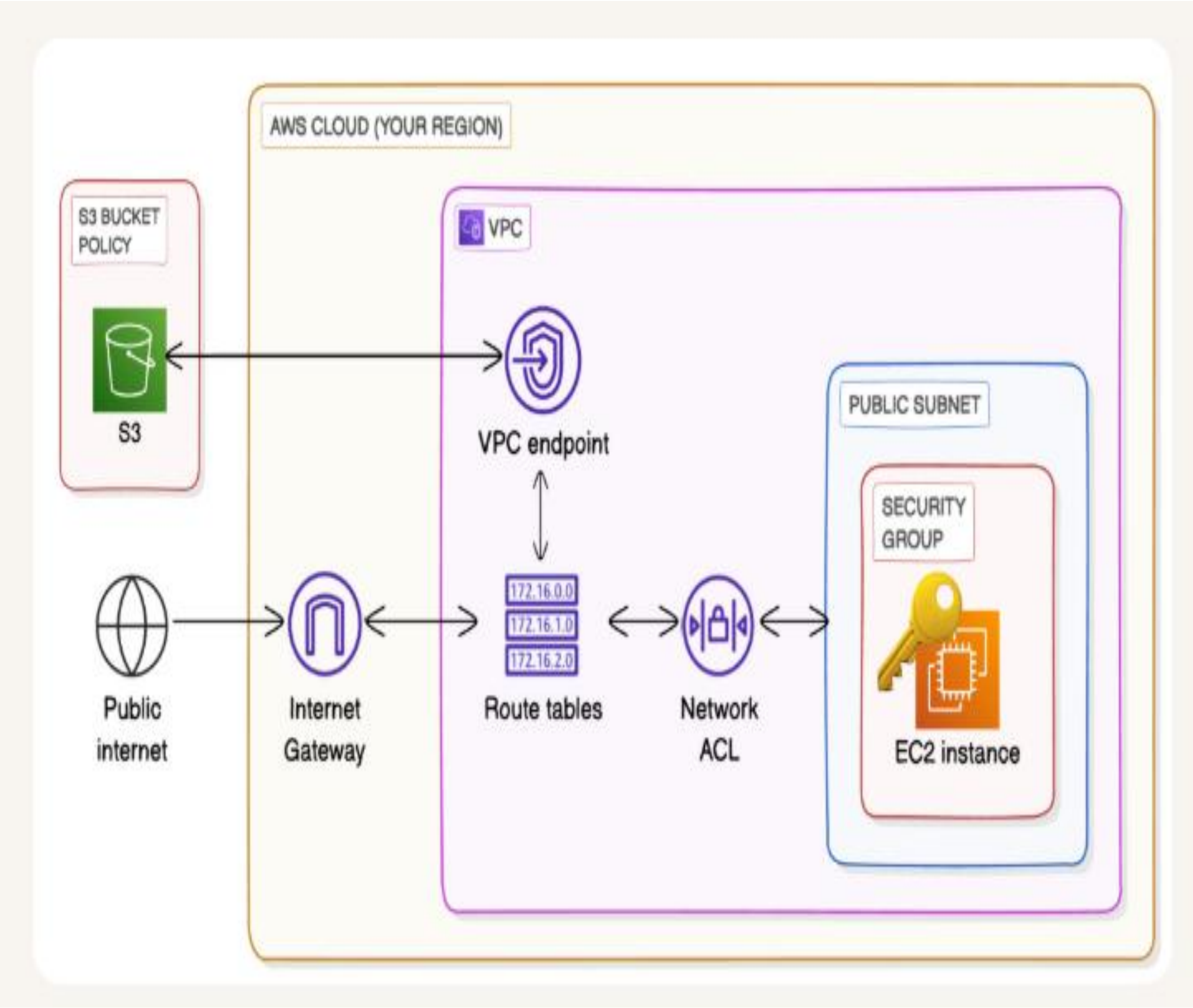
Project 3: Private S3 Access via VPC Gateway Endpoint



Objective: Create an S3 bucket outside the VPC and access it privately from an EC2 instance using a Gateway VPC Endpoint, enforced by a restrictive bucket policy.

Architecture

- VPC (10.0.0.0/16) with one public subnet + EC2 (public IP for EIC).
- S3 bucket (global service, outside VPC).
- Gateway VPC Endpoint for S3 associated to the public route table.
- Bucket policy that denies all unless aws:sourceVpce = your Endpoint ID.

Build Steps

- Create VPC and public subnet; attach IGW; route 0.0.0.0/0 → IGW.
- Launch EC2 with public IP; create SG allowing SSH.
- Create S3 bucket (unique name) and upload 2 test files.
- On EC2, configure AWS CLI with temporary access keys (aws configure).
- Verify internet-based access: `aws s3 ls s3://<bucket>` (should work).
- Create Gateway Endpoint for S3; associate with public route table.
- Apply bucket policy to allow only requests via `aws:sourceVpce` (endpoint ID).
- Re-test: access works via endpoint; flip endpoint policy to Deny → access blocked.

Bucket Policy Template

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<your-bucket>",
        "arn:aws:s3:::<your-bucket>/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-xxxxxxxx"
        }
      }
    }
  ]
}
```