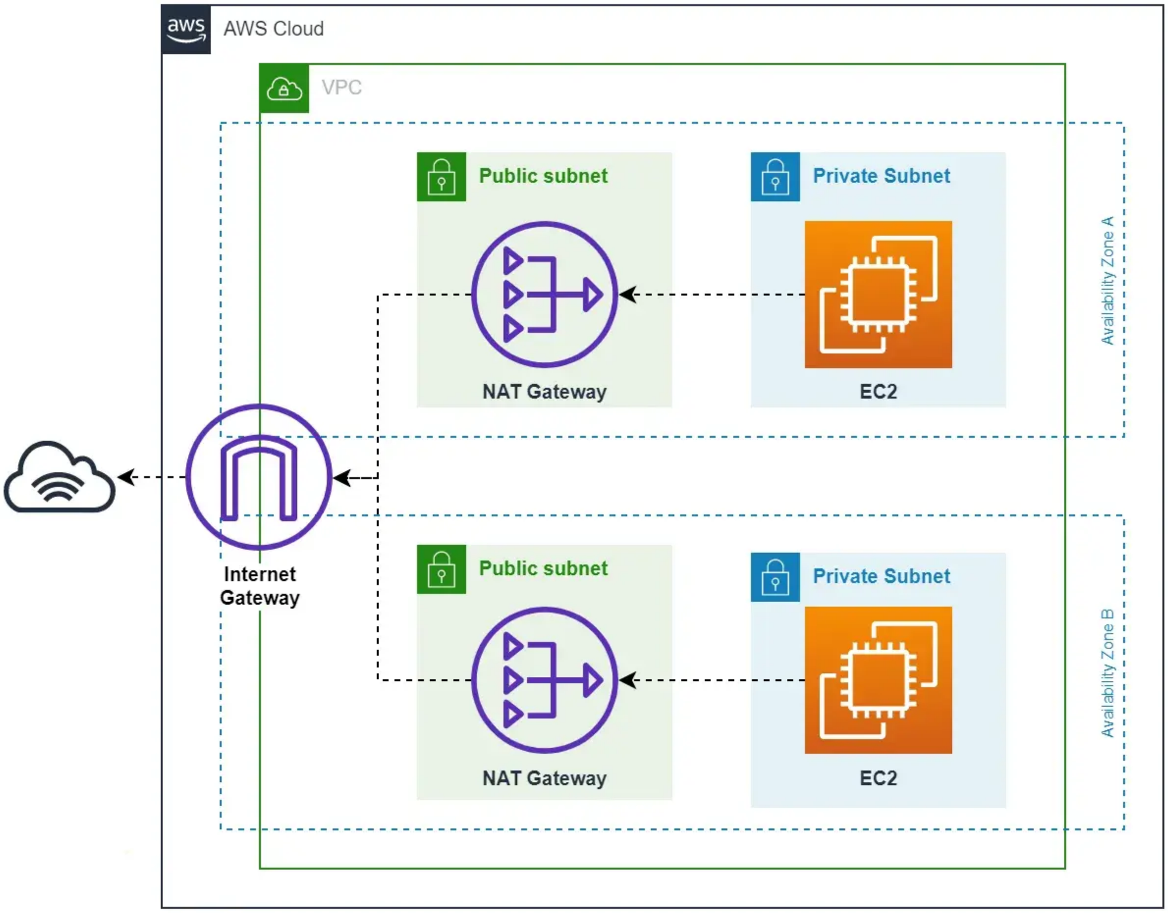
NAT and Internet Gateways

Network Address Translation or NAT for short, allows instances in a private subnet to access the internet while preventing the internet from initiating connections to those instances. This is crucial for maintaining security, as it helps shield private resources from external threats. In modern AWS environments Network Address Translation (NAT) services are provided by something called NAT Gateways. NAT gateways are used so that our AWS resources such as EC2 or RDS instances that are occupying a private subnet can connect to external services i.e. services outside the VPC, but said external services cannot initiate a connection with the instances inside the private subnet, allowing our web servers and databases to scour the internet or fetch software updates for example, without the risk of malicious actors accessing them.

When we create a NAT gateway, we must specify one of the following connectivity types for it:

- **Public** – The default connectivity type, instances in private subnets can connect to the internet through a public NAT gateway, but cannot receive unsolicited inbound connections from the internet. You create a public NAT gateway in a public subnet and must associate an elastic IP address with the NAT gateway at creation. You route traffic from the NAT gateway to the internet gateway for the VPC. Alternatively, you can use a public NAT gateway to connect to other VPCs or your on-premises network. In this case, you route traffic from the NAT gateway through a transit gateway or a virtual private gateway.
- **Private** – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway. You can route traffic from the NAT gateway through a transit gateway or a virtual private gateway. You cannot associate an elastic IP address with a private NAT gateway.

Internet gateways on the other hand, are a more general purpose VPC component, allowing the resources within a VPC to have full access to the internet, and scour it in a manner which is more similar to how we browse it ourselves, allowing both inbound and outbound connections to be established. Internet Gateway therefore serves as both a bridge for outbound traffic from your VPC to the internet whilst providing a path for inbound traffic as well.



Architecture showing NAT Gateways connected to an Internet Gateway

Note in the above diagram how the NAT Gateways are visualized as an additional layer between the EC2 instances and Internet gateway, this is because the presence of an internet gateway is necessary for the functioning of a NAT Gateway though the opposite is never true.