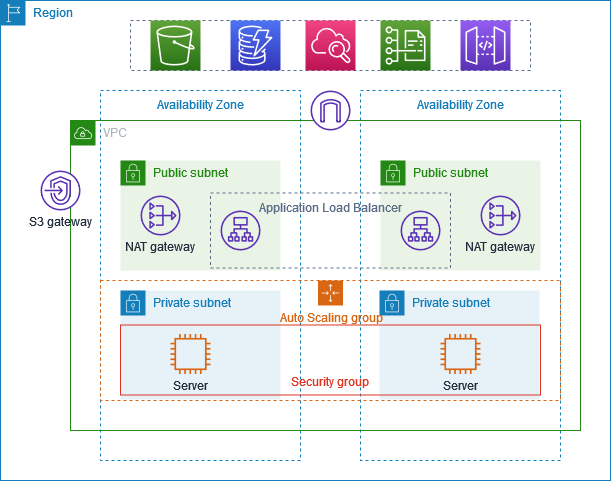
**VPC with servers in private subnets and NAT**



The above diagram is the creation of VPC that you can use for servers

To improve resiliency, you deploy servers in two availability zones, by using an Auto scaling group and an Application load balancer. For additional security, you deploy servers in private subnets. The servers receive requests through load balancer. The servers can connect to internet using NAT gateway. To improve resiliency, you deploy NAT gateway in both availability zones.

**STEP BY STEP PROCEDURE:**

**1. VPC (Virtual Private Cloud):**

**- A virtual network dedicated to your AWS account.**

**- You define IP address ranges using CIDR blocks (e.g., 10.0.0.0/16).**

**2. Subnets:**

**- Subdivide a VPC into smaller IP ranges.**

**- Public Subnet: Has route to Internet Gateway.**

**- Private Subnet: No direct route to Internet Gateway.**

**3. Route Tables:**

**- Determine traffic routing within the VPC.**

**- Each subnet must be associated with a route table.**

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

**- Enables communication between instances in your VPC and the internet.**

**- Must be attached to the VPC and routes must be configured.**

**5. NAT Gateway / NAT Instance:**

**- Allow instances in private subnets to access the internet for updates without exposing them to incoming traffic**

**6. Security Groups:**

**- Act as virtual firewalls for instances to control inbound and outbound traffic.**

**7. Network Access Control Lists (NACLs):**

**- Optional layer of security that acts at the subnet level.**

**8. VPC Peering:**

**- Connects one VPC with another via private IP addresses.**

**9. VPN and Direct Connect:**

**- Enable secure connections from on-premise networks to AWS.**

**10. Flow Logs:**

**- Capture information about the IP traffic going to and from network interfaces.**

**VPC Design Best Practices:**

**- Design for availability: Use multiple AZs.**

**- Use security groups and NACLs wisely.**

**- Monitor using VPC Flow Logs.**

**- Isolate critical resources in private subnets.**