vpc , IGW , nat gateway

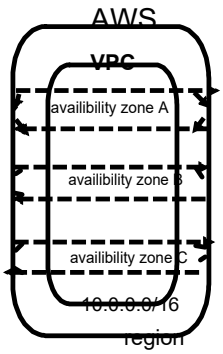
VPC ---Virtual private cloud

virtual network resemble just like traditional network operate in own datacenter

dedicate to your own aws account

logically isolated from other virtual network (region vpc)

aws resources in vpc-------create subnet
----ip address range
----routing table
---network gateway
---security
--vpc nelongs that region
--create a vpc must seeing range of ip address



--vpc not in availability zone it create in region

--different subnet create in vpc

--different subnet for different availability zone

1st CIDR (block) assign vpc is primary CIDR
another secondary CIDR

vpc configuartion

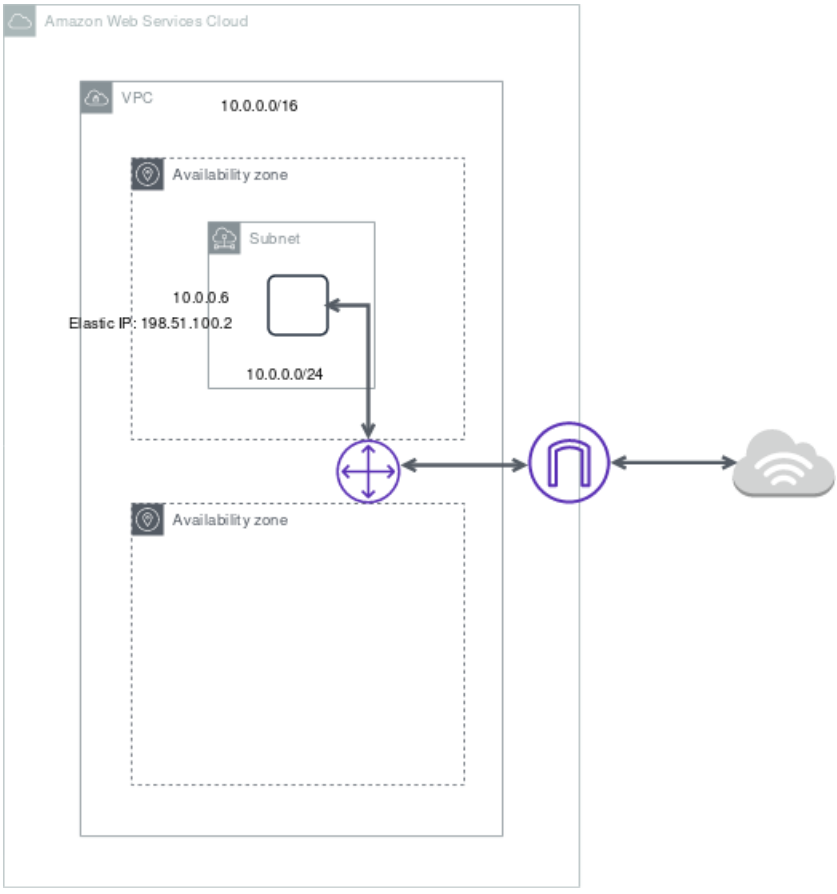
1 vpc with single public subnet
2 vpc with public and private subnet
3 vpc with public and private subnet and hw vpn access
4 vpc with private subnet only and hw vpn access

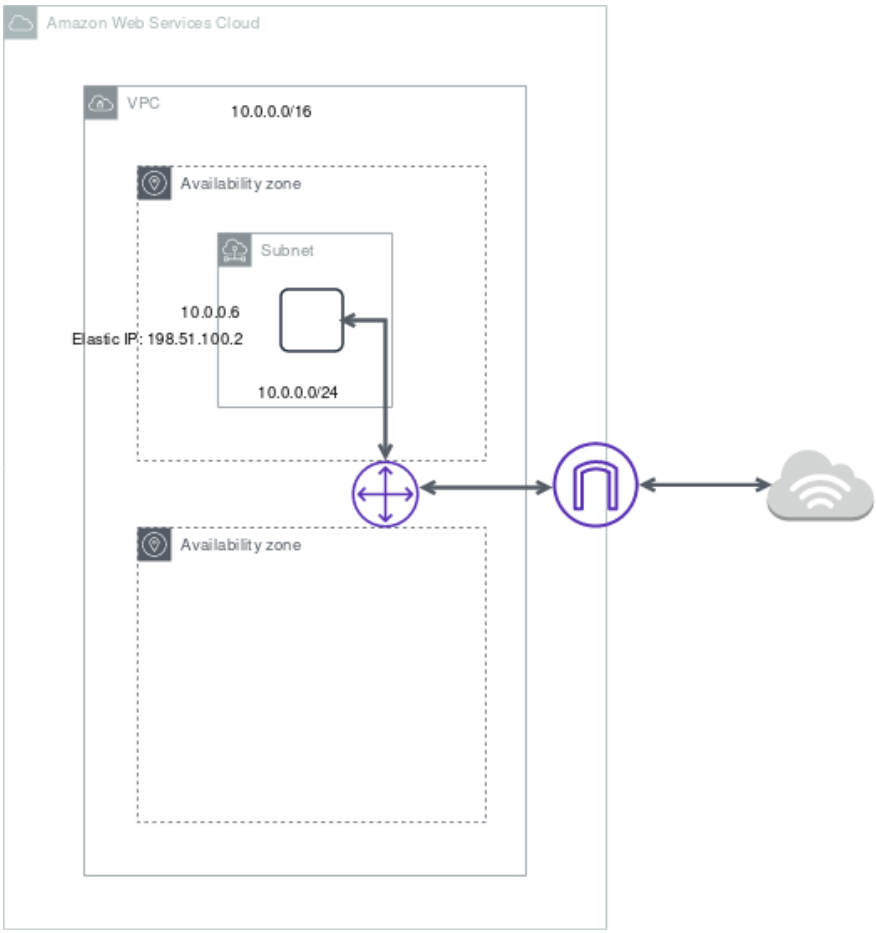
1---vpc with single public subnet

vpc ------availability zone

public subnet------it means a subnet that associate with routing table that has a route to internet gateway and access by internet

network access control list(inbound rule)



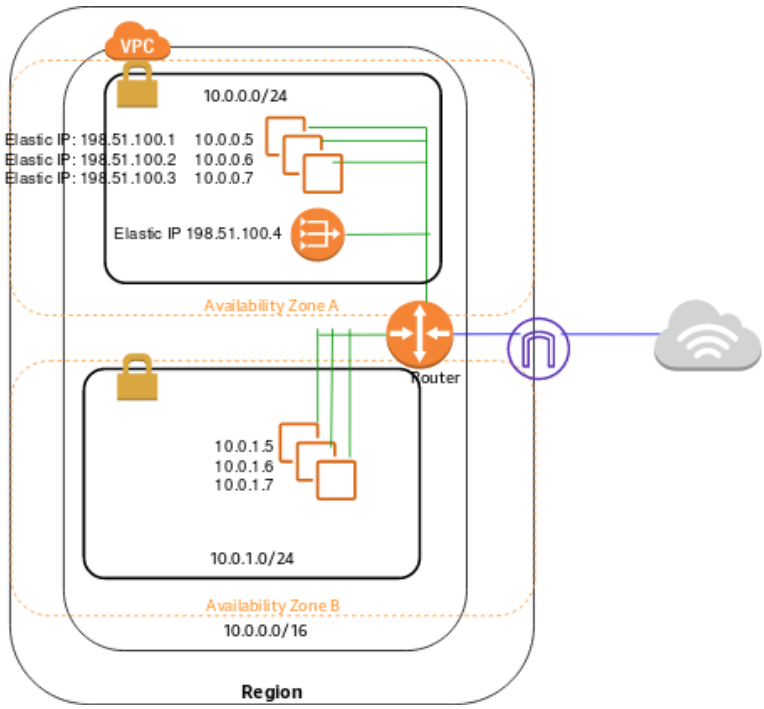

Amazon Web Services Cloud
VPC
10.0.0.0/16
Availability zone
Subnet
10.0.0.6
Elastic IP: 198.51.100.2
10.0.0.0/24
Availability zone

VPC with public and private subnet

one vpc --create two subnet

1st one public---access from Internet (elastic ip)

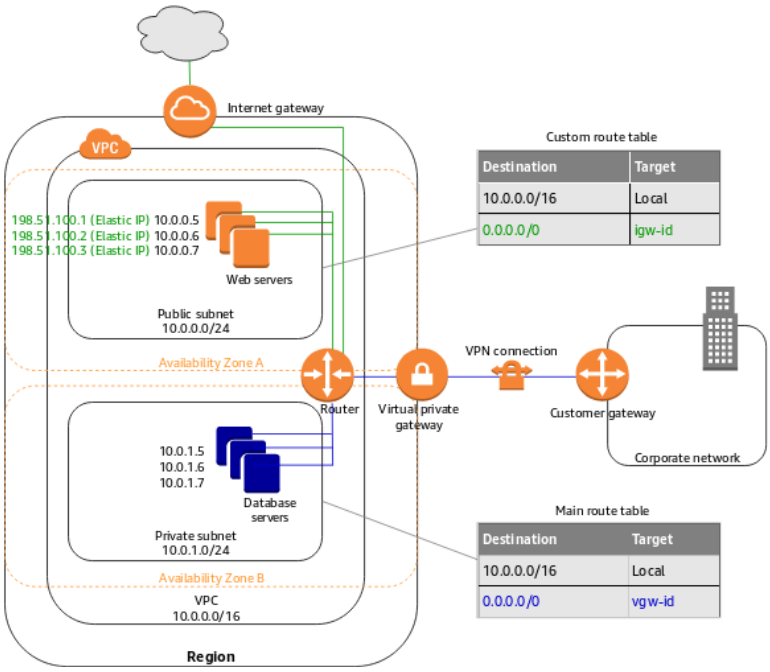
2nd one private ---not access by Internet
access Internet by that machine need NAT gateway



VPC with public and private subnet and hw vpn access

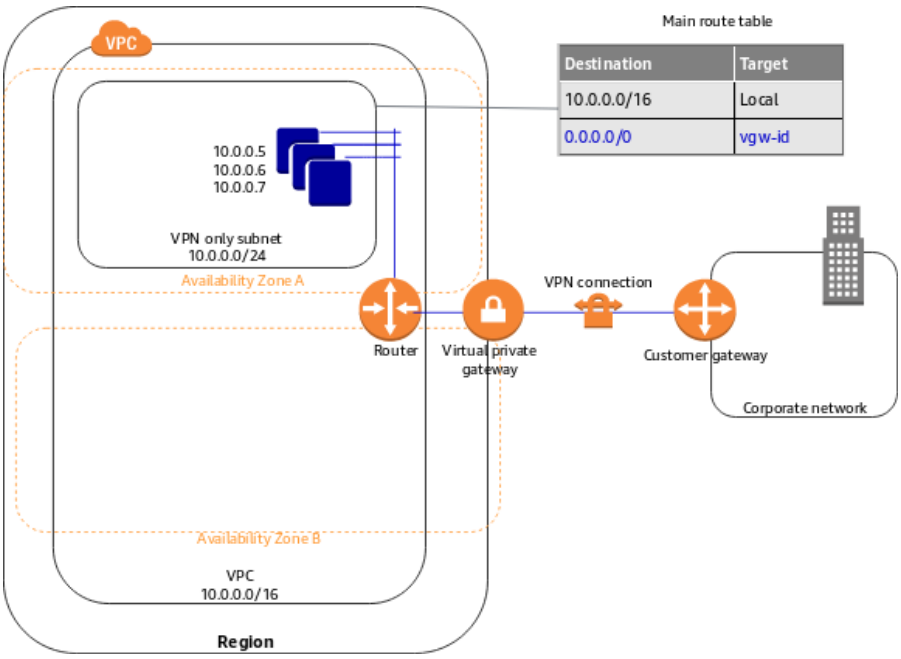
vpc
pubilc sunet
(multiple instace)
public ip

private subnet
multiple subnet
only office or corporate network
vpn se



vpc with private subnet only and hw vpn access

ek vpc ---private subnet
active directory , multiple server dont access from internet
vpc----subnet (private)



VPC

subnet
routing table
Internet gateway
DHCP option set
elastic IP
endpoint
NAT gateway
peering connection
virtual private gateway
customer gateway

subnet

one region--create vpc--create subnet--subnet assign to availibilty zone
AWS resource associate VPC subnet

public subnet
internet access (IGW, elastic ip)
(resources)
public ip

private subnet
does not access from internet
resources

subnet between /16 and /28
first four ip address and last ip addess not available for us
10.0.0.0-------network address
10.0.0.1------for vpc router
10.0.0.2-----DNS server
10.0.0.3-----future use
10.0.0.255-----broadcast address
aws dont support broadcast in vpc
aws reserve this address

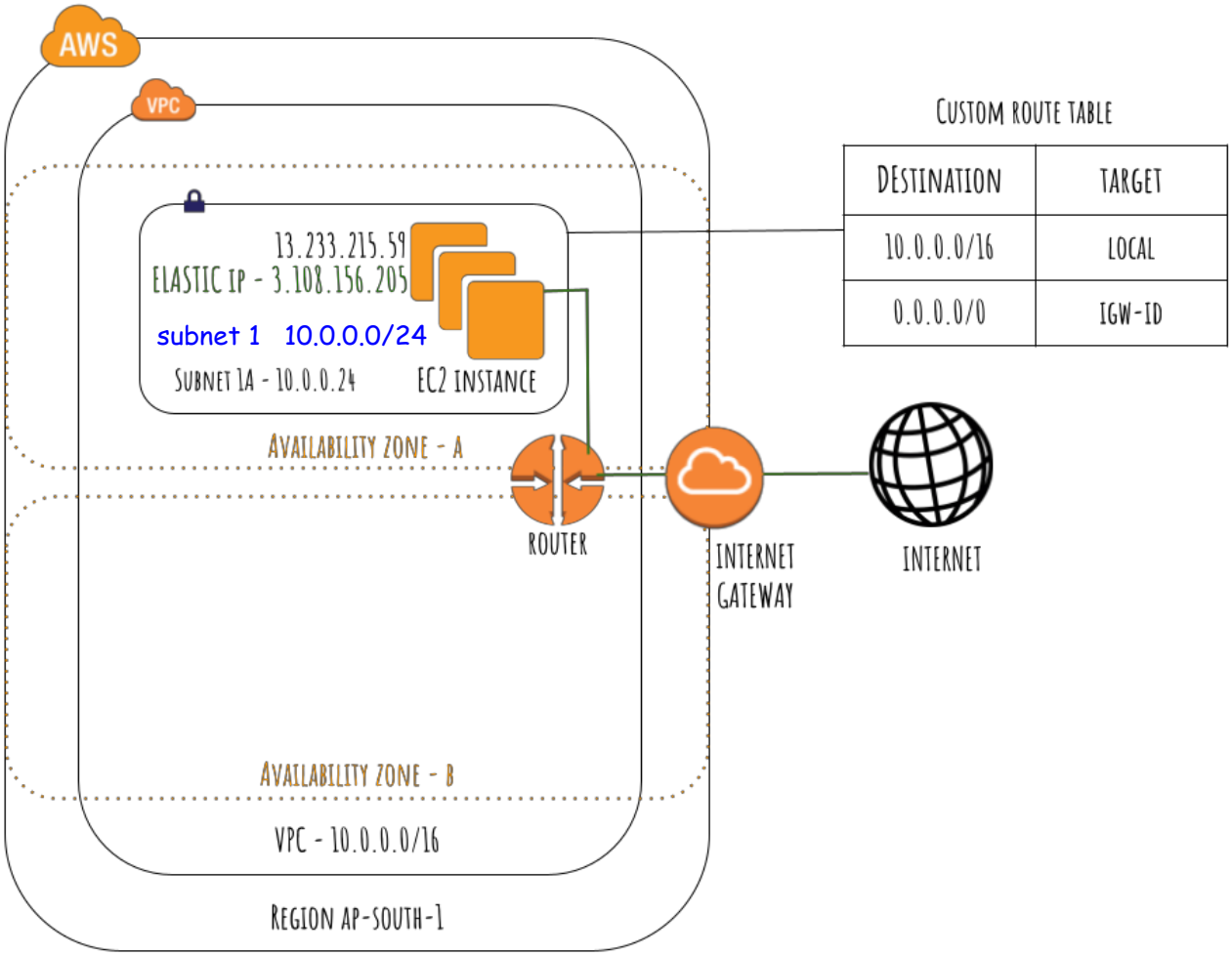
Routing table

--routing table contain rules--direct the network traffic
--each subnet in your vpc must be associated with routing table
--a subnet associtae with only one routing table
--multiple subnet can associate with same routing table
--vpc automatically comes with a main routing table that can modify additional custom routing table
--if we dont associate a subnet with particular table the subnet implicitly associte with main routing table
--routing table controls the routing for the subnet
--you can not delete the main routing table but you can replace the main routing table with custom table that you have created so this table is default table and each new subnet associate with

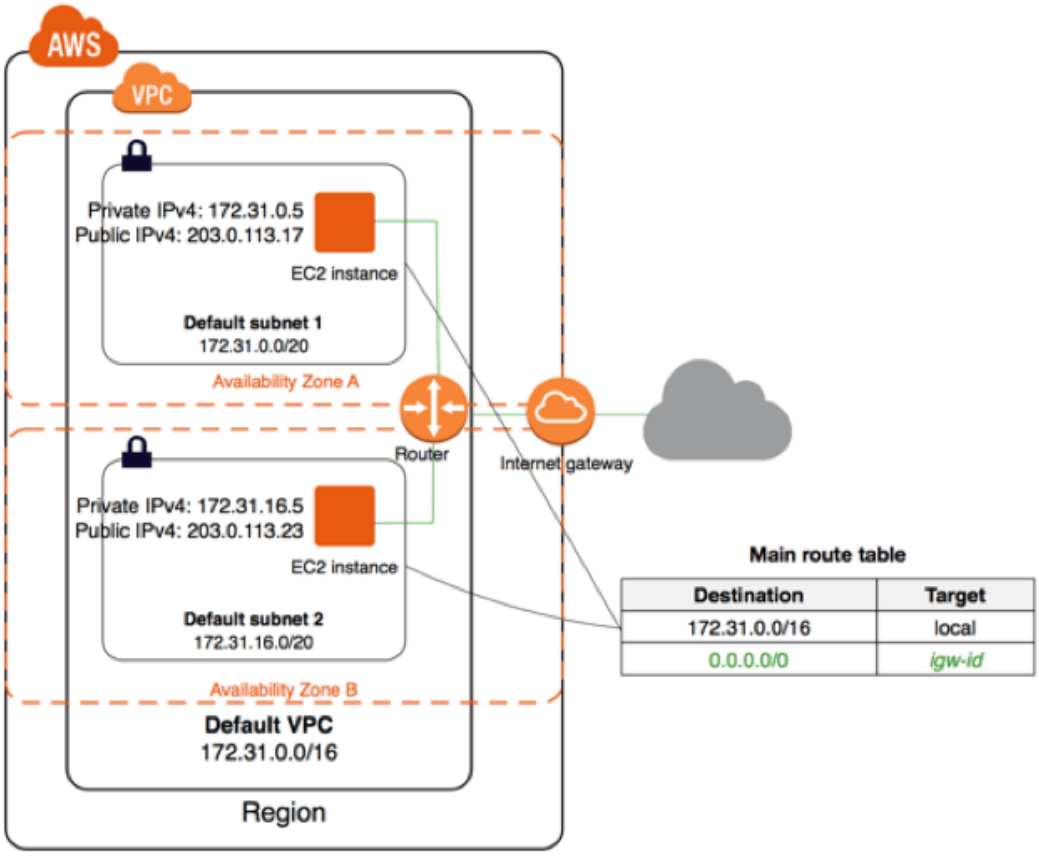
Internet gateway

--internal gateway is a virtual router that connect a vpc to the internet
--default vpc is already attch with internel gateway
--if we create a new vpc then you must attach the Internet gateway in order to access the internet

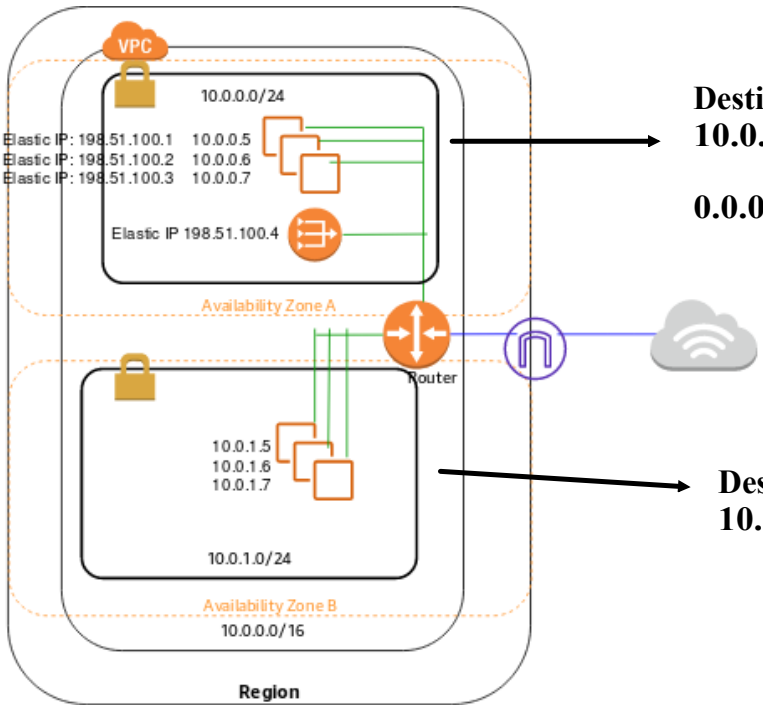
VPC with public subnet



VPC with two public subnet--



vpc configure with public and private subnet



custom routing table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

main routing table

Destination	Target
10.0.0.0/16	local