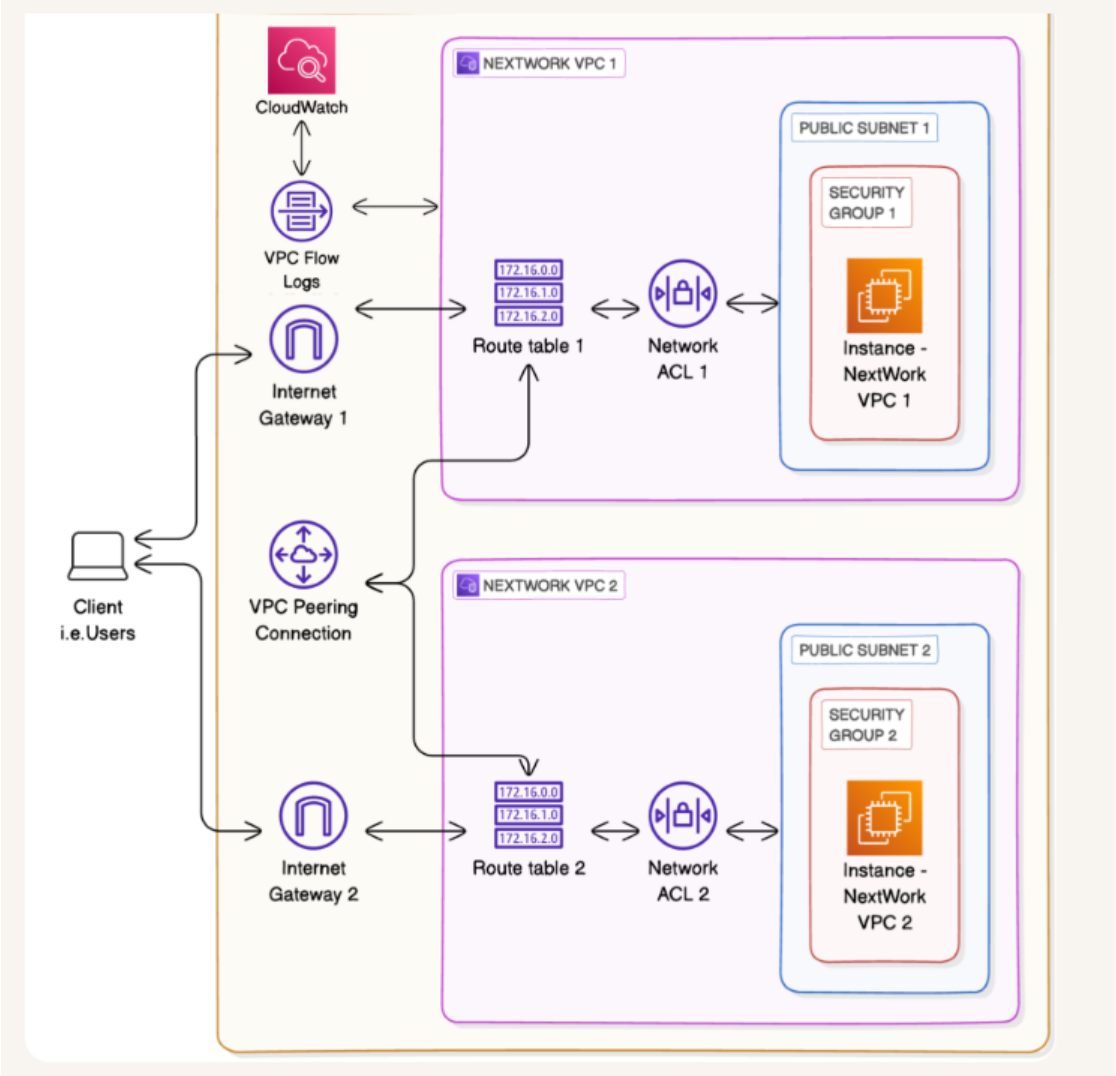
Project 2: VPC Peering + VPC Flow Logs (CloudWatch)



Objective: Create two VPCs, peer them for private communication, then enable Flow Logs to capture and analyze network traffic in CloudWatch.

Architecture

- VPC 1: 10.1.0.0/16 (public subnet + EC2)
- VPC 2: 10.2.0.0/16 (public subnet + EC2)
- Security Groups: allow 'All ICMP - IPv4' (ping)
- VPC Peering: VPC1 ↔ VPC2 (same Region)
- Routing:
- • VPC1 RT: 10.2.0.0/16 → peering connection
- • VPC2 RT: 10.1.0.0/16 → peering connection
- Monitoring: Flow Logs → CloudWatch log group; IAM role with logs:* actions

Build Steps

- Create VPC1 (10.1.0.0/16) & VPC2 (10.2.0.0/16).
- Add one public subnet each and launch EC2 (Amazon Linux 2023, t2.micro, public IP enabled).
- Create SGs to allow All ICMP - IPv4 for test pings.
- Create VPC Peering: VPC1 requester → VPC2 accepter; accept request.
- Update route tables with the opposite VPC CIDRs to the peering connection target.

Enable VPC Flow Logs to CloudWatch

- Create CloudWatch Log Group: NextWorkVPCFlowLogsGroup.
- Create IAM Policy (logs:CreateLogGroup, CreateLogStream, PutLogEvents, Describe*).
- Create IAM Role with trust: Service = vpc-flow-logs.amazonaws.com; attach policy.
- Create Flow Logs on VPC(s) → destination: CloudWatch → select role & log group.

Validate

From VPC1 EC2 via EC2 Instance Connect:

```
ping <vpc2-private-ip>
# also try: ping <vpc2-public-ip>
```

- Use CloudWatch Logs Insights sample query: Top 10 byte transfers by src/dst.