

VPC Endpoints

[vpc endpoint](#) enables creation of a private connection between VPC to supported AWS services and VPC endpoint services powered by PrivateLink using its private IP address. Traffic between VPC and AWS service does not leave the Amazon network.

There are two types of VPC endpoints:

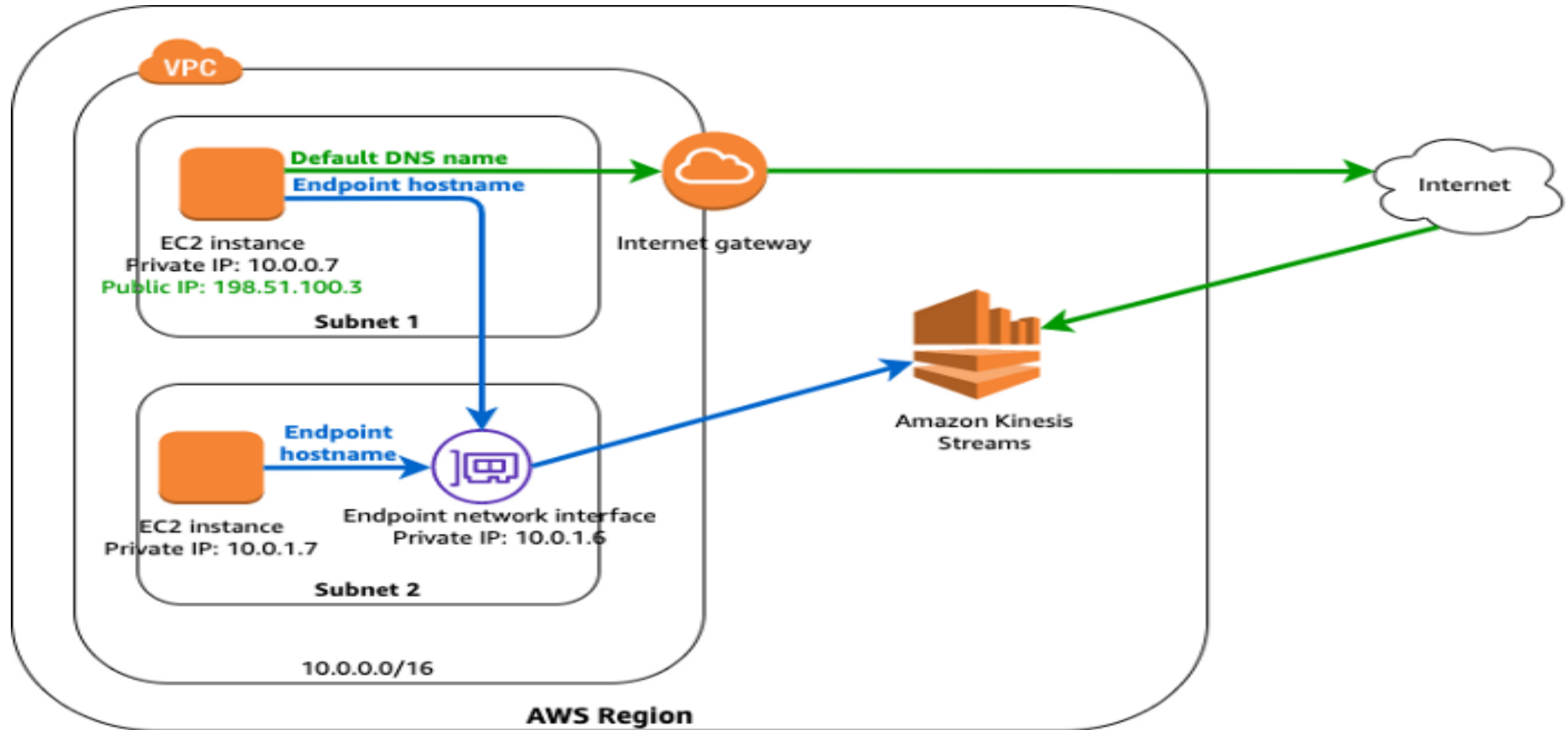
[Interface endpoint](#) is an elastic network interface (ENI) with a private IP address from the IP address range of user's subnet that serves as an entry point for traffic destined to a supported service. It enables you to privately access services by using private IP addresses.

[Gateway endpoint](#) is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. Currently supports S3 and DynamoDB services.

VPC Endpoints Key points

- VPC endpoint enables users to privately connect their VPC to supported AWS services.
- VPC Endpoint does not require a public IP address, access over the Internet, NAT device, a VPN connection or AWS Direct Connect to communicate with resources in the service.
- Endpoints are virtual devices, that are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in the VPC.
- Access to the resources in other services can be controlled by endpoint policies.
- By default, Endpoint policy, allows full access to the service. Endpoint policies must be written in JSON format.
- Endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies).

Endpoint Network Interface



Default DNS name: kinesis.us-east-1.amazonaws.com

Endpoint-specific DNS hostname: vpce-123-ab.kinesis.us-east-1.vpce.amazonaws.com

VPC Endpoints Limitations

- VPC endpoints support IPv4 traffic only.
- Endpoints are supported within the same Region only. You cannot create an endpoint between a VPC and a service in a different Region.
- Endpoints cannot transfer an endpoint from one VPC to another, or from one service to another.

Interface Endpoints:

- For each interface endpoint, you can choose only one subnet per Availability Zone.
- Each interface endpoint can support a bandwidth of up to 10 Gbps per Availability Zone by default. Additional capacity may be added automatically based on your usage.
- Interface Endpoint supports TCP traffic only.
- Endpoints cannot be transferred from one VPC to another, or from one service to another.

VPC Endpoints Limitations

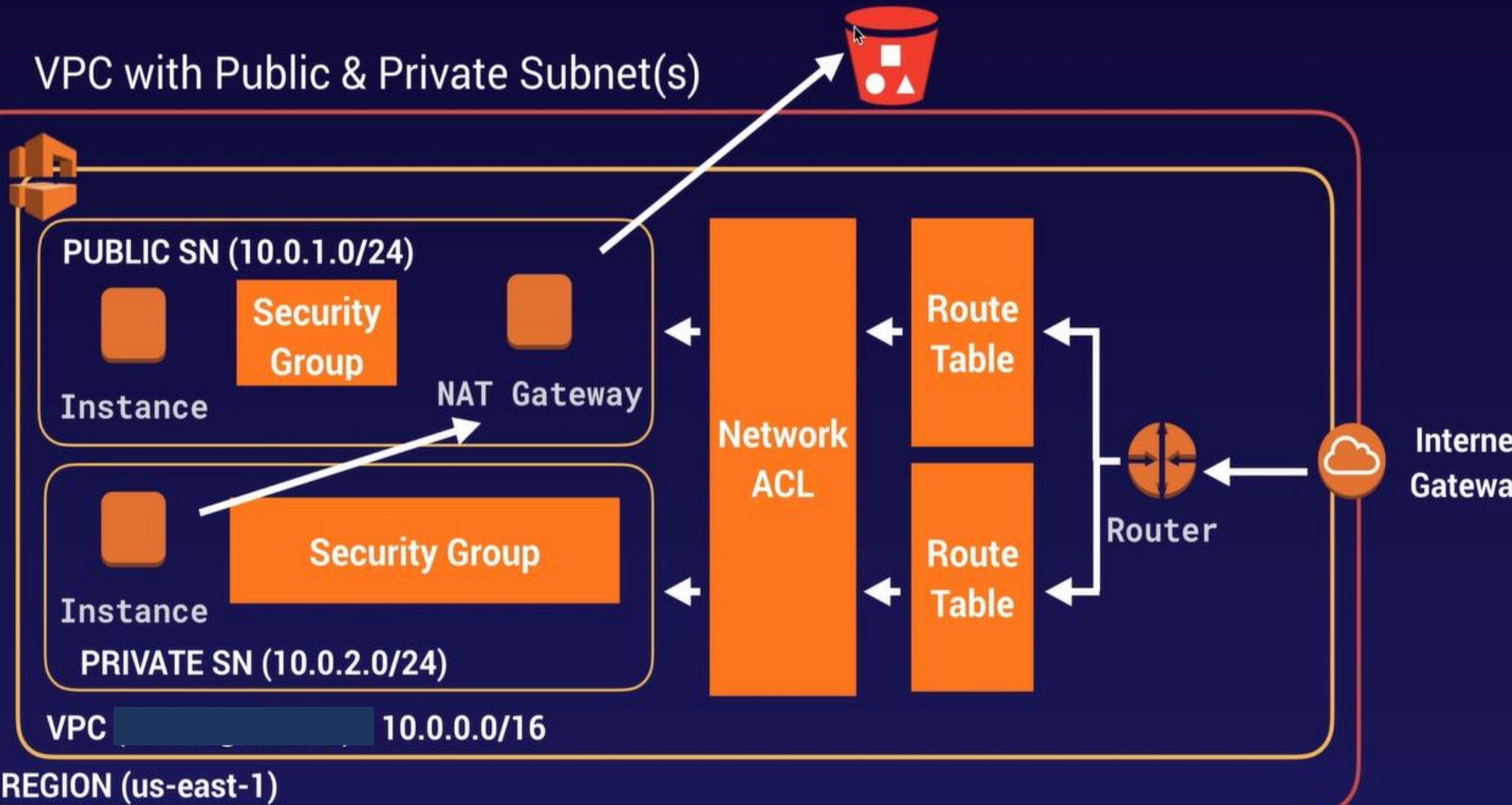
- **Gateway Endpoints:**
- Endpoint connections cannot be extended out of a VPC i.e. resources across the VPN connection, VPC peering connection, AWS Direct Connect connection cannot use the endpoint

A VPC Endpoint:

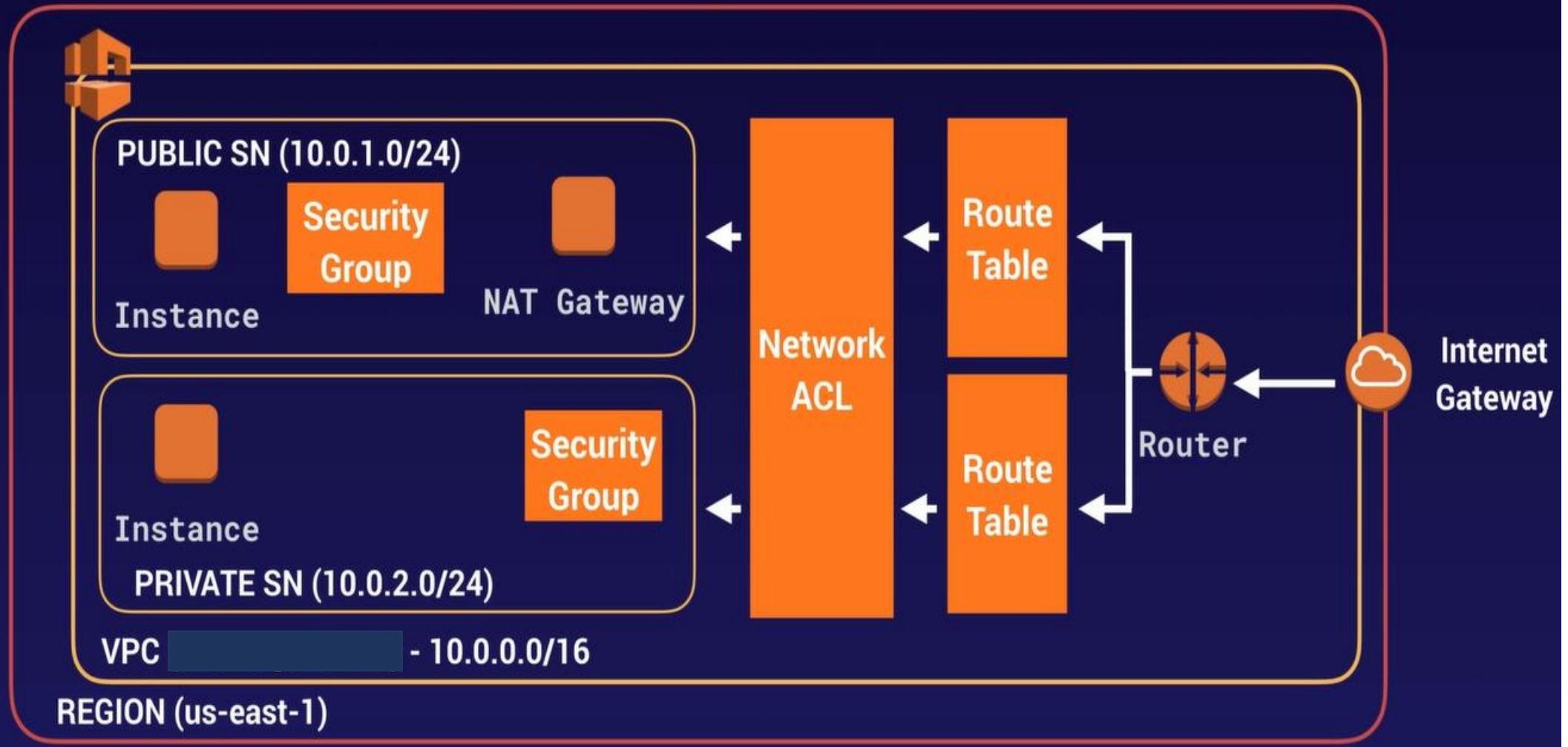
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

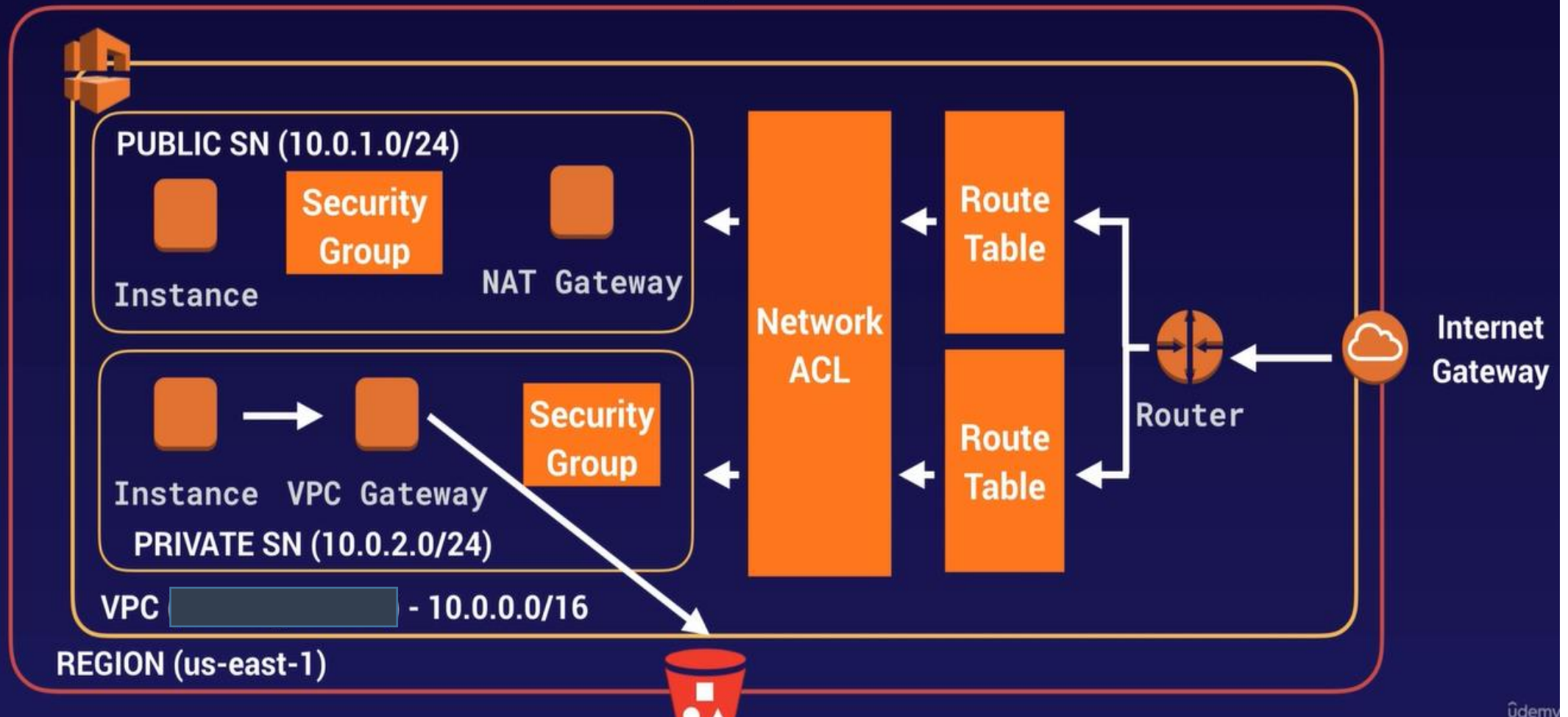
VPC with Public & Private Subnet(s)



VPC with Public & Private Subnet(s)

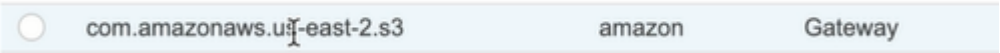


VPC with Public & Private Subnet(s)



- Go to IAM
 - Create ROLE
 - Select ec2 service
 - Select s3 full access
 - Create role
-
- Go to DB server
 - Select it and go with instance setting
 - Click on change / attached replace IAM role
 - Add role which you have created earlier
 - Apply it

- Go to NACL
- Click on default NACL which is with VPC
- And assign both subnet via subnet association
- Now connect with public server
- Sudo su
- SSH to private IP for DB server
- Aws s3 ls
- ```
[root@ip-10-0-2-235 ec2-user]# echo "test" > test.txt
```
- Ls
- Aws s3 cp test.txt s3:// (bucket arn)
- Test S3 bucket . You can find the file

- Go with Private RT
- Delete the NAT gateway from routes
- Now type aws s3 ls
- Nothing to happen
- Go with VPC endpoint
- Create endpoint
- Select aws services
- Select amazon s3 gateway
- 
- Select VPC
- Select private RT and create end point

- Now check Private RT
- Endpoint will associate there automatically
- Now go with putty type `aws s3 ls ..` If stuck then type below same command with region

```
[root@ip-10-0-2-235 ec2-user]# aws s3 ls --region us-east-2
```