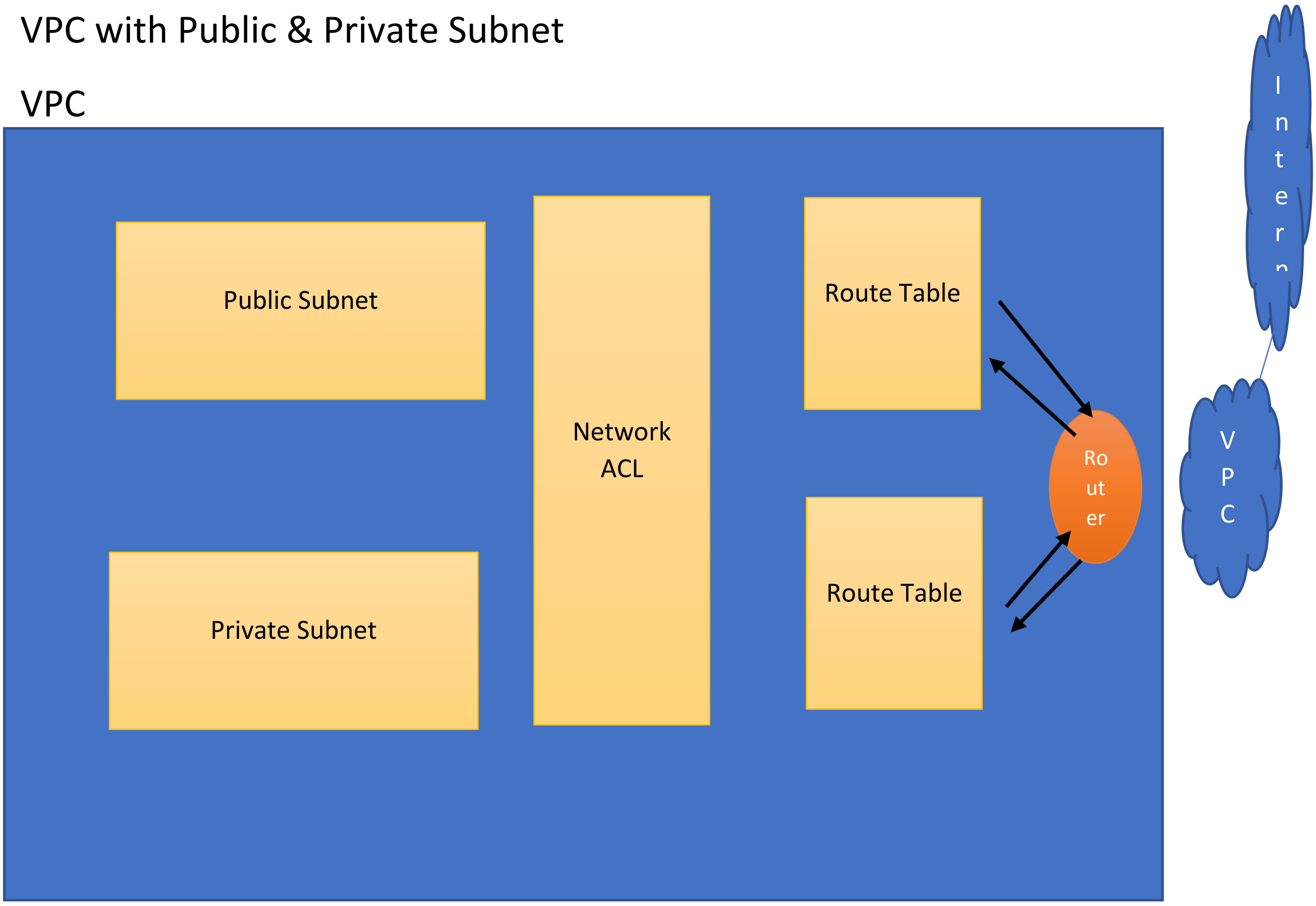
Bastion Host

A bastion Host is a special purpose computer on a public ip designed and configured to withstand attacks

Proxy server

VPC with Public & Private Subnet

VPC



Key points about Bastion host

Bastion Host will be launched in public subnets it acts as a proxy to the private subnets.

It provides secured infra by reducing attacks

A bastion host is also used to administer EC2 instances using SSH securely.

The other name of Bastion Host is called as Jump Boxes

You cannot use NAT-Gatway as a Bastion Host

Whenever you want to SSH your private subnet you can configure a Bastion host.

1. Create VPC called "BasVPC" CIDR-
    a. 10.40.0.0/16
2. Create 1 public subnet & private subnet in the vpc
    a. Public subnet 10.40.1.0/24
    b. Private subnet 10.40.2.0/24
3. Configure the network by editing routing table and do the subnet associations
4. Launch instance(VM) in public subnet with public IP enabled
5. Launch 2 instances(VM) in private subnet where public IP is disabled
6. Do SSH to public VM
7. In Public VM create Bastion host
    a. Copy paste the pem file of your private instance
        i. vi bashtion.pem
    b. Provide access rights to the pem file
        i. Chmod 400 bashtion.pem
    c. Add agent bash
        i. ssh-agent bash
        ii. ssh-add bashtion.pem
    d. ping public instance to the internet

        i. ping www.google.com

    e. SSH to private instance via public instance

        i. Ssh -A ec2-user@<<Private IP of VM>>

    f. Ping private instance to internet

        i. Ping www.google.com

8. Through public vm connect(SSH) to private VM.