**LAB: AWS VPC Peering Explained with Practical Demo**

**1. Introduction**

* **Scenario:**
  + Company uses AWS with VPCs in multiple regions (e.g., us-east-1, eu-west-1).
  + Need communication between instances (e.g., App Server ↔ DB Server) in different VPCs.
* **Old Solution:** Public endpoints/VPNs → **Issues:** Latency, security risks, cost.
* **New Solution:** **VPC Peering** (secure, low-latency private connection).

**2. Key Concepts**

**VPC Peering Requirements**

* **Non-overlapping CIDR blocks** (e.g., 10.0.0.0/16, 172.16.0.0/16, 192.168.0.0/16).
* **No transitive peering** (direct connections only).
* **Cross-region peering** requires manual route table updates.

**Components Involved**

* **VPCs** (App, Web, DB servers in different regions).
* **Route Tables** (Define paths for traffic).
* **Security Groups** (Temporarily allow all traffic for testing; restrict in production).

**3. Step-by-Step Demo**

**Step 1: Create VPCs**

* **App Server VPC** (North Virginia): 10.0.0.0/16
* **Web Server VPC** (North Virginia): 172.16.0.0/16
* **DB Server VPC** (Ohio): 192.168.0.0/16

**Step 2: Launch Instances**

* **App Server**: Subnet in us-east-1a, Security Group (SG) allows all traffic.
* **Web Server**: Subnet in us-east-1b, SG allows all traffic.
* **DB Server**: Subnet in us-east-2a, SG allows all traffic.

**Step 3: Establish VPC Peering**

1. **Same-Region Peering (App ↔ Web in**us-east-1**)**
   * Create peering connection (app-to-web).
   * **Accept request** in target VPC.
   * Update **Route Tables**:
     + App VPC: Add route to 172.16.0.0/16 via peering connection.
     + Web VPC: Add route to 10.0.0.0/16 via peering connection.
   * **Test**: Ping between instances (should work).
2. **Cross-Region Peering (App ↔ DB in**us-east-1**↔**us-east-2**)**
   * Create peering connection (app-to-db).
   * **Accept request** in Ohio region.
   * Update **Route Tables**:
     + App VPC: Add route to 192.168.0.0/16 via peering.
     + DB VPC: Add route to 10.0.0.0/16 via peering.
   * **Test**: Ping from DB to App instance.
3. **Web ↔ DB Peering**
   * Repeat steps for web-to-db peering.

**4. Diagram**

plaintext

Copy

Download

[us-east-1]

App Server (10.0.0.0/16) ↔ Web Server (172.16.0.0/16)

↓

[us-east-2]

DB Server (192.168.0.0/16)

**5. Best Practices & Warnings**

* **Security Groups**: Never allow All Traffic in production; restrict to specific ports.
* **CIDR Blocks**: Ensure no overlap between VPCs.
* **Documentation**: Share your lab work on LinkedIn/Medium to showcase skills.