AWS

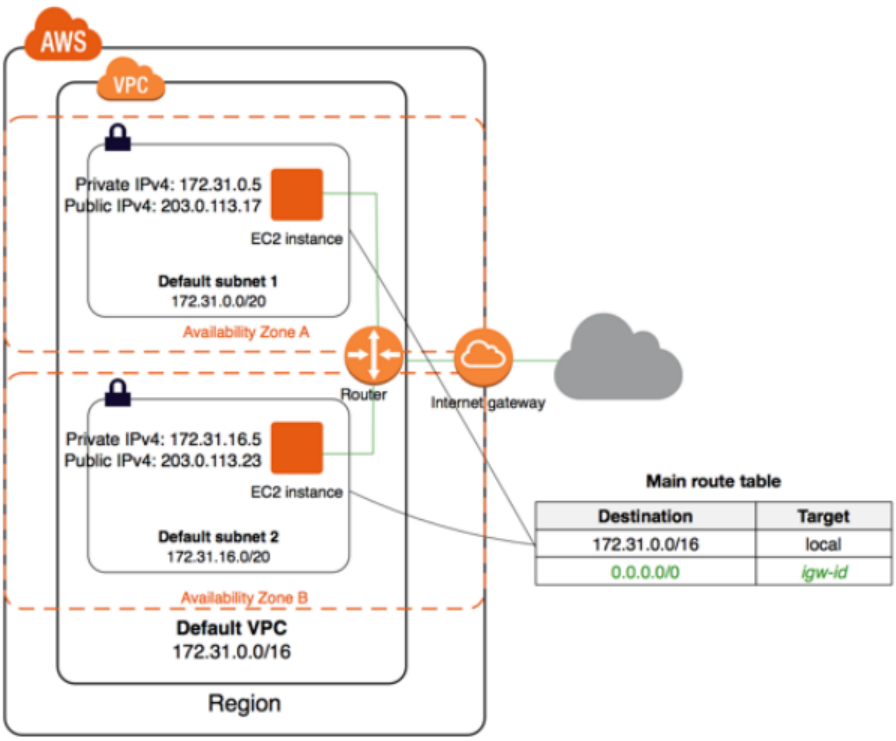
Virtual Private Cloud (VPC)

what is it?

A Virtual Private Cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud.

You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. Access is controlled using Route Tables, Internet Gateways, NAT Gateways, and Network Access Control Lists.

Diagram from AWS documentation



AWS

Virtual Private Cloud (VPC)

subnet

A subnet can be public or private. There can be up to 200 subnets per VPC. If you would like to increase this you will need to request this through AWS Support.

Key things to know

- You define which subnets you want to be exposed to the internet by attaching public IP addresses

route table

Each Subnet has a route table attached. This creates a set of rules to allow traffic to flow within a set of guidelines. This means that traffic stays inside the subnet until a route is created to allow it to travel to the next stop on the network.

Key things to know

- Route Tables create a set of rules to allow traffic to flow within a set of guidelines
- The Internet Gateway allows devices on a Public Subnet to connect to the internet
- In contrast, a Network Address Translation Gateway (NAT Gateway) facilitates the connection between Private Subnets and the internet

AWS

Virtual Private Cloud (VPC)

network access control lists (nacls)

Network Access Control Lists (NACL) allow us to limit traffic to safeguard against mistakes and accidents. Using NACLs lets us control traffic flow using a set of rules.

Key things to know:

- NACLs allow us to create a set of rules to allow and deny traffic to safeguard against mistakes and accidents
- The default NACL that comes with your VPC will allow all outbound and inbound traffic. When you create a NACL it will deny by default
- They are stateless which means the incoming rule will not be applied to the outgoing

web application firewall (waf)

WAFs protect web applications from attacks by filtering traffic based on rules. A WAF can be deployed on Amazon CloudFront, protecting resources and content at edge locations.

Use cases

- **Block IP addresses that exceed request limits** - this lets you control access to your content whether that's by IP address, country, blocking SQL injections, malicious scripts and the length of requests.
- **Block IP addresses that submit bad requests** - this lets you block IP addresses using Lambda, CloudWatch and AWS WAF to block requests after a threshold has been reached.