

**Step 1: Create a New VPC**

1. Log in to the AWS Management Console.
2. Navigate to the VPC Dashboard:
   * Go to Services > VPC.
3. Create a New VPC:
   * In the VPC Dashboard, click Create VPC.
   * Choose VPC only.
   * Provide the following details:
     + Name tag: CustomVPC.
     + IPv4 CIDR block: 10.0.0.0/16. Or 192.168.0.0./16
     + IPv6 CIDR block: None (unless needed).
     + Tenancy: Default (unless you need dedicated hardware).
   * Click Create VPC.

**Step 2: Create Subnets**

1. **Public Subnet:**
   * Go to Subnets in the VPC Dashboard and click Create subnet.
   * Select the CustomVPC you just created.
   * Provide the following details:
     + Subnet name: PublicSubnet.
     + Availability Zone: Choose any zone (e.g., us-east-1a).
     + IPv4 CIDR block: 10.0.1.0/24.
   * Click Create subnet.
2. **Private Subnet:**
   * Repeat the steps above to create a private subnet.
   * Use the following details:
     + Subnet name: PrivateSubnet.
     + Availability Zone: Choose the same zone as the public subnet.
     + IPv4 CIDR block: 10.0.2.0/24.
   * Click Create subnet.

**Step 3: Configure the Internet Gateway**

1. Create an Internet Gateway:
   * Go to Internet Gateways in the VPC Dashboard.
   * Click Create internet gateway.
   * Provide a name tag (e.g., CustomIGW) and click Create.
2. Attach the Internet Gateway to the VPC:
   * Select the created internet gateway.
   * Click Actions > Attach to VPC.
   * Select CustomVPC and click Attach.

**Step 4: Configure Route Tables**

1. Public Route Table:
   * Go to Route Tables and click Create route table.
   * Provide a name tag (e.g., PublicRouteTable).
   * Select the CustomVPC and click Create.
2. Add Routes to the Public Route Table:
   * Select the created route table.
   * Go to the Routes tab and click Edit routes.
   * Add a route:
     + Destination: 0.0.0.0/0.
     + Target: Select the Internet Gateway (CustomIGW).
   * Click Save changes.
3. Associate the Public Subnet with the Route Table:
   * Go to the Subnet associations tab and click Edit subnet associations.
   * Select PublicSubnet and click Save.

**Step 5: Launch an EC2 Instance in the Private Subnet**

1. Go to EC2 Dashboard and click Launch instance.
2. Configure the Instance:
   * Choose an Amazon Machine Image (AMI), e.g., Amazon Linux 2 AMI.
   * Select an instance type (e.g., t2.micro).
   * In the Network settings:
     + Select CustomVPC.
     + For the Subnet, select PrivateSubnet.
     + Ensure that Auto-assign Public IP is disabled.
   * Click Launch and select a key pair for SSH access.
3. Verify the Instance Launch:
   * Go to the Instances page and check the status of the EC2 instance.

**Step 6: Set Up a VPN Gateway**

1. Create a Virtual Private Gateway:
   * Go to Virtual Private Gateways and click Create virtual private gateway.
   * Provide a name tag (e.g., CustomVPNGateway).
   * Select Amazon default ASN and click Create.
2. Attach the VPN Gateway to the VPC:
   * Select the created virtual private gateway.
   * Click Actions > Attach to VPC.
   * Select CustomVPC and click Attach.
3. Create a Customer Gateway:
   * Go to Customer Gateways and click Create customer gateway.
   * Provide a name (e.g., CustomerVPN).
   * Choose Static routing and enter the public IP address of your on-premises network (or any external system).
   * Click Create customer gateway.
4. Set Up a VPN Connection:
   * Go to Site-to-Site VPN Connections and click Create VPN connection.
   * Provide the following details:
     + Name tag: CustomVPNConnection.
     + Target gateway type: Virtual private gateway.
     + Virtual private gateway: Select CustomVPNGateway.
     + Customer gateway: Select CustomerVPN.
     + Routing options: Static.
     + Static IP prefixes: Enter your on-premises IP range.
   * Click Create VPN connection.
5. Download the VPN Configuration:
   * Once the VPN connection is created, download the configuration file compatible with your router.

Step 7: Test the VPN Connection

1. Configure your on-premises router or firewall using the downloaded VPN configuration.
2. Ensure that the VPN tunnel is active.
3. Verify that instances in the private subnet can be accessed from your on-premises network through the VPN.

**Network IP address and related configurations on an Ubuntu system**

**ubuntu@ip-172-31-11-39:~$ sudo apt-get update**

**ubuntu@ip-172-31-11-39:~$ sudo apt install net-tools**

**ubuntu@ip-172-31-11-39:~$ ifconfig**

1. ip addr - Show IP addresses of all network interfaces

2. ifconfig - Display active network interfaces (requires net-tools)

3. ip route show - Check default gateway

4. cat /etc/resolv.conf - Show DNS server configuration

5. ping -c 4 google.com - Ping a website to test connectivity

6. ping -c 4 <gateway-ip> - Ping the default gateway

7. systemctl status networking - Check network service status

8. ethtool <interface-name> - View detailed network interface statistics

9. ip link show - Display network interfaces

10. nmcli dev show - Show network device information

11. dig google.com - Perform a DNS lookup

12. nslookup google.com - Perform a DNS query

13. traceroute google.com - Trace the route packets take to a destination (requires traceroute)

14. netstat -r - Display routing table (requires net-tools)

15. ss -tuln - Show listening ports and services

16. curl ifconfig.me - Display external/public IP address

17. host google.com - Look up DNS information for a domain

18. wget --spider google.com - Check if a website is reachable

19. mtr google.com - Network diagnostics and real-time traceroute (requires mtr)

20. arp -a - Display ARP table