**Steps:**

1. **Planning:**

* Define the project scope, including the required resources (e.g., number of EC2 instances, subnets, security groups).
* Determine the region in which you'll create the VPC.
* Plan IP addressing for the VPC and subnets.

1. **Create a VPC:**

* Go to the AWS Management Console and navigate to the VPC service.
* Create a new VPC with an appropriate CIDR block.
* Create public and private subnets within the VPC. Public subnets will have internet access, while private subnets will not be directly accessible from the internet

**3. Internet Gateway (IGW):**

* Create an Internet Gateway and attach it to the VPC.
* Update route tables to route traffic destined for the internet through the IGW.

**4. NAT Gateway (optional for private subnets):**

* If you have private subnets, create a NAT Gateway in a public subnet.
* Update route tables of private subnets to route outbound traffic through the NAT Gateway.

1. **Security Groups:**

* Create security groups for EC2 instances. Define inbound and outbound rules to control traffic.
* Ensure that only necessary ports are open, and access is restricted based on IP ranges.

1. **EC2 Instances:**

* Launch EC2 instances within the appropriate subnets.
* Choose appropriate instance types and Amazon Machine Images (AMIs) based on your requirements.
* Assign security groups created earlier to the instances.

1. **Key Pairs:**

* Create SSH key pairs for Linux instances or password authentication for Windows instances.
* Use these key pairs to securely connect to the instances.

1. **Testing:**

* Test connectivity to the EC2 instances.
* Ensure that security measures are effective and traffic flows as expected.

1. **Monitoring and Maintenance:**

* Set up monitoring and logging for the VPC and EC2 instances.
* Regularly review security groups, NACLs, and other configurations for any necessary updates or improvements.