Armageddon Project: California VPC Contribution

This Terraform project is part of the **Armageddon Project**, which aims to deploy a global J-Tele-Doctor application for Tokyo Midtown Medical Center (TMMC). The California VPC module contributes to the localized application hosting requirements in the **California region**, ensuring scalability, security, and compliance with project-specific guidelines.

---

1. Project Scenario

TMMC seeks to expand its telemedicine services to Japanese and foreign customers abroad. The goal is to enable customers to consult doctors remotely while maintaining strict data privacy and security. As part of the project, AWS regions across the globe, including California, must host application infrastructure compliant with local and global requirements.

---

2. Purpose of the California VPC Module

The California VPC module is designed to:

- Provide a secure and scalable infrastructure for local application hosting.
- Comply with the following **Stage One** requirements:
    1. Deploy infrastructure in the **California region** with at least two availability zones (AZs).
    2. Use an Auto Scaling Group (ASG) for redundancy and fault tolerance.
    3. Include at least one EC2 instance for current test deployment.
    4. Transfer syslog data securely to Japan while ensuring the data is stored in private subnets.
    5. Open only **port 80** to the public for application access.

---

3. Key Contributions of the California VPC Module

a. Networking

- **VPC CIDR Block**: `10.106.0.0/16` (65,536 IP addresses for future scalability).
- **Subnets**:
    - Public Subnets:
        - `10.106.1.0/24` in AZ 1
        - `10.106.2.0/24` in AZ 2
    - Private Subnets (syslog data and backend instances):
        - `10.106.101.0/24` in AZ 1
        - `10.106.102.0/24` in AZ 2
- **Internet Gateway**: Provides internet connectivity for public resources.
- **NAT Gateway**: Facilitates secure internet access for private subnets.

b. Compute

- **Auto Scaling Group (ASG)**:
    - Minimum Instances: 2
    - Maximum Instances: 6
    - Desired Instances: 3
    - Ensures availability across AZs for fault tolerance.
- **EC2 Instances**:
    - Instance Type: `t3.micro` (for test deployment).
    - AMI: Amazon Linux 2.
    - User Data: Configured to support syslog integration.

c. Security

- **Security Groups**:
    - Inbound Rule: Allows HTTP traffic on port 80 only.
    - Outbound Rule: Allows all necessary application traffic.
- **Private Subnets**:
    - Syslog data storage is isolated in private subnets to comply with data transfer limitations.

d. Routing

- **Public Subnet Route**:
    - Default route to the Internet Gateway for internet traffic.
- **Private Subnet Route**:
    - Default route to the NAT Gateway for secure outbound traffic.

e. Outputs

- VPC ID and subnet IDs for monitoring and verification.
- Load Balancer DNS name for accessing the deployed application.

---

4. Deployment Workflow

Initialize Terraform

terraform init

1.

Plan the Deployment

terraform plan

2.

Apply the Configuration

terraform apply

3.
4. **Verify Outputs** Use the Terraform outputs to:
    - Access the application via the load balancer.
    - Verify resource IDs and configurations in the AWS console.

---

5. Compliance with Project Requirements

Requirement	California VPC Contribution
Deploy ASG with a minimum of 2 AZs	Configured ASG spans two AZs in California with redundancy.
Deploy at least 1 EC2 for test purposes	One `t3.micro` instance included for testing.

Transfer syslog data securely	Syslog data is stored in private subnets, ready for transfer to Japan.
Open only port 80	Security groups restrict public access to port 80.
Store syslog data in private subnets	Ensures syslog data remains isolated and secure within private subnets.

---

6. Overall Value

The California VPC module provides a robust infrastructure for localized hosting while meeting the Armageddon Project's global compliance and scalability requirements. It ensures:

- **Fault Tolerance**: Multi-AZ deployment.
- **Scalability**: Auto Scaling adapts to traffic demand.
- **Data Security**: Strict compliance with syslog and private subnet restrictions.
