VPC Endpoint: -

Introduction

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS Private Link 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.**

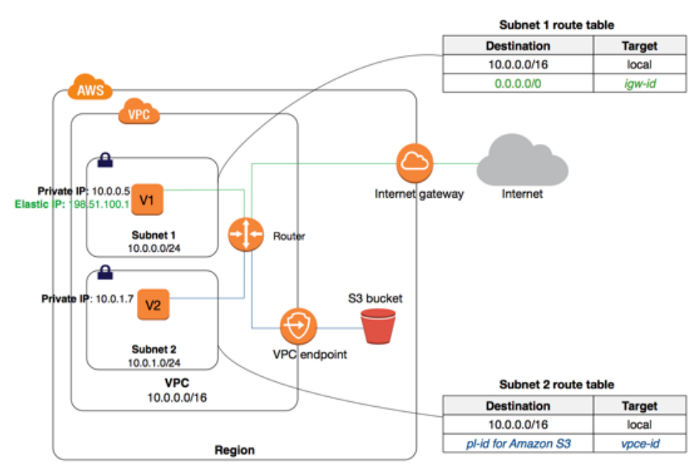
They allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

VPC endpoints concepts

The following are the key concepts for VPC endpoints:

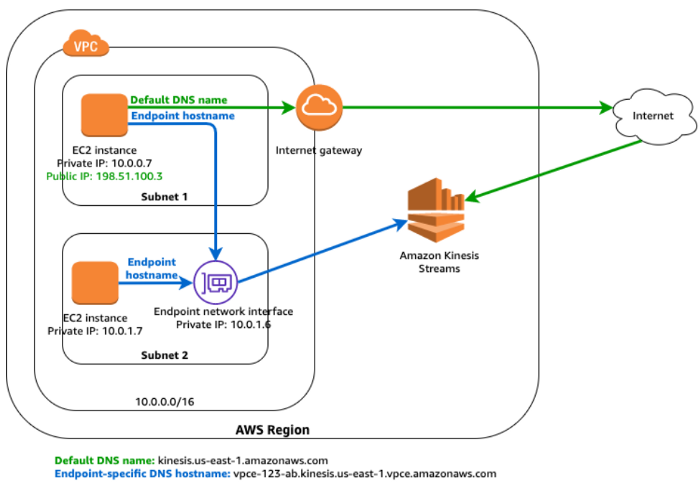
**Endpoint service** — Your own application in your VPC. Other AWS principals can create a connection from their VPC to your endpoint service.

**Gateway endpoint** — A [gateway endpoint](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html) is a gateway that you specify as a **target for a route in your route table** for traffic destined to a supported AWS service.

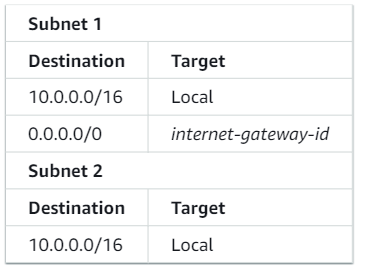


**Interface endpoint** — An [interface endpoint](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html) is an elastic **network interface** with a **private IP** address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service.

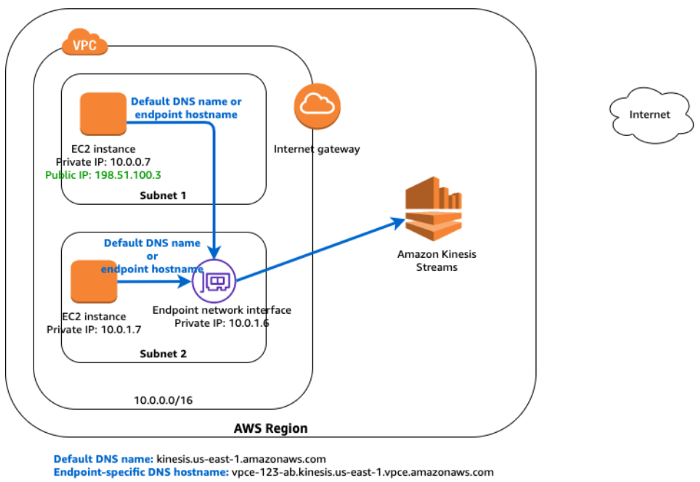
**Traffic flow *BEFORE*enabling Interface endpoint**: Traffic routes via IGW and internet towards Amazon Kinesis.



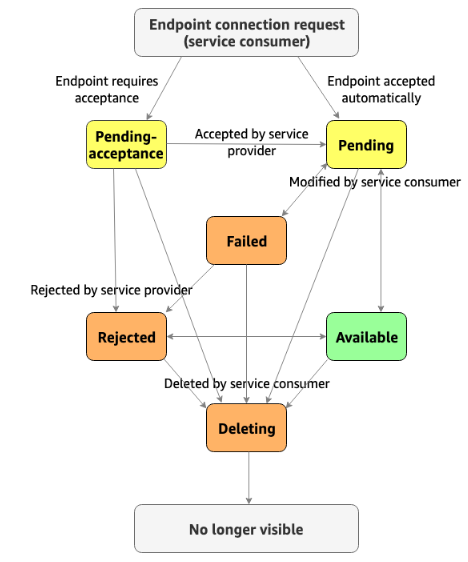
**Enable the routes in Route table like below:**



**Traffic flow *AFYER*enabling Interface endpoint**: Traffic routes via Endpoint’s Network interface, towards Amazon Kinesis.



**Lifecycle**: An interface endpoint goes through various stages starting from when you create it (the endpoint connection request). At each stage, there might be actions that the service consumer and service provider can take.



Rules:

* A service provider can configure its service to accept interface endpoint requests automatically or manually. AWS services and AWS Marketplace services generally accept all endpoint requests automatically.
* A service provider cannot delete an interface endpoint to its service. Only the service consumer that requested the interface endpoint connection can delete the interface endpoint.
* A service provider can reject the interface endpoint after it has been accepted (either manually or automatically) and is in the available state.

Limitations:

**VPC Endpoint**:

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

**VPC Interface Endpoints Limitation:**

* One interface endpoint can choose only one subnet per Availability Zone per region.
* By default, 10 GBPS bandwidth supported by VPC interface endpoint per AZ. Based on your uses AWC can support additional bandwidth capacity.
* Interface Endpoint supports TCP traffic only.
* Endpoints cannot be transferred from one VPC to another, or from one service to another.

**VPC Gateway Endpoints Limitation:**

* 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

Conclusion:

The above explanation is a High-Level difference between VPC Gateway Endpoints and VPC Interface endpoints’ with their Limitations. Also lifecycle & its rules of Interface endpoints, define in a short way. This is one of the most important topics for any AWS Certification exam. Especially all three Associate level (Solution Architect, SysOps Administrator & Developer Associate)