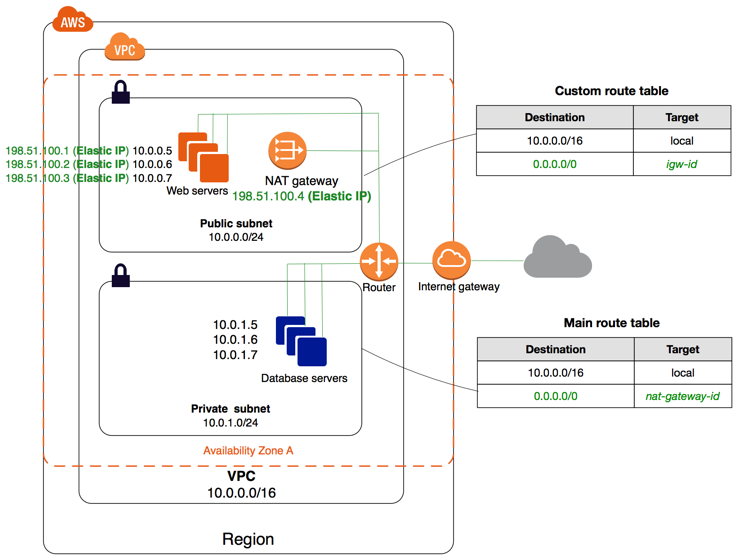
**Component used in VPC**



**Router (Logical Router)-**

* It work as a central router which help to connect different availability zone subnet with each other, it also connect out subnet with internet gateway.
* In one VPC we can create 200 Route table in VPS, create 50 routes entries per route table.
* Each subnet must be associated with only one route table at a given time.
* if we not specify subnet route table associate then the subnet will be associated with the default VPC route table.
* we can also edit main route table as per requirement but cant delete main route table.

=======================================================

**Internet Gateway -**

* It also works as a logical/virtual router, which help to connect a vpc to internet.
* Default VPC is by default connected with internet gateway.
* If we create new custom VPC then we need to connect the internet gateway in order to access to internet.
* It also performs the NAT between your private and public ipv4 address, it support for ipv4 & ipv6.

==================================================================

**NAT Gateway -**

* It always use in public subnet, network address translator use for enable instances in private network to connect internet and other services of AWS, but prevent internet users to connect back to the private instances.
* It is chargeable service when we creating and using NAT gateway in AWS account, it not cover-up in free services.
* To create NAT gateway should be specify the public subnet in which NAT gateway will be setup.
* we need to specify Elastic ip address to associate with NAT gateway when you create it.
* we does not required assign public ip address to private instances.
* After create NAT gateway, we need to update it in routing table of private subnets to enable it when need to connect internet via NAT gateway. so it allow private subnet instances to connect with internet.
* Finally after delete NAT gateway, de-associated its Elastic IP address, but not release from your account ( AWS charge it),release it earlier.

===================================================================

**Security Group:**

* It work as like a Virtual Firewall at ENI(Elastic Network Interface) Level.
* we can create maximum 5 security group for EC2 instance.
* It have only permit rules, does not available deny rules
* It works as a statefull, return traffic, allow inbound traffic is allowd, even if there are no rules to allow it.

**NACL:**

* It is work as a security mechanism work on Logical Router, all traffic come from outside into VPC it filters out from NACL.
* Defaults VPC come with a default Network ACL which allow inbound and outbound traffic allow.
* When we create custom vpc NACL and associate it with a subnet by default, each custom network ACL denies all inbound and outbound traffic until we allow them.
* It work subnet Level, It can have permit and deny rules.

**Security Group vs NACL**

* Security group work at instance level where as NACL work at subnet level.
* Security group have allow rules only where as NACL have allow and deny rules.
* Security group work stateful means return traffic allow automatically where as NACL work stateless means return traffic need to allowed (in/out both)
* Security group applicable Instance only where as NACL applicable in all instances in subnet.