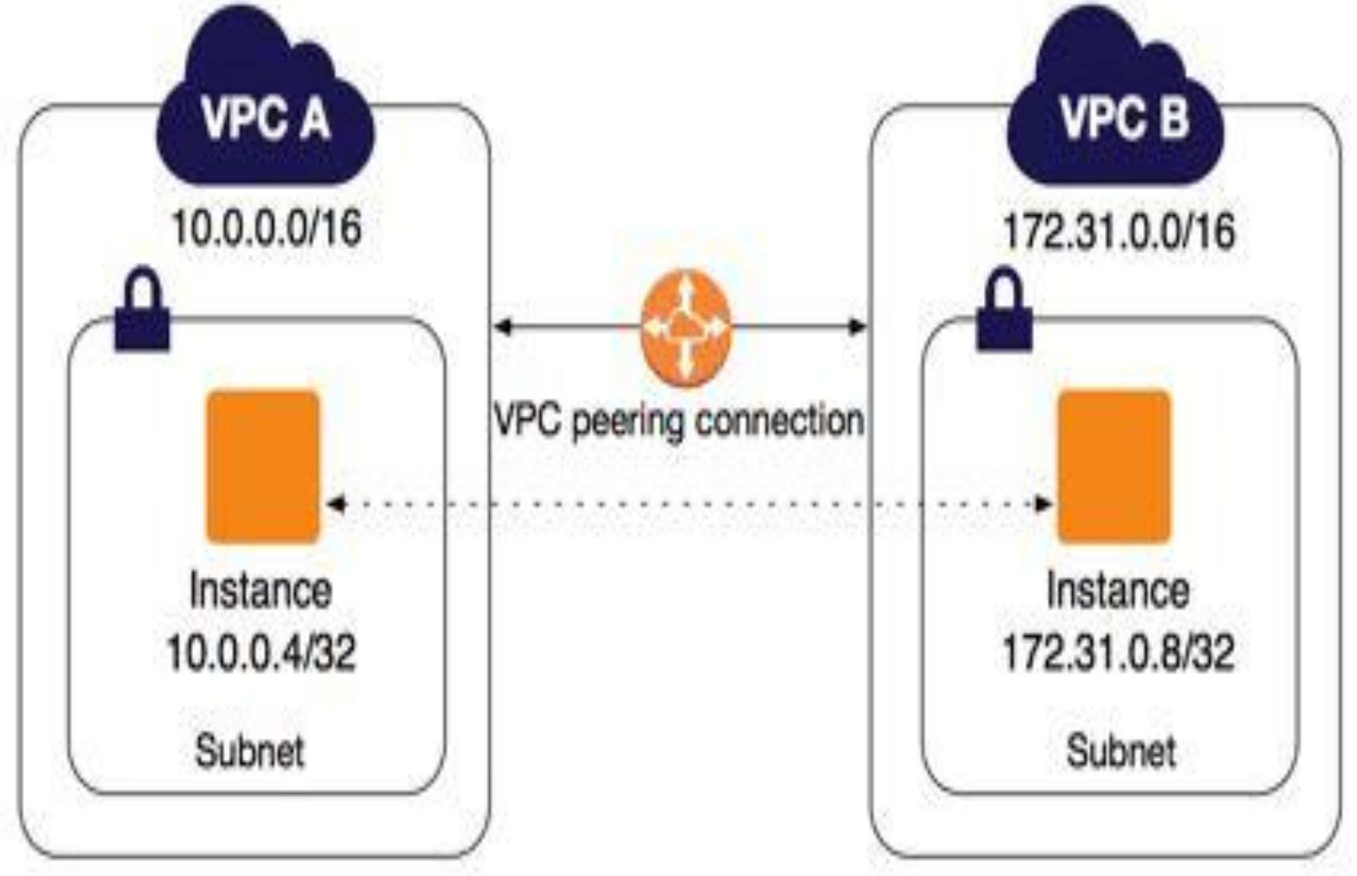
Amazon Virtual Private Cloud

aws academy

VPC Peering

- It is a networking connection between two VPCs that enables to route traffic between them using private IPv4 or IPv6 addresses.
- It is neither a gateway nor a VPN.
- Peered instances communicate with each other as if they are within the same network.
- Traffic remains in the private IP space with encrypted communication.



VPC Peering cont …

- **Ways to do peering -**
  - VPCs belong to same account
  - Inter account VPC peering
  - Inter-region VPC peering
- **Which services can be accessed through VPC peering ?**
  - EC2 Instances
  - Amazon RDS services
  - Access Lambda function running in different AWS regions to communicate with each other using private IP addresses without using gateways, VPN or other appliances.

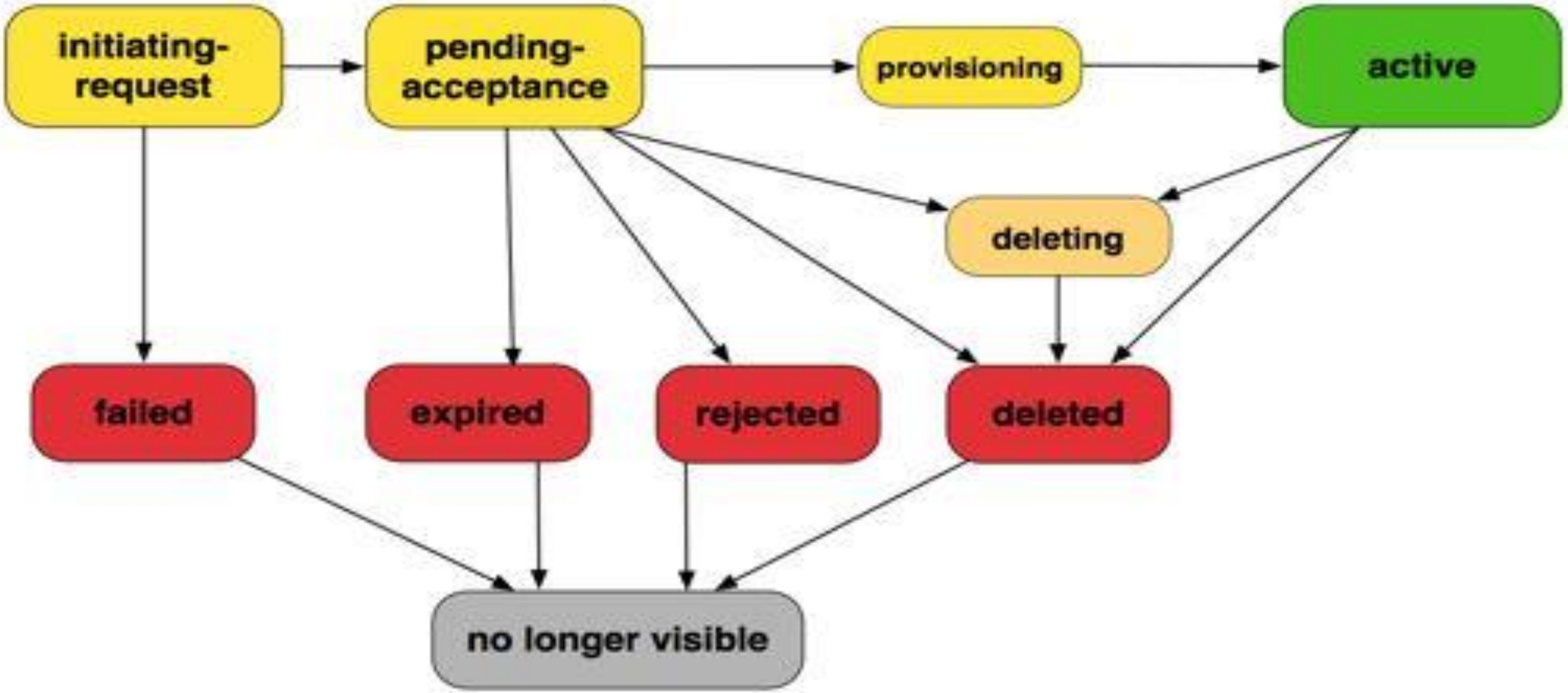
VPC Peering Benefits

- **Benefits of VPC peering-**
  - Traffic never flow to public Internet which so we can reduce threats, such as common exploits, and DDoS attacks.
  - A simple and cost-effective way to share resources between regions or replicate geographic redundancy.

VPC Peering Limitations

- Peering between VPCs with matching or overlapping IPv4 or IPv6 CIDR blocks are not possible.
- Maximum 50 peering (extended upto 125) active VPC peering connections per VPC is allowed.
- It does not support transitive peering relationships.
- You cannot have more than one VPC peering connection between the same two VPCs at the same time.
- Unicast reverse path forwarding in VPC peering connections is not supported.
- Any tags that you create for your VPC peering connection are only applied in the account or region in which you create them.

VPC Peering connection stages

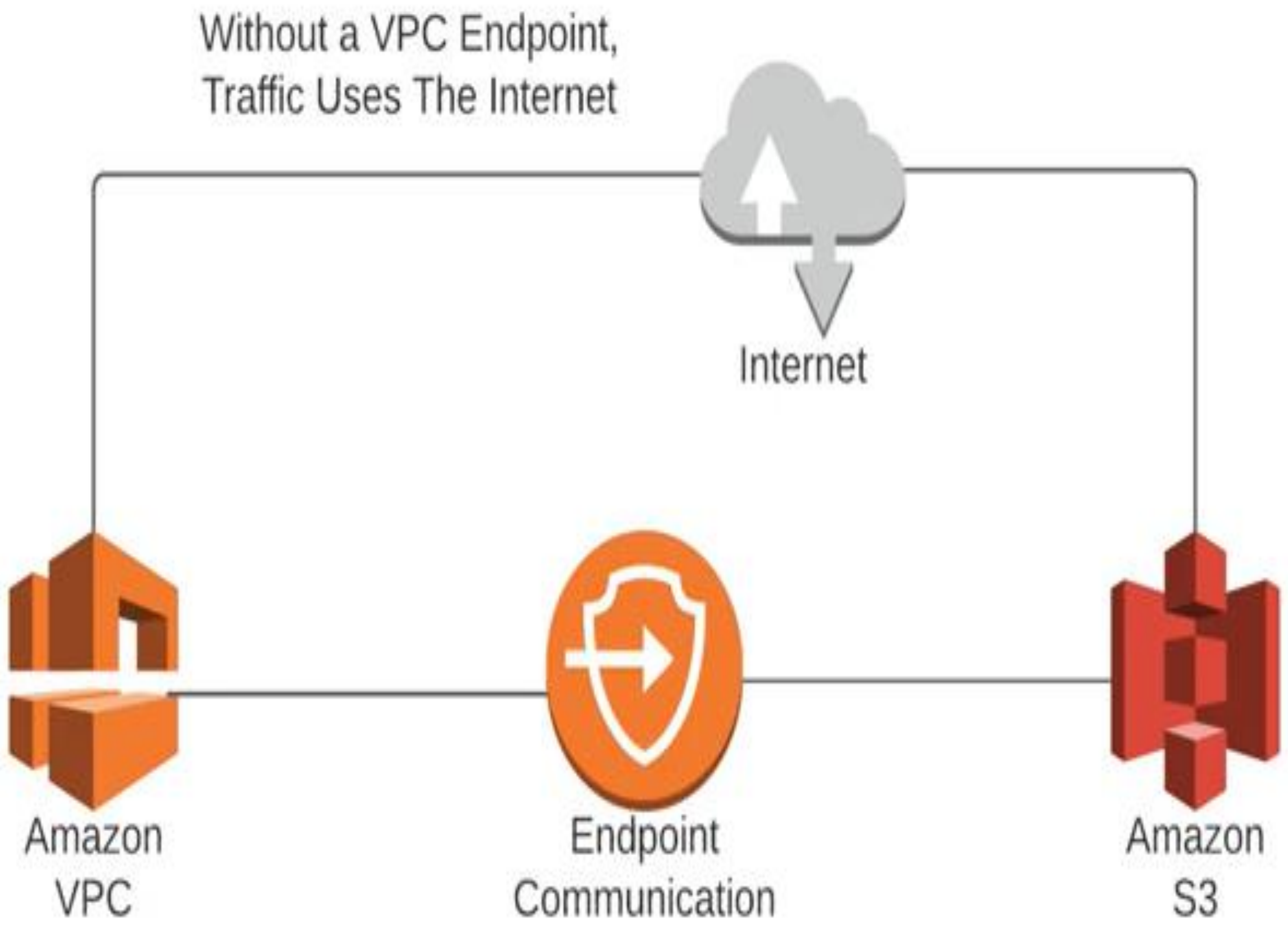


AWS PrivateLink and VPC endpoints

- **AWS PrivateLink** enables us to privately connect the VPC to supported AWS services.
- The services can be hosted by other AWS accounts (**VPC endpoint services**), and supported AWS Marketplace partner services.
- The communication between VPC and the services can be established without using Internet gateway, NAT device, public IP address etc.
- Traffic communication is not exposed to the public internet.
- A VPC endpoint service, powered by AWS PrivateLink, can be created and used to enable AWS customers to access the service.

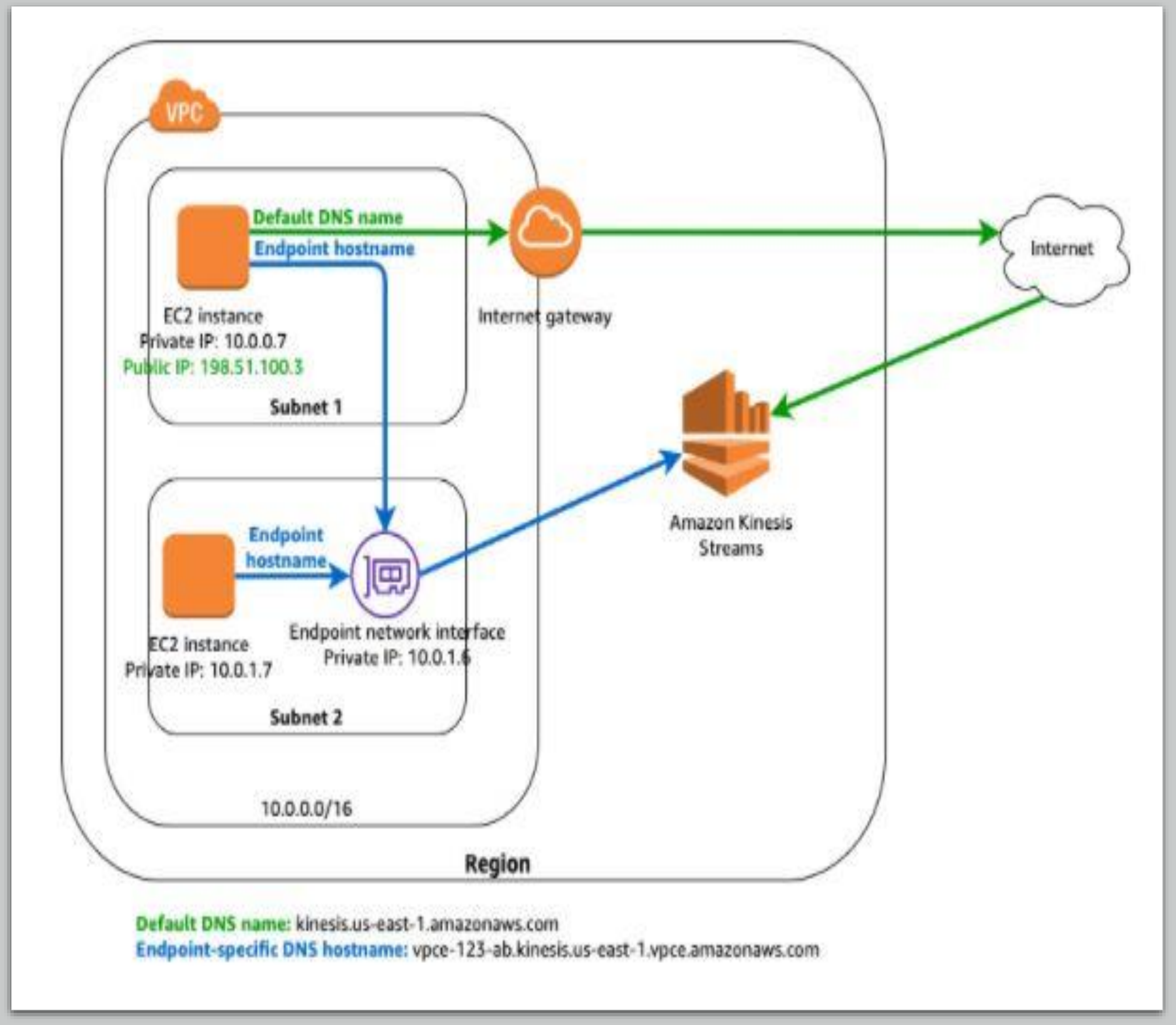
VPC endpoints concepts

- **VPC endpoint** — The entry point in the VPC that enables to connect privately to a service.
- **Endpoint service** — Your own application or service in your VPC.
- They are horizontally scaled, redundant and highly scalable.
- Types:
  - Interface endpoints
  - Gateway endpoints



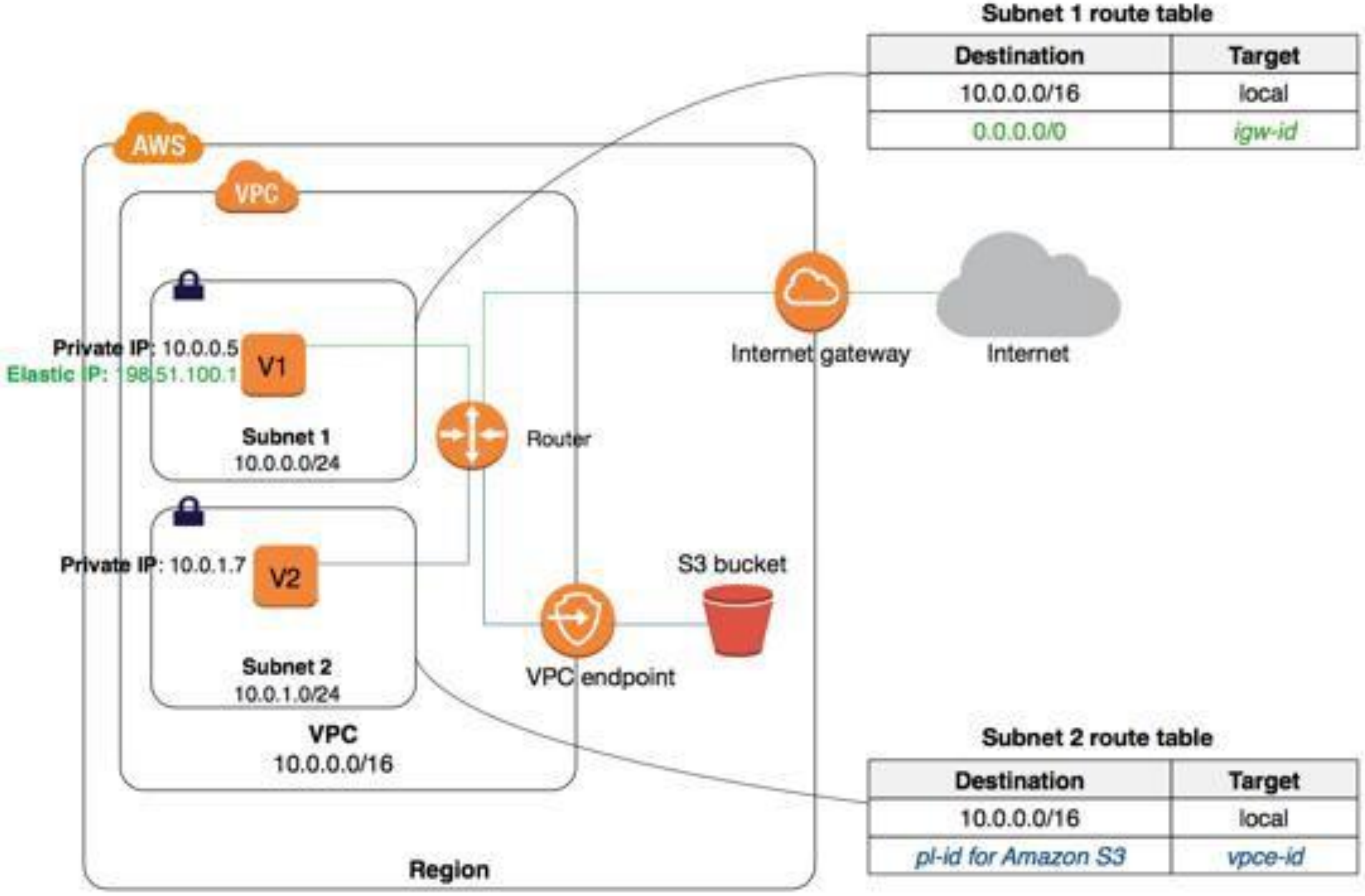
VPC endpoints Types

- **Interface endpoints -** An ENI with a private IP address which serves as an entry point for traffic destined to a supported AWS service or a VPC endpoint service.



VPC endpoints Types

- **Gateway endpoints-**
- A gateway that is specified as a target for a route in a RT for traffic destined to a supported AWS services.
- It provides an entry point in the VPC to connect privately to **Amazon S3** and **DynamoDB** service



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*