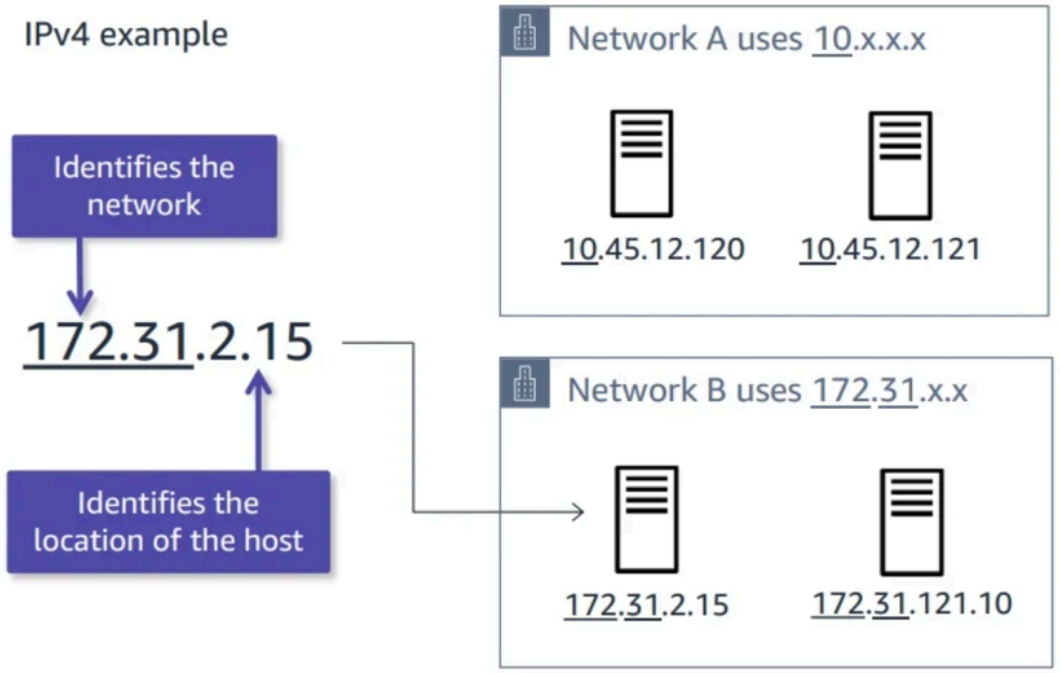
HEPAPI
DIGITAL TRANSITION PARTNER

SESSION-2: NETWORK

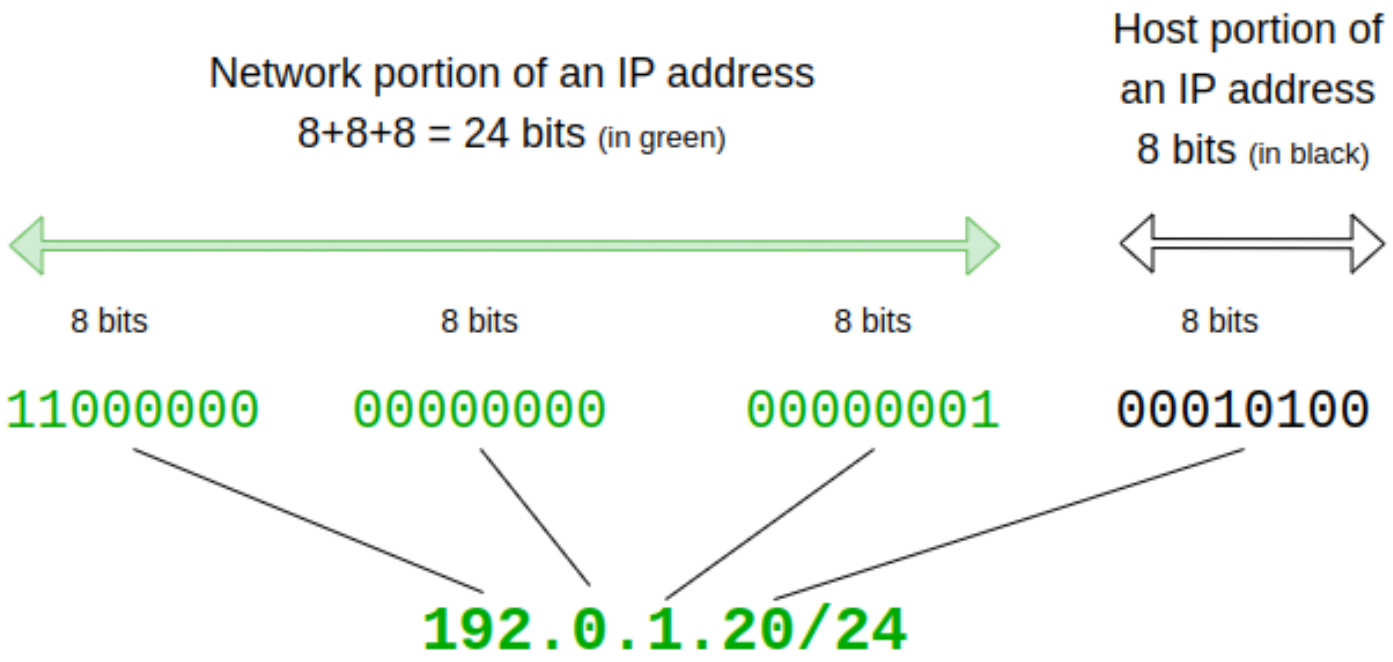
IP Address

- An IP address identifies a location within a network.
- It consists of two parts, the network and the host.
- There are two types of IP address: IPv4 and IPv6



Classless Inter-Domain Routing (CIDR)

- CIDR specifies a range of IP addresses called a CIDR block.

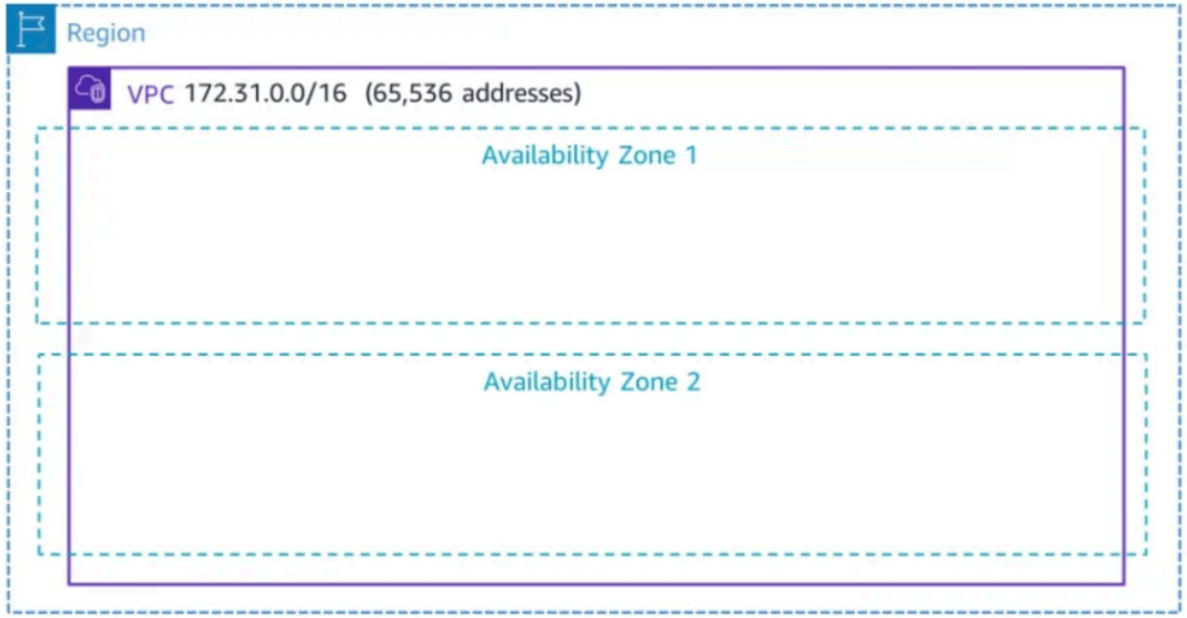


VPC Topics

- Amazon VPC
- Subnets
- Internet Gateway
- Route Table
- Elastic IP address
- NAT Gateway

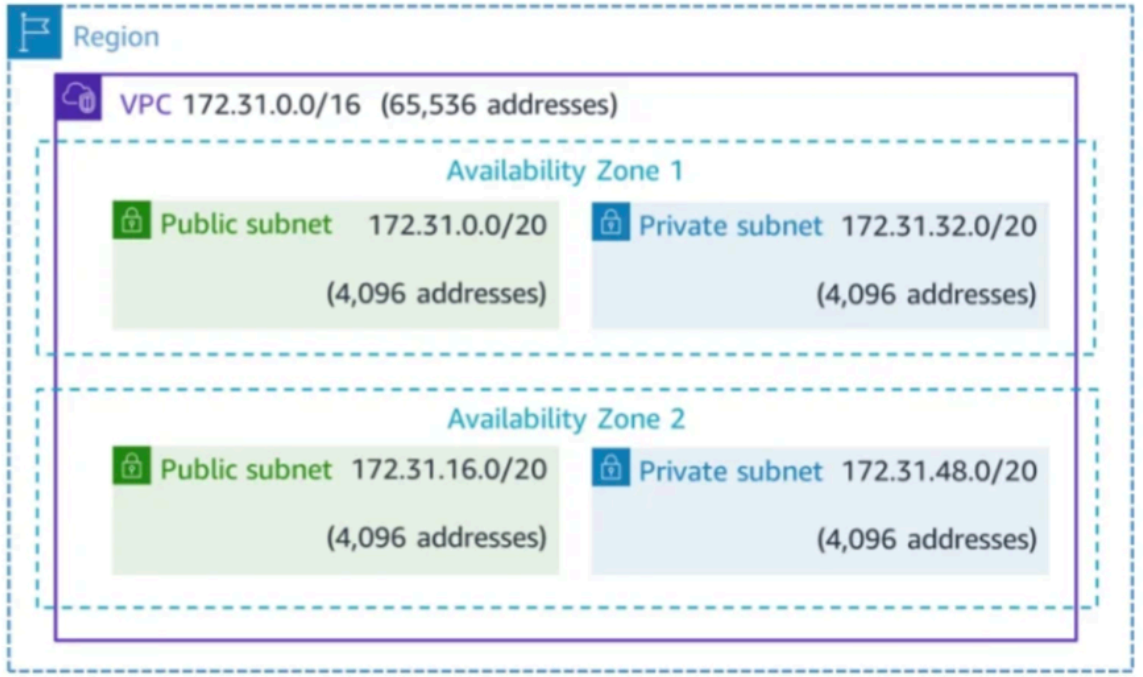
Amazon VPC

- Provides logical isolation for workloads.
- Permits custom access control and security settings for resources.
- Stays within a single AWS Region.
- Each account has preconfigured default VPC which spans all Availability Zones within the Region.



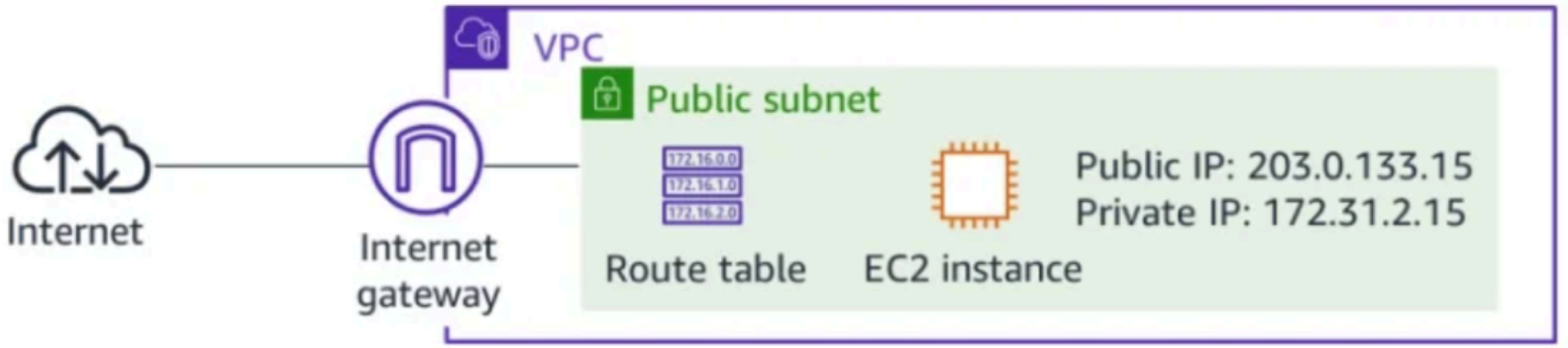
Subnet

- Subnet is a subset of the CIDR block.
- Subnet CIDR blocks cannot overlap.
- A subnet stays in one Availability Zone.
- An Availability Zone can contain multiple subnets.



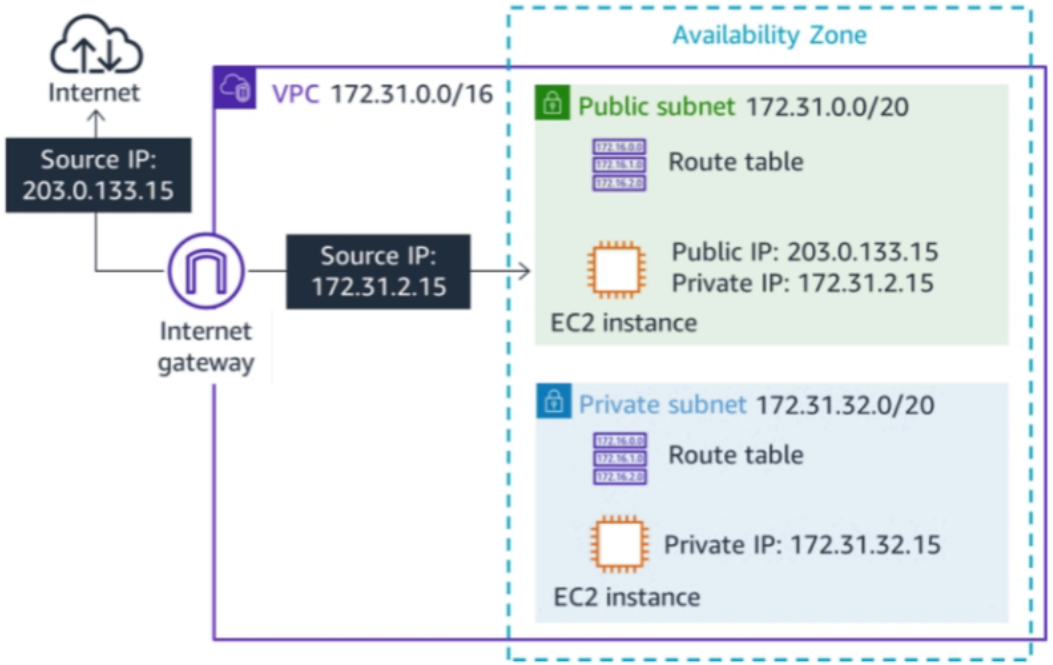
Public Subnet

- It consists of resources that work with inbound and outbound internet traffic.
- Route Table: A set of rules that the VPC uses to route network traffic.
- Internet Gateway: Allows communication between resources in VPC and the internet.
- Public IP Address: IP addresses that can be reached from the internet.



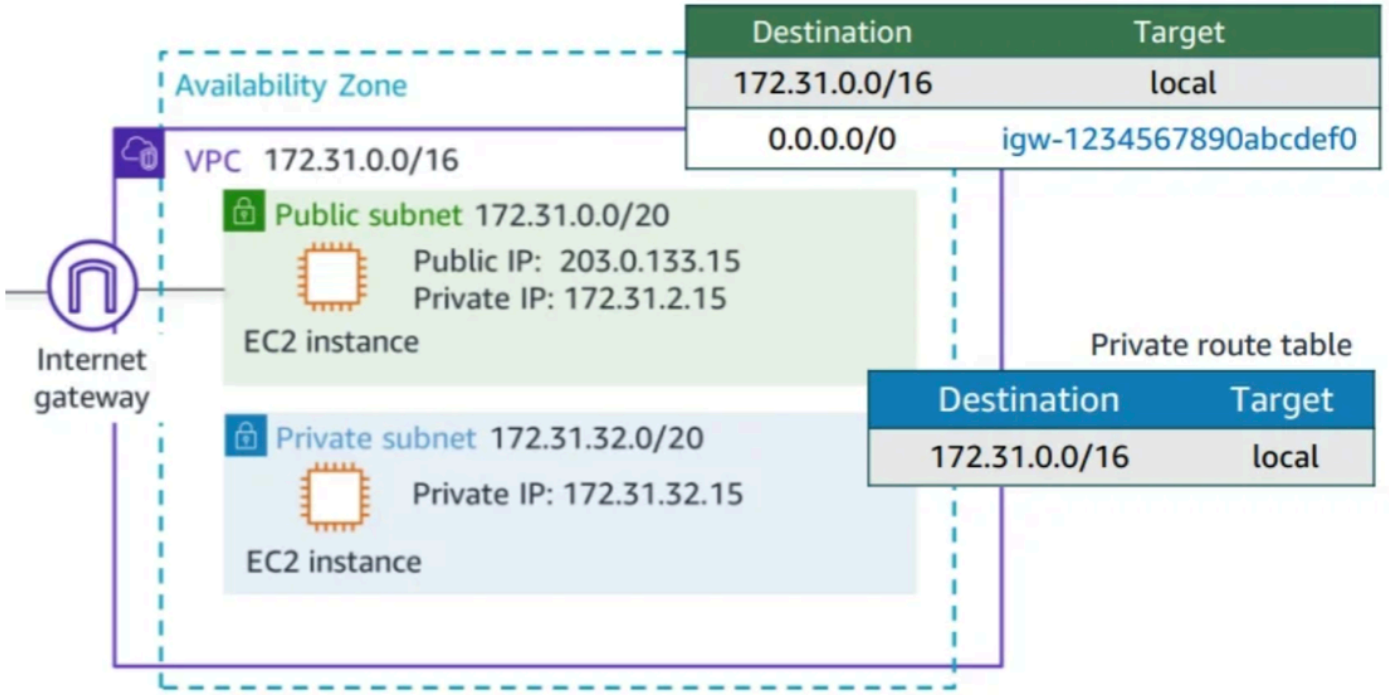
Internet Gateway

- It permits communication between instances in VPC and the internet.
- It is a target in subnet route tables for internet traffic.
- It protects IP address by performing Network Address Translation.



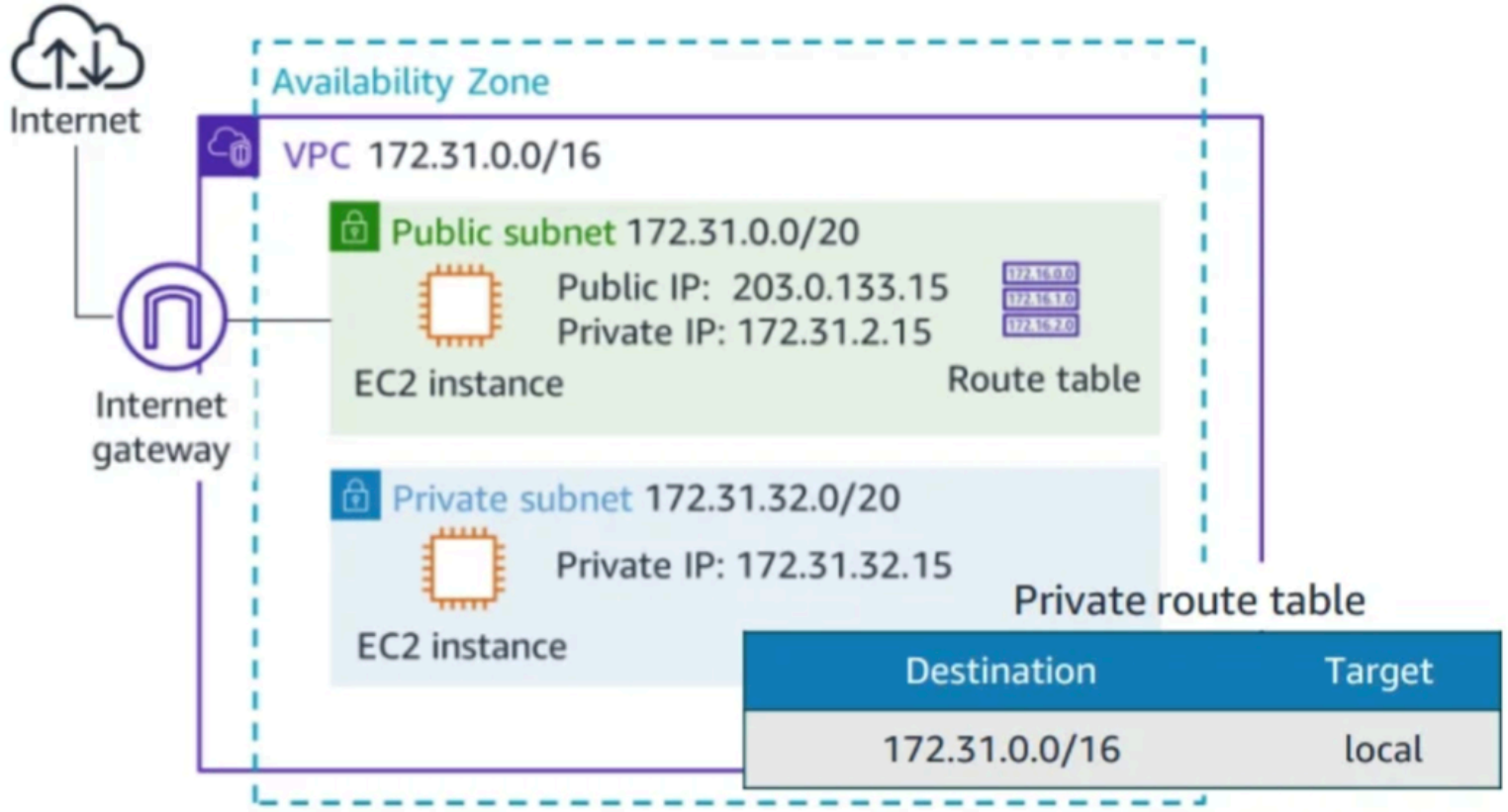
Route Table

- Each VPC has an implicit route table.
- It is used to control where internet traffic is directed.



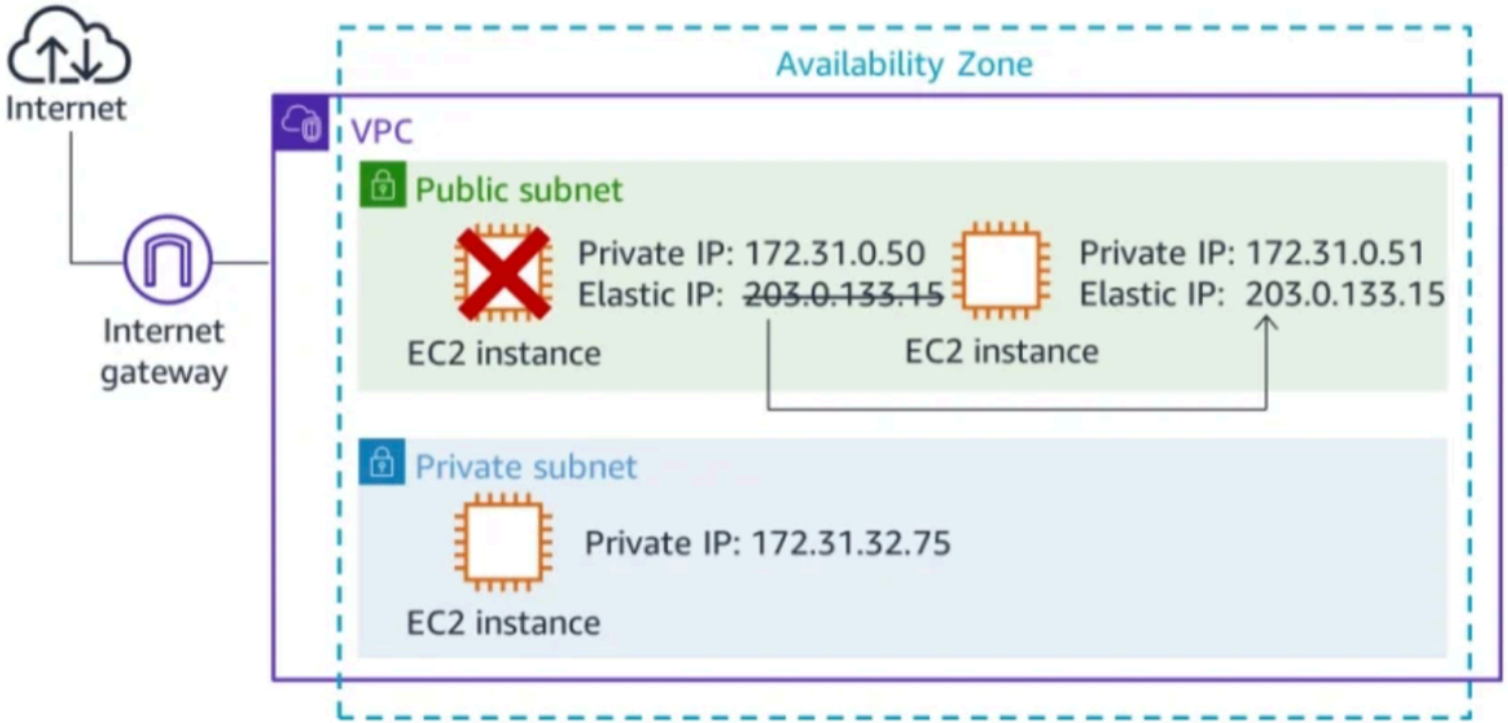
Private Subnet

- It allows indirect access to the internet and it never changes.



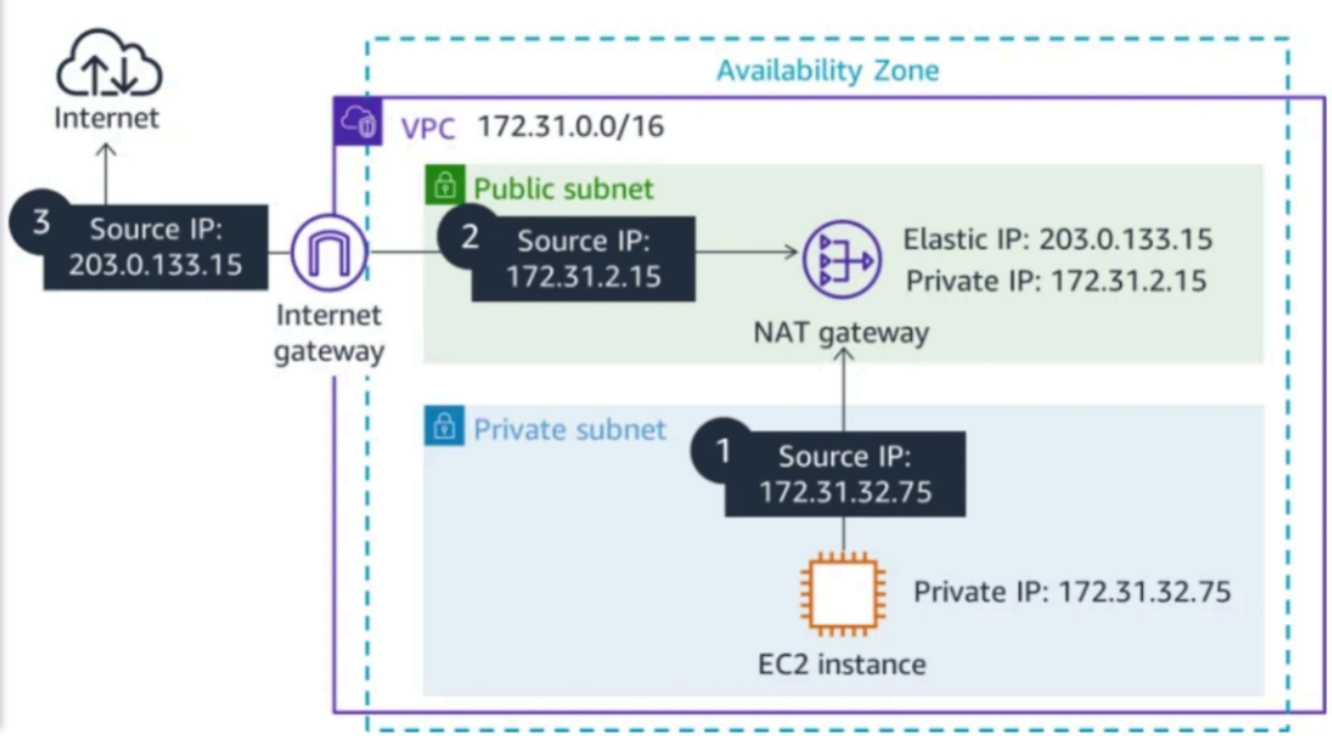
Elastic IP Address

- It permits association with an instance.
- It can be re-associated and can direct new traffic immediately.



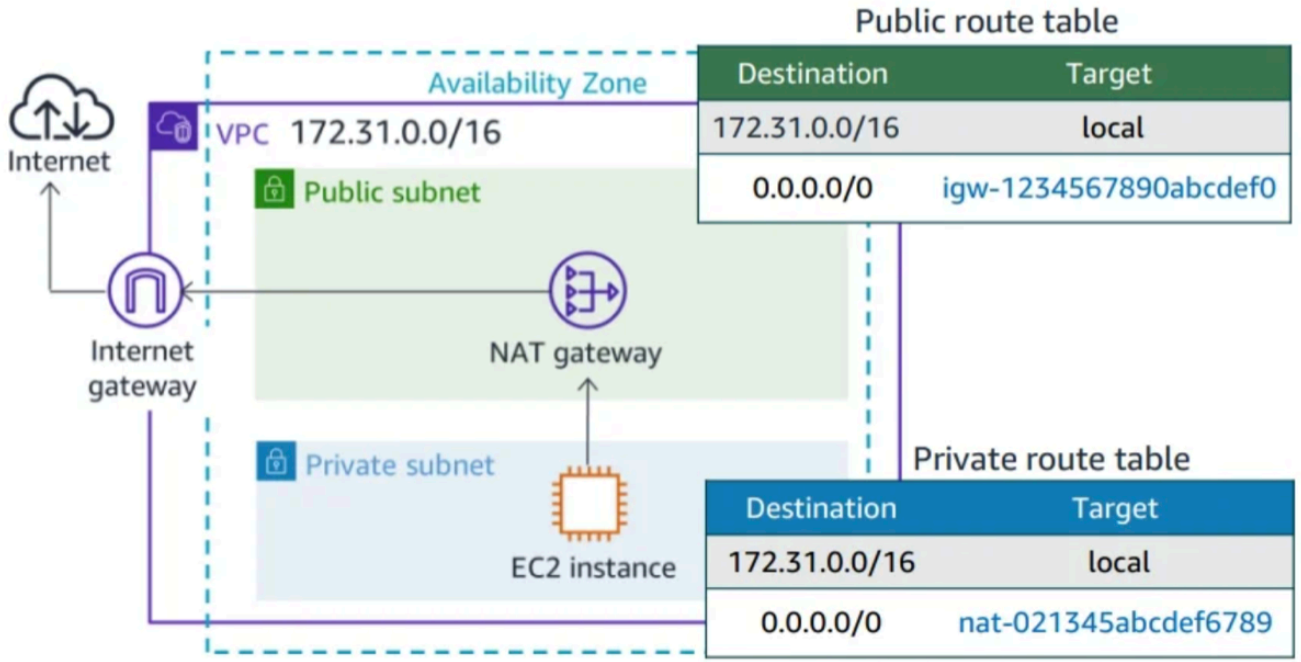
NAT Gateway

- It is used to protect private IP address.
- It uses an Elastic IP address as the source IP address for traffic from the private subnet.



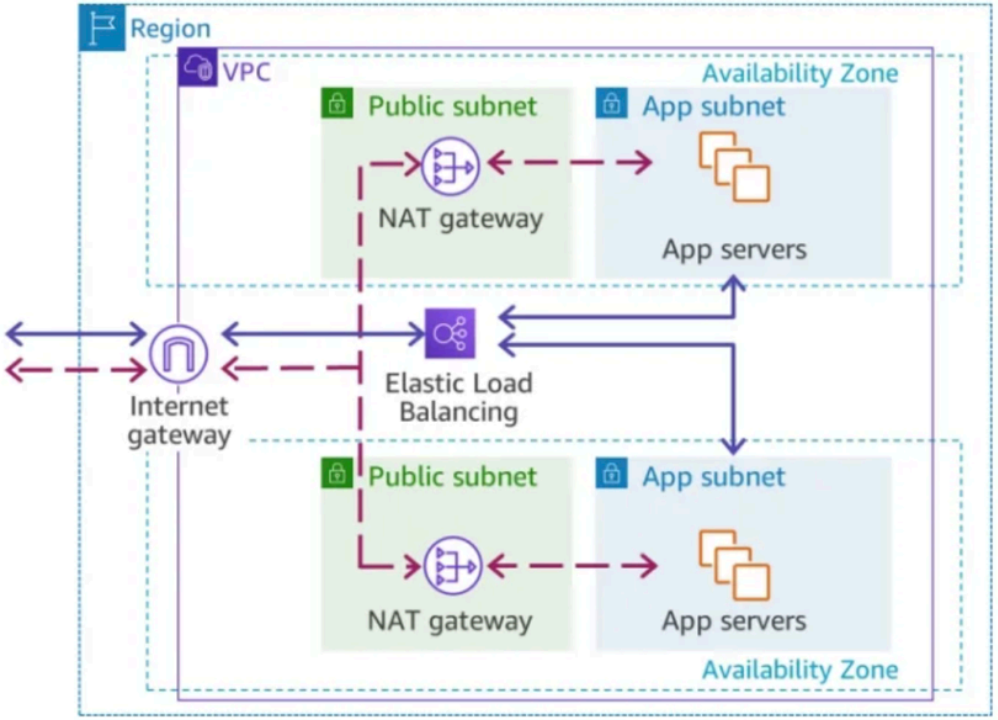
From Private Subnet to the Internet

- First, the route table of the private subnet directs the internet traffic to the NAT gateway.
- Then, the route table of the public subnet directs the internet traffic to the internet gateway.



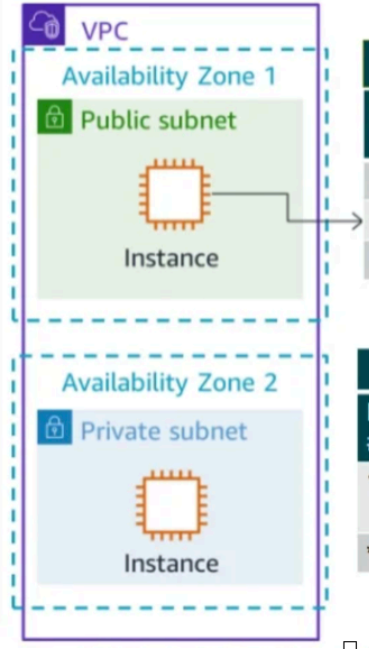
Architecting Tip

- Deploy VPC across multiple AZs. (High Availability)
- Create subnet in each AZ. (Public and Private)
- Deploy resources in subnets.
- Distribute the between the AZs using Load Balancers.



Network Access Control List

- It acts as a firewall at the subnet level.
- It allows all inbound and outbound traffic by default.
- It is stateless and requires explicit rules for all traffic.
- It evaluates rules, starting with the lowest numbered rule.



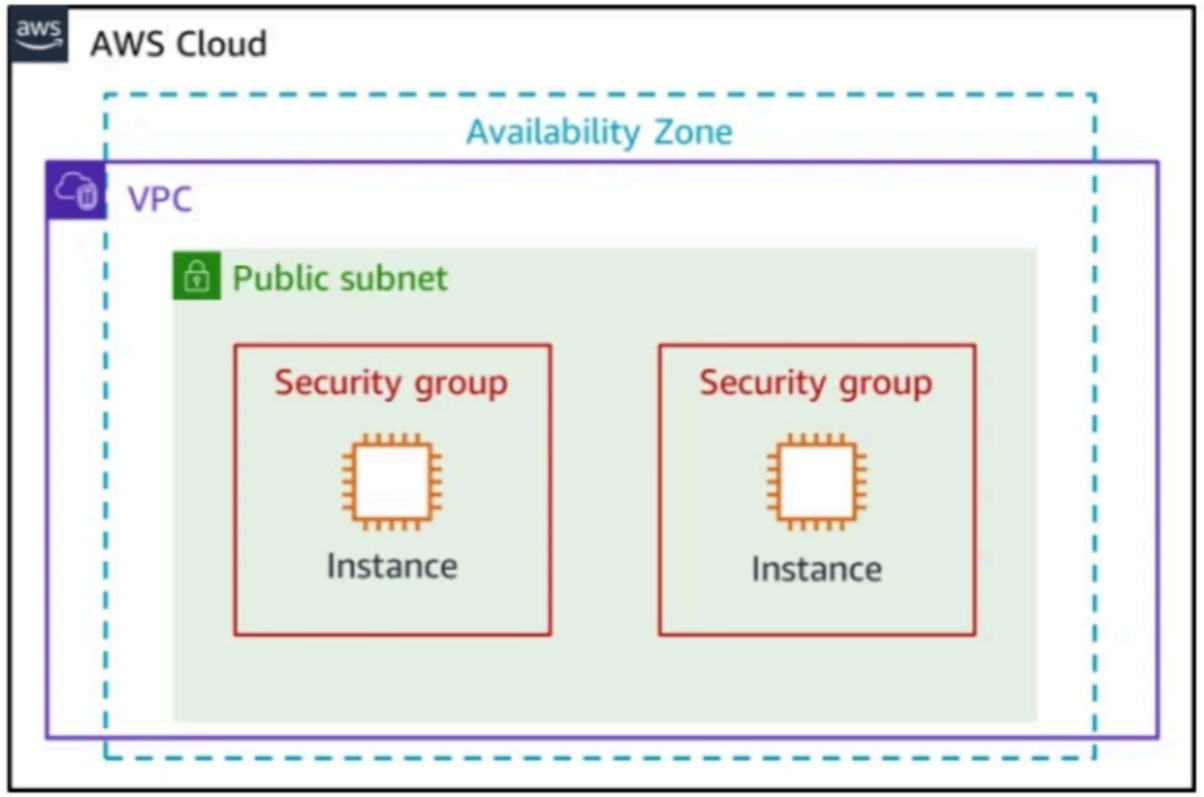
nacl-MyNACL1

Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow or Deny
100	HTTP	TCP	80	0.0.0.0/0	*Allow*
101	HTTPS	TCP	443	0.0.0.0/0	*Allow*
*	ALL Traffic	ALL	ALL	0.0.0.0/0	Deny

Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow or Deny
100	Custom TCP Rule	TCP	1024-65535	0.0.0.0/0	*Allow*
*	ALL Traffic	ALL	ALL	0.0.0.0/0	Deny

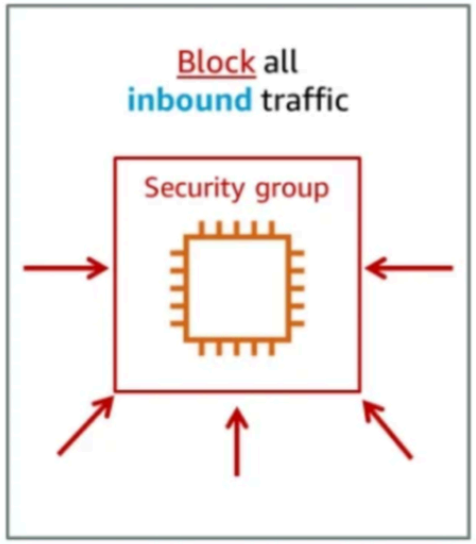
Security Groups

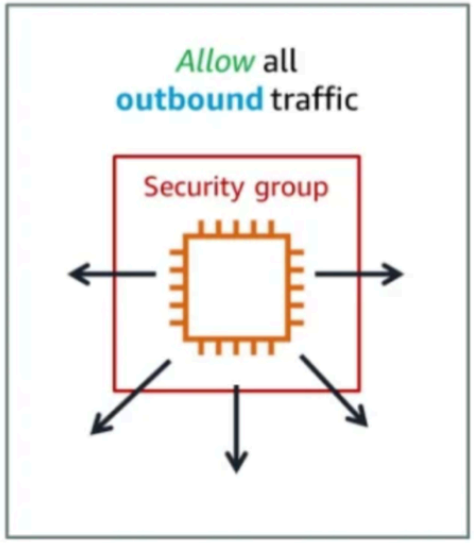
- It is virtual firewall that controls inbound and outbound traffic into AWS resources based on IP, protocol, port or IP address.



Security Groups

- Security Groups in default VPCs allow all outbound traffic.
- Custom security groups have no inbound rules.





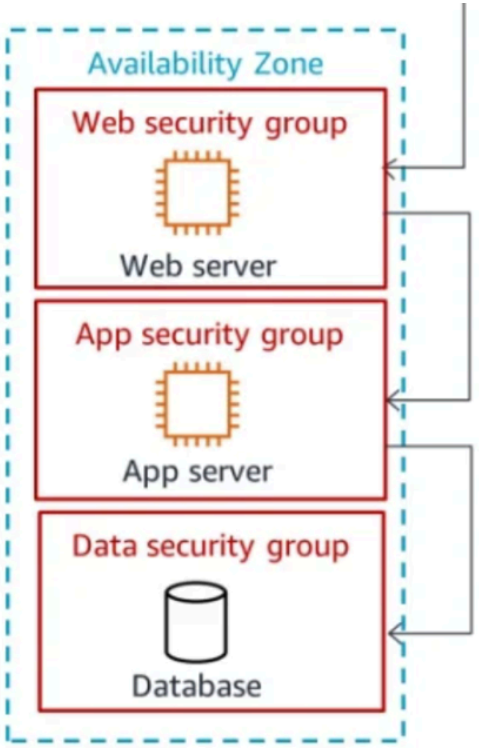
Inbound

Source	Protocol	Port	Comments
0.0.0.0/0	TCP	80	Allows inbound HTTP access from all IPv4 addresses
0.0.0.0/0	TCP	443	Allows inbound HTTPS traffic from anywhere

Outbound

Destination	Protocol	Port	Comments
SG ID of DB servers	TCP	1433	Allows outbound Microsoft SQL Server access to instances in the specified security group
SG ID of MySQL servers	TCP	3306	Allows outbound MySQL access to instances in the specified security group

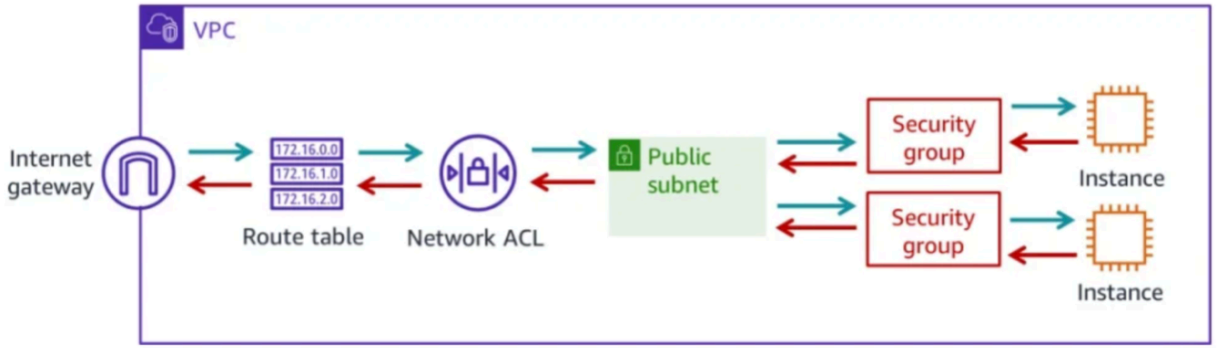
Architecting Tip



Inbound rule
Allow HTTPS port 443
Source: 0.0.0.0/0 (any)

Inbound rule
Allow HTTP port 80
Source: Web security group

Inbound rule
Allow TCP port 3306
Source: App security group



Security Groups and Network ACLs

Security Group	Network ACL
Associated to an elastic network interface and implemented in the hypervisor	Associated to a subnet and implemented in the network
Supports Allow rules only	Supports Allow rules and Deny rules
A stateful firewall	A stateless firewall
All rules evaluated before deciding whether to allow traffic	All rules processed in order when deciding whether to allow traffic
Applies to an instance only if it is associated with the instance	Applies to all instances deployed in the associated subnet

HEPAPI
DIGITAL TRANSITION PARTNER

THANKS FOR LISTENING