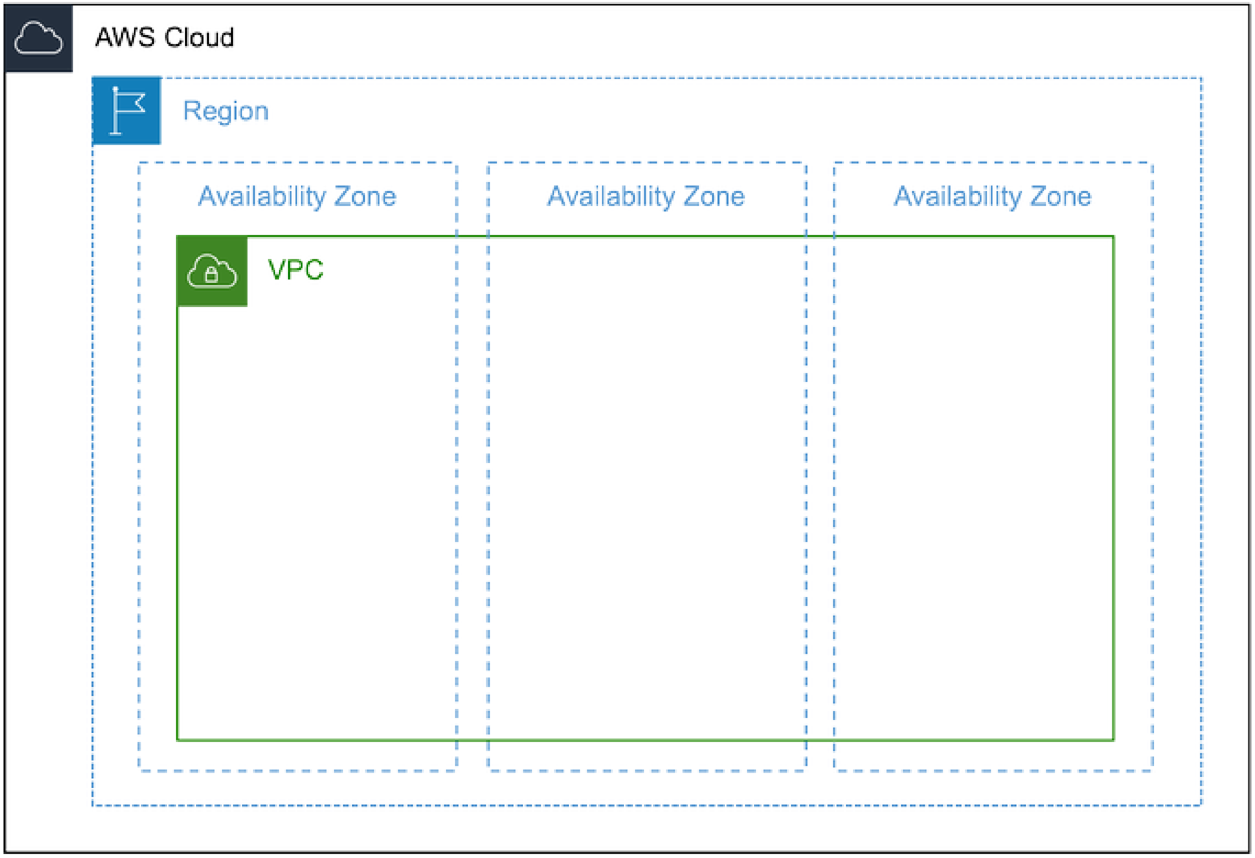
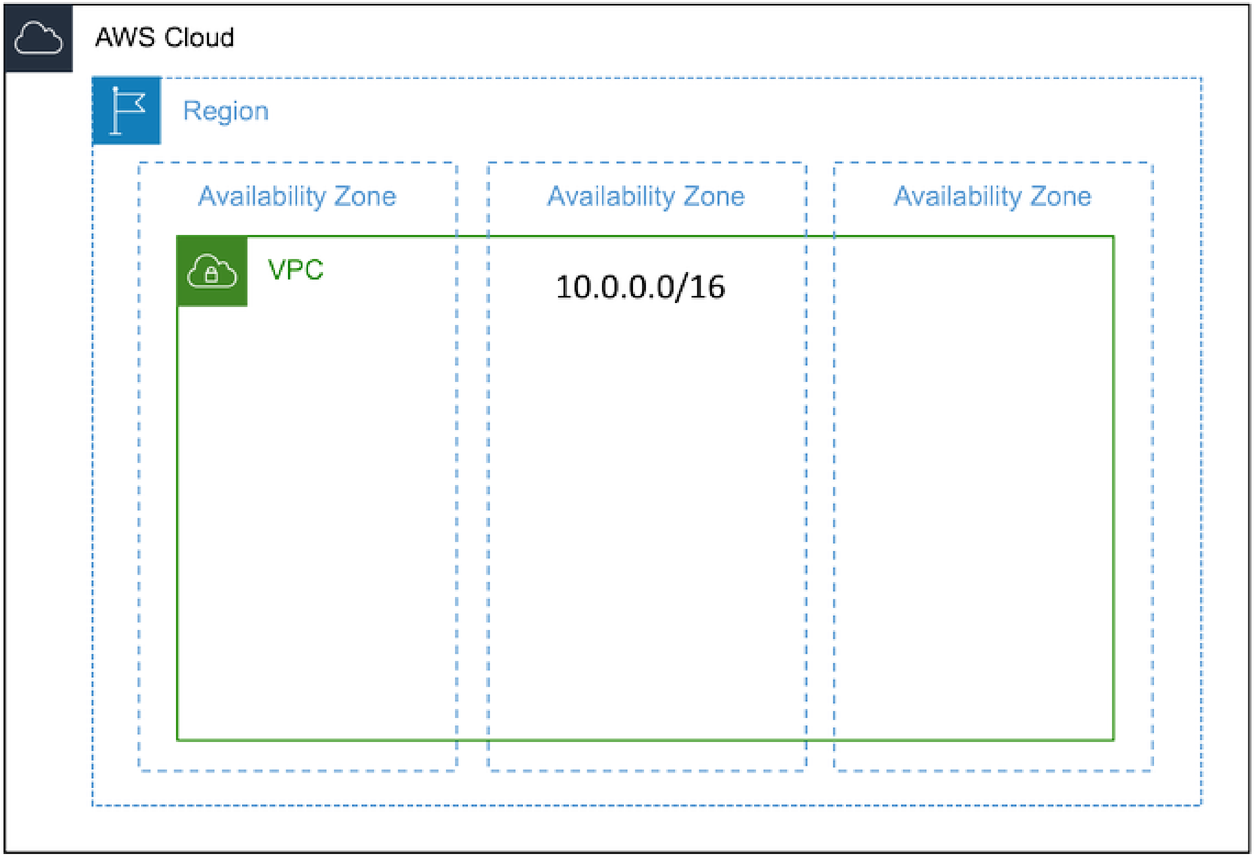
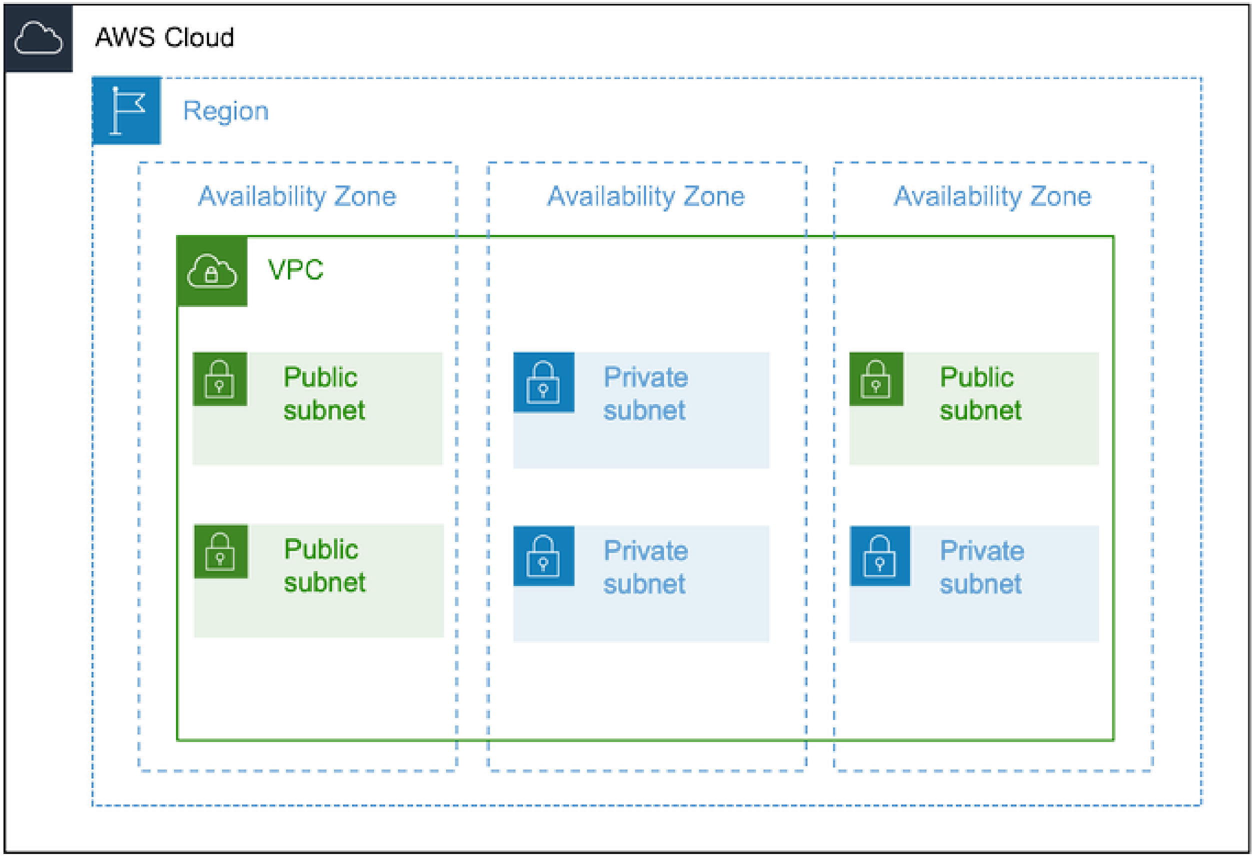
A VPC is basically a virtual representation of a physical network in the cloud. It's logically isolated and you need one to launch resources on AWS like EC2 instances. A VPC is created on a per-region basis and spans across all Availability Zones in that region.



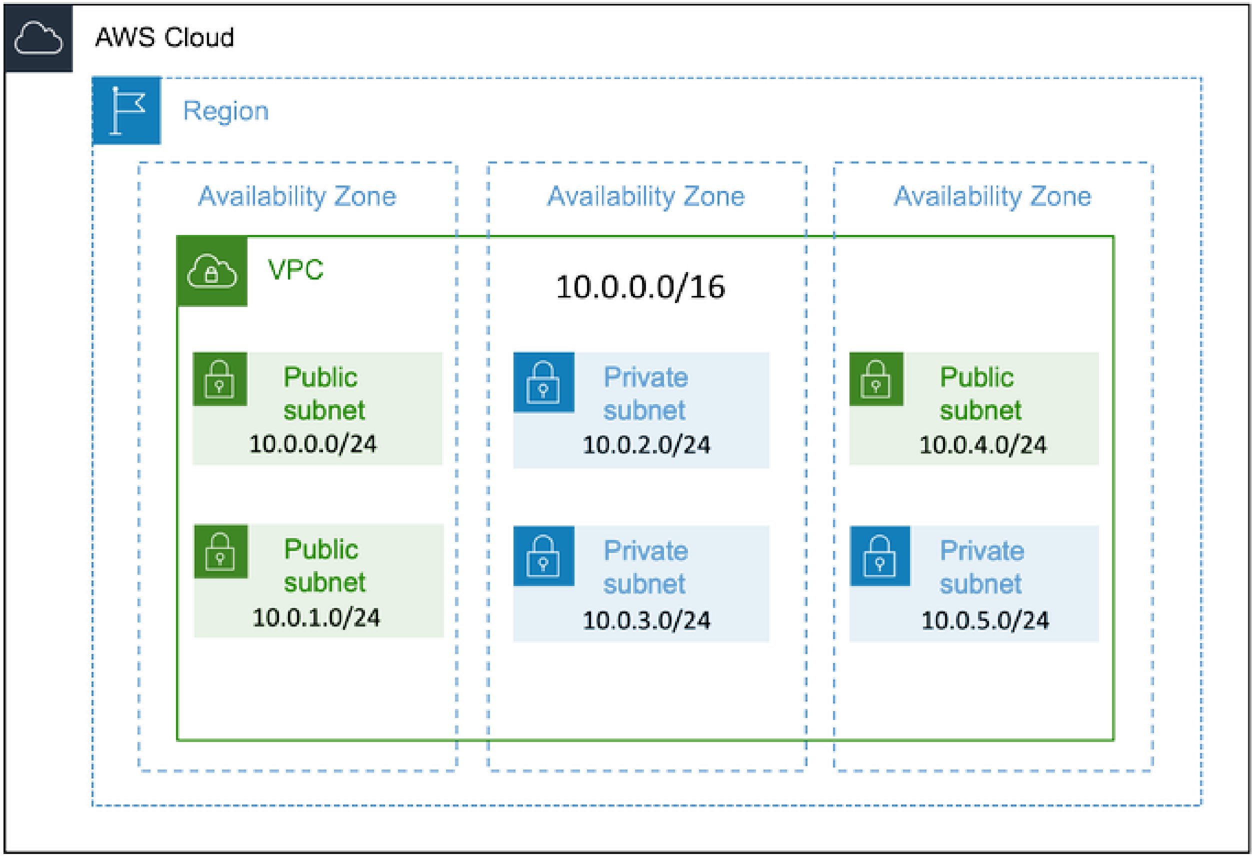
For creating a VPC, we have to assign a range of IPv4 addresses as CIDR (Classless Inter-Domain Routing) blocks. The allowed block size is between /16 & /28 netmask (65,536 - 16 IP addresses).



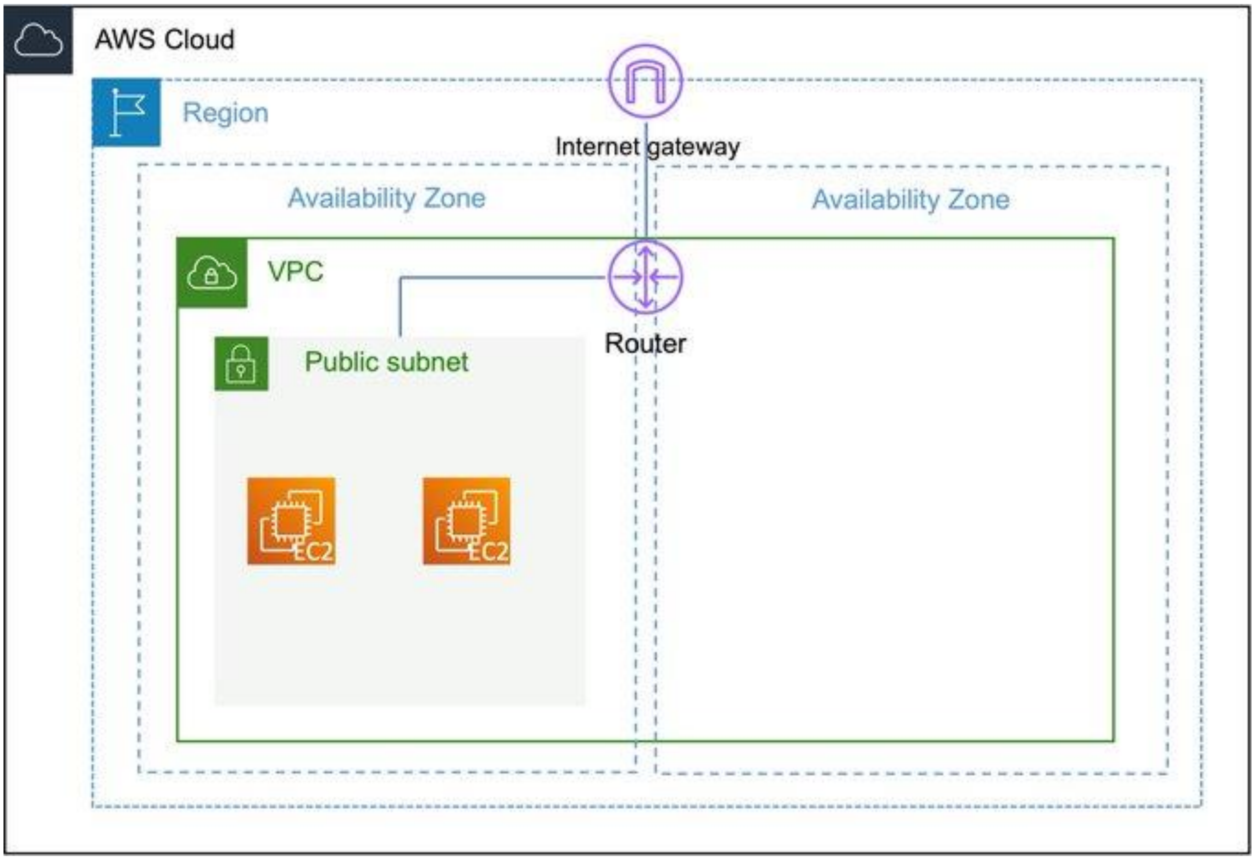
After creating a VPC, we can further break it into so-called subnets. Subnets are ranges of IP addresses from the VPC CIDR block that contain your resources in one Availability Zone. Your subnets can either be public (internet-facing) or private.



n this example, we have created 6 subnets in our VPC (10.0.0.0/16). Each one receives 256 IPv4 addresses: Subnet-1: 10.0.0.0/24 Subnet-2: 10.0.1.0/24 Subnet-3: 10.0.2.0/24

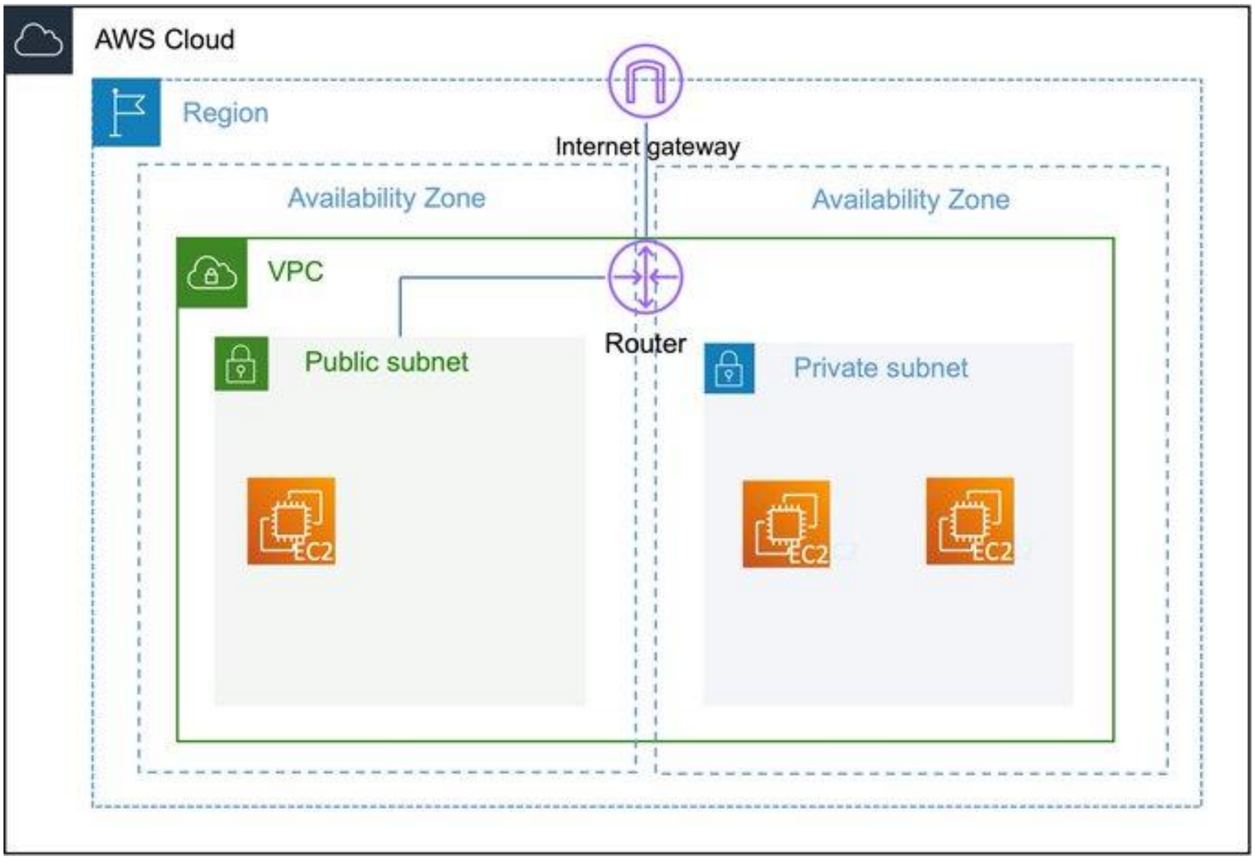


Let's take a closer look at the subnets. In a subnet, you can host your resources. A subnet is public when its traffic is routed through an Internet Gateway. The IGW is basically the door between your VPC and the World Wide Web.

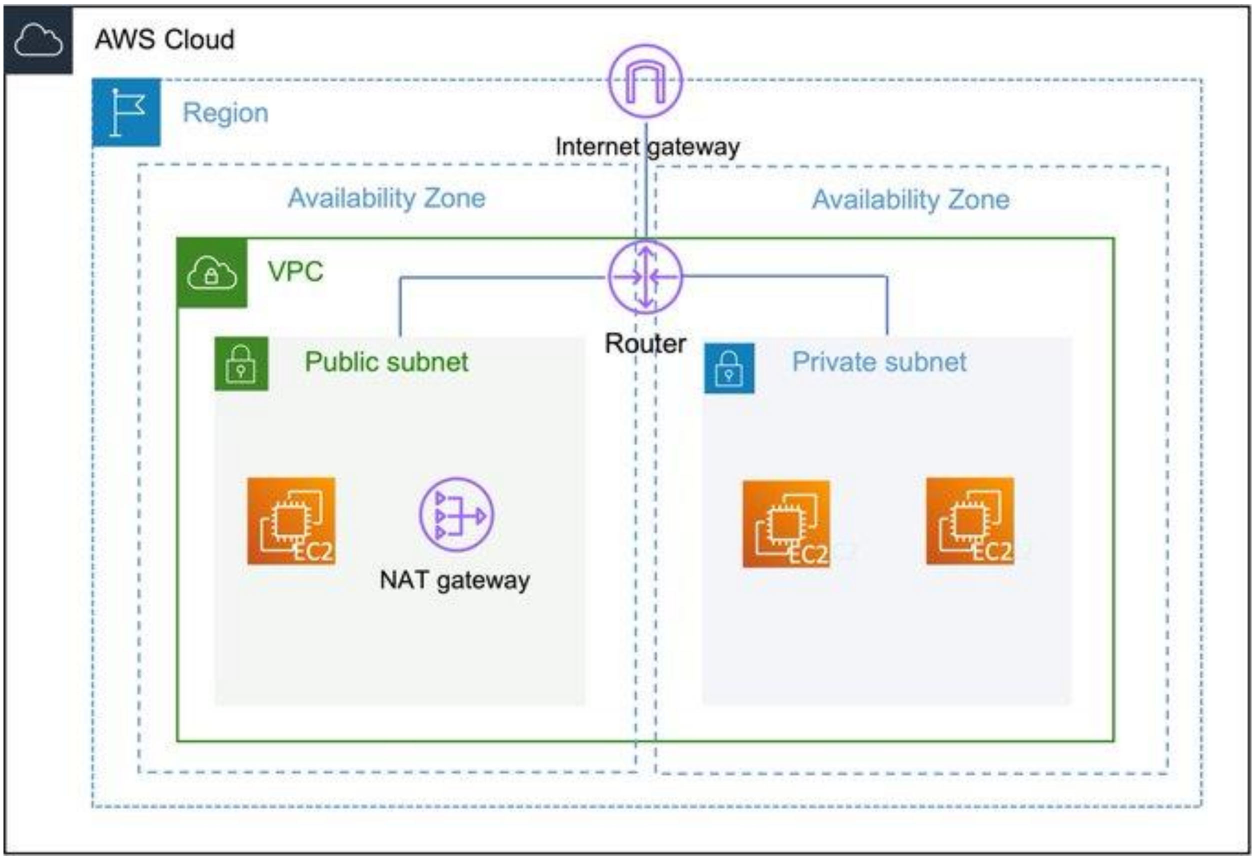


To allow instances in public subnets access to the public internet, they also need a public IPv4 address or an Elastic IP address (EIP). They still have a private IP address as well! You can access these instances via their public IP addresses.

Besides being public, subnets can also be private. That means that resources in that subnet cannot access the public internet by default because there is no routing connection to the IGW. The instances in this private subnet have only private IP addresses assigned to them.

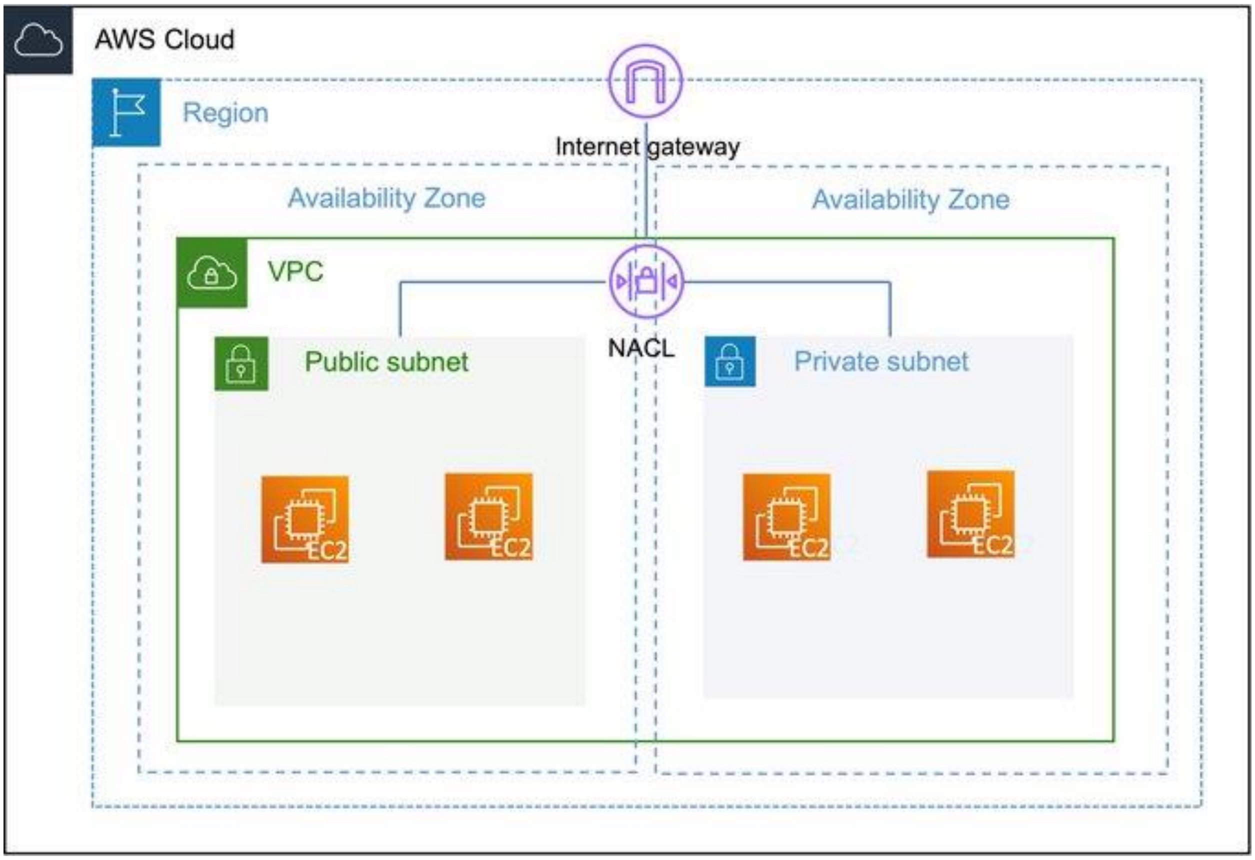


If you still want your instances in a private subnet to access the internet, you need to deploy something called a NAT Gateway in one of your public subnets and adjust the route table. The NAT-GW has an EIP and routes traffic to the Internet Gateway.



A route table basically contains rules (called routes) for how the traffic follows in your VPCs. It helps the instances in your subnets to reach a NAT Gateway or Internet Gateway and to communicate with each other.

Another important aspect of a VPC is a Network Access Control List (NACL). It's basically a firewall that controls traffic in and out of your subnets. This adds an additional layer of security to your VPC. Each subnet must be assigned to a NACL.



Although NACLs and SGs are quite similar, there are some important differences. SGs are stateful which means that if incoming traffic is allowed, returning traffic is allowed as well. NACLs are stateless so return traffic has to be explicitly allowed!