**Practical Guide: Setting up a Basic Network on Huawei Cloud**

This guide will walk you through the process of creating a VPC, two subnets, custom route tables, security groups, and an Elastic Load Balancer (ELB) to distribute traffic to two backend servers.

**Prerequisites:**

* An active Huawei Cloud account.
* Two Elastic Cloud Server (ECS) instances already deployed in the same region where you plan to create your VPC. These will serve as your backend servers.

**Step 1: Create a Virtual Private Cloud (VPC)**

1. Log in to the Huawei Cloud console.
2. Navigate to **Networking** > **Virtual Private Cloud (VPC)**.
3. Click **Create VPC**.
4. Configure the following:
   * **Name:** my-demo-vpc
   * **Region:** Select your desired region.
   * **IPv4 CIDR Block:** 10.0.0.0/16
5. Click **Create Now**.

**Step 2: Create Two Subnets**

Now, create two subnets within your new VPC.

1. In the VPC console, click on the VPC you just created (my-demo-vpc).
2. Go to the **Subnets** tab and click **Create Subnet**.
3. **Subnet 1 (Web Tier):**
   * **Name:** subnet-web
   * **CIDR Block:** 10.0.1.0/24
   * **Availability Zone:** Select a preferred AZ (e.g., AZ1).
   * **Gateway:** 10.0.1.1
4. Click **Create Now**.
5. **Subnet 2 (App Tier):**
   * **Name:** subnet-app
   * **CIDR Block:** 10.0.2.0/24
   * **Availability Zone:** Select a different AZ (e.g., AZ2).
   * **Gateway:** 10.0.2.1
6. Click **Create Now**.

**Step 3: Configure Custom Route Tables**

Every VPC has a default route table. In this step, we'll create a custom one to show how to control traffic flow.

1. In the VPC console, navigate to the **Route Tables** section.
2. Click **Create Route Table**.
3. **Name:** my-custom-routes
4. **VPC:** Select my-demo-vpc.
5. Click **Create Now**.
6. Click on your new route table's name (my-custom-routes).
7. Go to the **Routes** tab and click **Add Route**.
8. **Example Route:** Let's say you want to route traffic for a specific network (172.16.0.0/16) through a NAT Gateway or another VPC peering connection.
   * **Destination CIDR Block:** 172.16.0.0/16
   * **Next Hop Type:** Select the appropriate next hop (e.g., NAT Gateway).
   * **Next Hop:** Select the specific instance or gateway.
9. Now, associate this custom route table with a subnet. Go to the **Associations** tab, click **Associate Subnet**, and select subnet-app. Click **OK**. The subnet-web will continue to use the default route table.

**Step 4: Create and Apply Security Groups**

1. Navigate to **Networking** > **Security Groups** in the VPC console.
2. Click **Create Security Group**.
3. **Name:** web-tier-security-group
4. **Description:** Rules for web servers
5. Click **Create Now**.
6. Click on the security group name. Add the following inbound rules:
   * **Rule 1 (HTTP traffic):**
     + **Direction:** Inbound
     + **Protocol:** TCP
     + **Port:** 80
     + **Source:** 0.0.0.0/0 (Allows all public IPs)
   * **Rule 2 (SSH access):**
     + **Direction:** Inbound
     + **Protocol:** TCP
     + **Port:** 22
     + **Source:** 0.0.0.0/0 (For demonstration, but for production, restrict this to your specific IP)
7. Create another security group named elb-access-security-group with the same inbound rules for SSH and HTTP. This will be used to restrict access from the load balancer to the backend servers.
8. To apply a security group, go to the **Elastic Cloud Server** service, select your ECS instances, and on their details page, modify their security groups to include web-tier-security-group and elb-access-security-group.

**Step 5: Set up an Elastic Load Balancer (ELB)**

1. Navigate to **Networking** > **Elastic Load Balance (ELB)**.
2. Click **Create Load Balancer**.
3. **Basic Settings:**
   * **Load Balancer Type:** Dedicated or Shared (Dedicated is recommended for production).
   * **Network Type:** Public or Internal.
   * **VPC:** Select my-demo-vpc.
   * **Subnet:** Select subnet-web.
   * **Bandwidth:** Set as needed.
4. **Listener Settings:**
   * **Listener Protocol:** HTTP
   * **Port:** 80
   * **Backend Protocol:** HTTP
   * **Port:** 80
5. **Backend Server Group:**
   * **Name:** my-web-servers
   * **VPC:** my-demo-vpc
   * **Health Check:** Configure health check parameters (e.g., HTTP path /, port 80).
6. **Add Backend Servers:**
   * In the backend server group details, click **Add Servers**.
   * Select your two ECS instances from the list.
7. Review all the settings and click **Create Now**.

Your ELB is now configured to distribute traffic on port 80 to your two ECS instances, and your security groups will ensure only the necessary traffic can reach them