**AWS-Privatelink (VPC End Point Service):**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

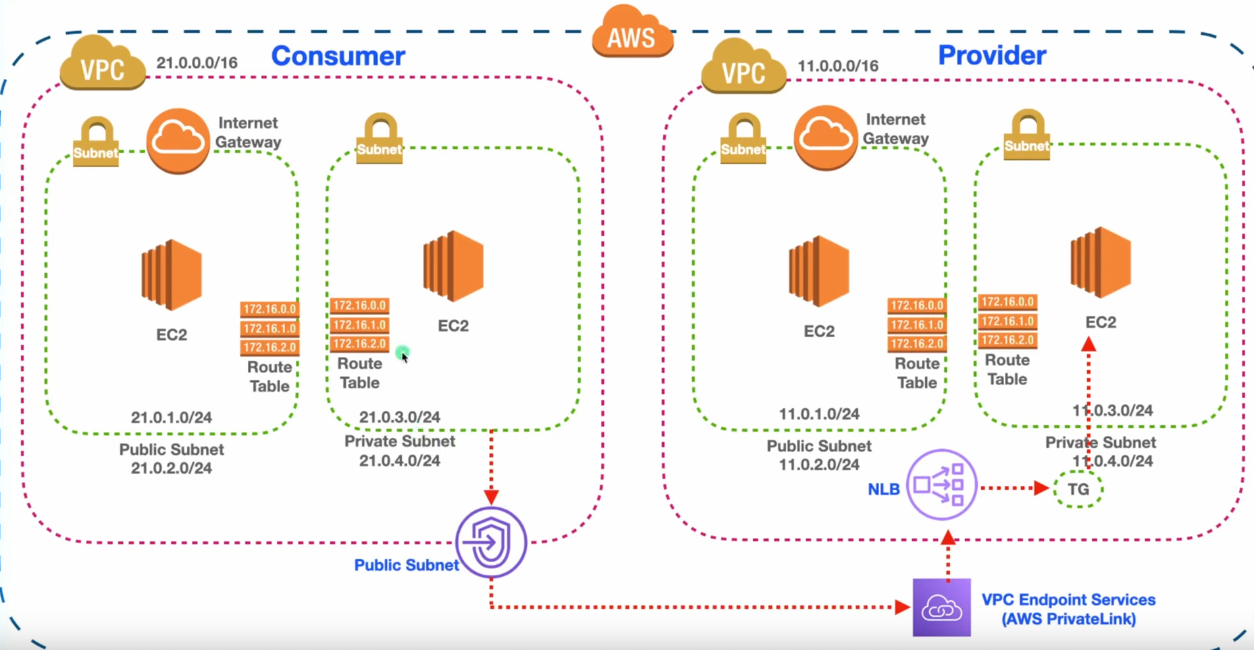


Fig 1.0

In This picture Clearly Shown the Architecture of AWS-privatelink.

Pre-Requirements:

-----------------------

1) Two VPC’s (Provider and Client)

2) Each Vpc’s should have Two subnets (one public,another one private)

3) Internetgateway(Two Vpc’s have two internet gateways for public subnets)

4) One NatGateway (for Provider private-server web server installation)

5) Each VPC should have two Routetables want to route the network(public and private subnets i)

6) One Network Loadblancer and targetgroup( for service provider vpc for communicating with the ec2)

7) One End-poni Service(for to serve the access from the provider vpc)

8) one vpc Endponit(for recevice the service)

Process:

----------

### 🔹 ****Step 1: Create Two VPCs****

* **VPC 1** (Service VPC) – Example CIDR: 10.0.0.0/16
* **VPC 2** (Client VPC) – Example CIDR: 10.1.0.0/16

Each VPC should have:

* 1 Public subnet (for bastion/SSH if needed)
* 1 Private subnet (for EC2 instances)

### 🔹 ****Step 2: Launch EC2 Instances****

**In VPC 1 (Service VPC):**

* Private EC2 instance (runs web service, e.g., NGINX)
* Optional public EC2 (bastion host for SSH)

**In VPC 2 (Client VPC):**

* Private EC2 instance (will act as service consumer)
* Optional public EC2 (bastion)

### 🔹 ****Step 3: Install Web Server on Private EC2 in VPC 1****

sudo apt update

sudo apt install nginx -y

echo "Hello from PrivateLink Server" | sudo tee /var/www/html/index.html

### 🔹 ****Step 4: Create a Network Load Balancer (NLB) in VPC 1****

* Listener: TCP, Port 80
* Target Group: Register private EC2 instance
* Subnets: Only **private subnets**

### 🔹 ****Step 5: Create a VPC Endpoint Service****

In VPC 1:

* Go to **VPC → Endpoint Services → Create**
* Select your **NLB**
* Enable **Acceptance Required**
* Share service name with target AWS Account/VPC

### 🔹 ****Step 6: Create Interface Endpoint in Client VPC****

In VPC 2:

* Go to **VPC → Endpoints → Create Endpoint**
* Choose “Find by service” → Paste the **service name** from VPC 1
* Select **private subnets**
* Attach to security group that allows port 80 traffic

### 🔹 ****Step 7: Accept the Connection (Service VPC)****

If acceptance is enabled:

* Go to **VPC → Endpoint Services**
* Approve the pending connection from the client VPC

### 🔹 ****Step 8: Test the Connection****

From **private EC2 in VPC 2**, run:

**curl http://<interface-endpoint-DNS>**

**o/p:**

Hello from PrivateLink Server

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***