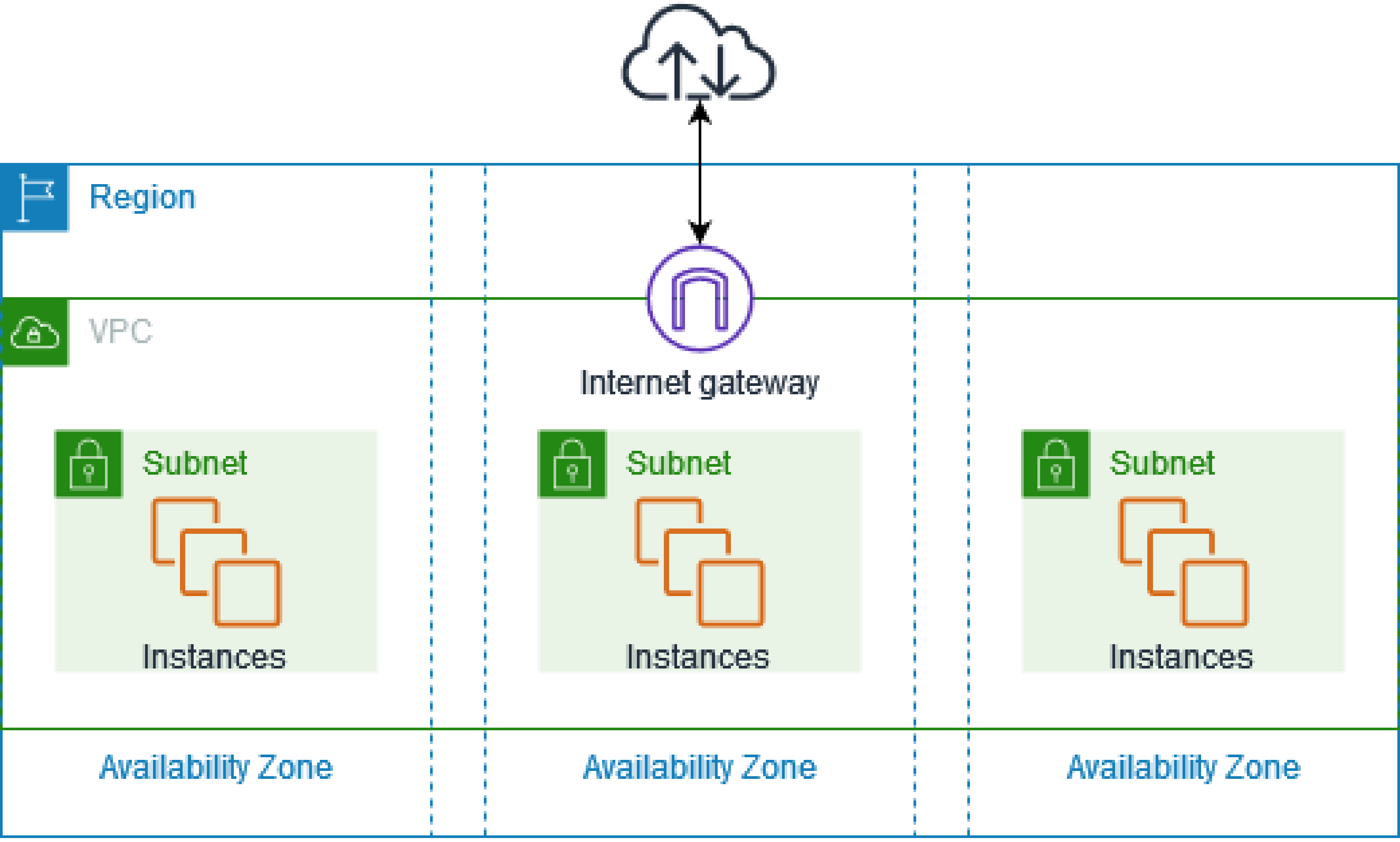
Region
VPC
Internet gateway
Subnet
Instances
Subnet
Instances
Subnet
Instances
Availability Zone
Availability Zone
Availability Zone

VPC (Virtual Private Cloud)

- A VPC is a virtual network or data center within AWS created for a specific client.
- It's isolated logically from other virtual networks in the AWS Cloud.
- Each AWS account can create a maximum of 5 VPCs.
- Within each VPC, you can establish up to 200 subnets.
- Allocation of up to 5 Elastic IP addresses is possible.
- Upon VPC creation, DHCP, NACL, and security groups are generated automatically.
- A VPC is specific to an AWS region and cannot extend across regions.
- The CIDR block range of a created VPC remains fixed and cannot be changed.
- To use a different CIDR size, you'll need to create a new VPC.
- Subnets within a VPC must not have overlapping CIDR ranges.
- You can expand a VPC's CIDR by adding new IP address ranges, except in GovCloud and AWS China regions.
-

Components of VPC:

- CIDR & IP address Subnets
- Implied Router & Routing Table
- Internet Gateway
- Security Groups
- Network ACL
- Virtual Private Gateway
- Peering Connections
- Elastic IP

VPC Types:

Default VPC:

- Created in each AWS region upon account creation.
- It has default CIDR, security group, NACL, and route table settings.
- Default VPCs include an Internet Gateway by default.

Custom VPC:

- Created by AWS account owners.
- AWS users creating custom VPCs can define the CIDR.
- Custom VPCs come with their own default security group, NACL, and route tables.
- Unlike default VPCs, custom VPCs don't have an Internet Gateway by default; one needs to be created if needed.

Steps to Create a VPC:

1. **Create a VPC:**
    - Specify an IPv4 CIDR Block for the VPC.
    - The allowed block size is between /16 to /28 netmask.
    - The first four and last IP addresses of the subnet cannot be assigned.
    - Example: 10.0.0.0/16
    - Reserved addresses:
        - 10.0.0.1: Reserved by AWS for the VPC router.
        - 10.0.0.2: Reserved by AWS for DNS server.
        - 10.0.0.3: Reserved for future use.

  - 10.0.0.255: Broadcast address (reserved, AWS does not support broadcast).
- Note: AWS doesn't support broadcast, but reserves the broadcast address.
- /16 = 65536 IPs - 255.255.0.0
- /24 = 256 IPs - 255.255.255.0

2. **Create Subnet:**
   - Public Subnet: Routed to an Internet Gateway.
      - Instances in this subnet can communicate with the internet over IPv4 if they have a public IPv4 address or Elastic IP.
   - Private Subnet: No route to the internet gateway.
      - Instances in this subnet can't directly communicate with the internet.

3. **Create an Internet Gateway:**
   - An Internet Gateway connects a VPC to the internet.
   - By default, the default VPC includes an Internet Gateway.

4. **Create a Route Table:**
   - Implied Router & Central Routing Function.
   - Connects different Availability Zones (AZs) and VPC to the Internet Gateway.
   - Up to 200 route tables can be associated with a VPC.
   - Up to 50 route entries per route table.
   - Each subnet must be associated with only one route table.
   - If you don't specify a subnet-to-route table association, the subnet will use the default VPC route table.
   - Main route table can't be deleted but can be manually changed to a custom route table as the main one.

- You can associate multiple subnets with the same route table.

Internet Gateway:

- An Internet Gateway is a virtual router connecting a VPC to the internet.
- The default VPC comes with an Internet Gateway attached.
- Creating a new VPC requires attaching an Internet Gateway to access the internet.
- Subnet's route table should point to the Internet Gateway for internet access.
- It performs Network Address Translation (NAT) between private and public IPv4 addresses.
- Supports both IPv4 and IPv6.

NAT Gateways:

- NAT Gateway enables instances in a private subnet to access the internet or AWS services while preventing incoming connections.
- You're charged for creating and using a NAT Gateway, including hourly usage and data processing rates, along with EC2 charges for data transfer.
- To create a NAT Gateway, specify the public subnet in which it should reside.
- Also, associate an Elastic IP address when creating a NAT Gateway.
- No need to assign a public IP address to private instances.
- After creating a NAT Gateway, update route tables of private subnets to direct internet-bound traffic to the NAT Gateway for communication.
- Deleting a NAT Gateway disassociates its Elastic IP but doesn't release it from your account.

Security Groups:

- Operates at the Elastic Network Interface (ENI) level.
- Up to 5 security groups can be applied per EC2 instance interface.

- Supports only permit rules; deny rules are not allowed.
- It's stateful, allowing return traffic of allowed inbound traffic even without explicit rules.

Network ACL:

- A function performed on the implied router.
- Network ACL (NACL) is used to control traffic in and out of one or more subnets as a firewall.
- Default VPC comes with a modifiable default Network ACL that permits all inbound and outbound IPv4 (and IPv6) traffic.
- A custom Network ACL denies all inbound and outbound traffic until rules are added.
- Every subnet in a VPC must be associated with a Network ACL.
- Subnets not explicitly associated with a Network ACL are automatically associated with the default Network ACL.
- You can associate a Network ACL with multiple subnets, but each subnet can be associated with only one Network ACL.
- Network ACLs function at the subnet level and are stateless. Outbound traffic corresponding to allowed inbound traffic must be explicitly allowed.
- Network ACLs support both permit and deny rules.

Security Group:

- Operates at the instance level.
- Supports allow rules only; deny rules are not allowed.
- Stateful: Return traffic is automatically allowed.
- Applies to an instance only.

Network ACL (NACL):

- Operates at the subnet level.
- Permits both allow and deny rules.
- Stateless: Return traffic must be explicitly allowed by rules.
- Applies to all instances in the subnet.

VPC Peering:

- A VPC Peering Connection is a networking link between two VPCs, enabling traffic routing using private IPv4 or IPv6 addresses.
- Instances in either VPC can communicate as if they're within the same network.
- You can create VPC Peering Connections between your own VPCs or with VPCs in different AWS accounts, across regions.
- Example:
    - VPC-A and VPC-B are separate VPCs in AWS.
    - The address range 172.3.0.8/24 is associated with a London location.
    - These VPCs are connected via VPC peering, facilitating communication.
- Transitive peering:
    - If VPC-A is peered with VPC-B and VPC-B is peered with VPC-C, VPC-A can indirectly communicate with VPC-C.
    - This is not possible in the concept of VPC peering.