  - The endpoints are powered by **PrivateLink**.
  - The traffic will not leave the AWS network.
  - It means endpoints will not require Internet Gateway, Virtual Private Gateway, NAT components.
  - The public IP address is not required for communication.
  - Communication will be established between the VPC and other services with high availability.

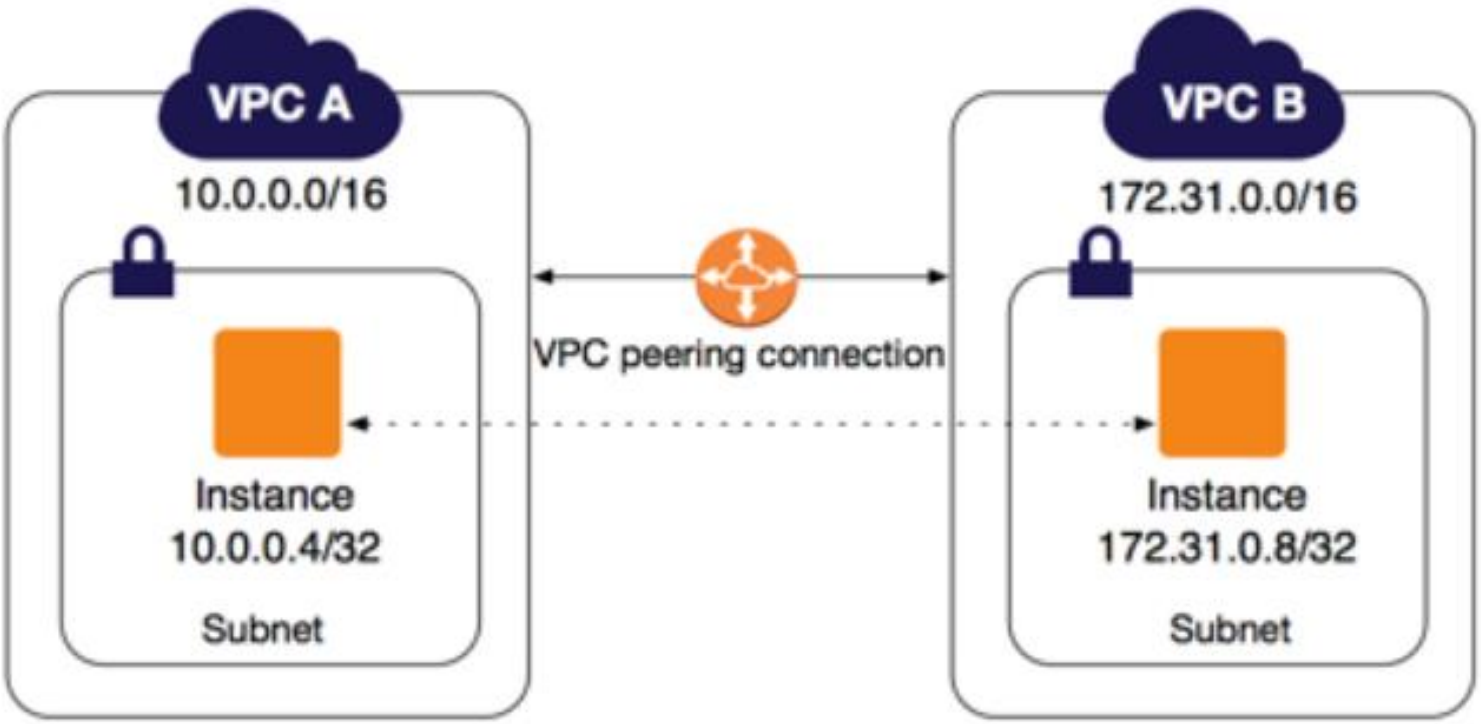
Components of VPC

- **Types of Endpoints**
  - **Interface Endpoints**
    - It is an entry point for traffic interception.
    - It will route the traffic to the service that you configure.
    - It will use an ENI with a private IP address.
    - For Example: it will allow instances to connect to Amazon Kinesis through interface endpoint.
  - **Gateway Load balancer Endpoints**
    - It is an entry point for traffic interception.
    - It will route the traffic to the service that you configure.
    - It will use load balancers to route the traffic.
    - For Example Security Inspection.
  - **Gateway Endpoints**
    - It is a gateway that you defined in Route Table as a Target.
    - And the destination will be the supported AWS Services.
    - Amazon S3, DynamoDB supports Gateway Endpoint.

Components of VPC

- **Egress Only Internet Gateway**
  - An egress-only internet gateway is designed only for IPv6 address communications.
  - It is a highly available, horizontally scaled component which will allow outbound only rule for IPv6 traffic.
  - It will not allow inbound connection to your EC2 Instances.
- **VPC Peering:**
  - VPC peering establishes a connection between two VPCs.
  - EC2 Instances in both the VPC can communicate with each other as if they are in the same network.
  - Peering connections can be established between VPCs in the same region, VPCs in a different region or VPCs in another AWS Account as well.

VPC Peering


VPC A
10.0.0.0/16
Instance
10.0.0.4/32
Subnet
VPC peering connection
VPC B
172.31.0.0/16
Instance
172.31.0.8/32
Subnet

Components of VPC

- **VPN**
  - Virtual Private Network (VPN) establish secure connections between multiple networks i.e., on-premise network, client space, AWS Cloud, and all the network acts
  - VPN provides a high-available, elastic, and managed solution to protect your network traffic.
- **AWS Site-to-Site VPN**
  - AWS Site-to-Site VPN creates encrypted tunnels between your network and your Amazon Virtual Private Clouds or AWSTransit Gateways.
- **AWS Client VPN**
  - AWS Client VPN connects your users to AWS or on-premises resources using a VPN software client.

Components of VPC

- **Use Cases:**
  - Host a simple public-facing website.
  - Host multi-tier web applications.
  - Used for disaster recovery as well.
- **Pricing:**
  - No additional charges for creating a custom VPC.
  - NAT does not come under the free tier limit you will get charged per hour basis.
  - NAT Gateway data processing charge and data transfer charges will be separate.
  - You will get charged per hour basis for traffic mirroring.