1 Region có 2 AZ trở lên

AZ là các data center

IAM:

- USER

- Group

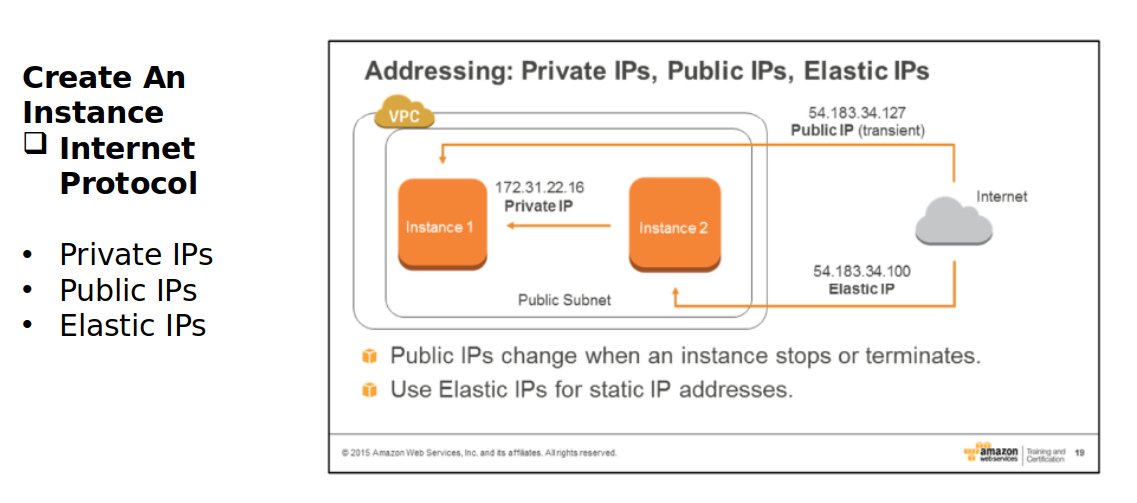
- Policy: định nghĩa quyền

- Roles: tập hợp 1 hoặc nhiều permission → service truy cập vào serviceservice

EC2 intance / Lambda / cloudfront,...

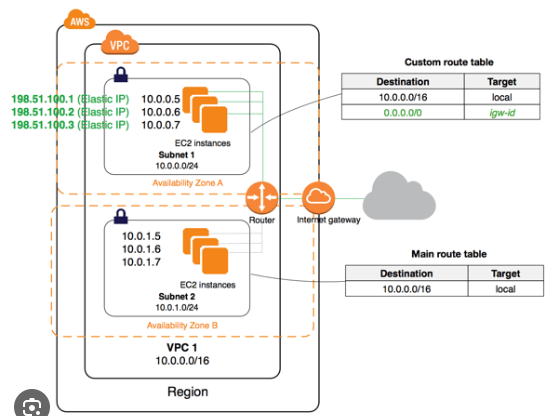
Resource AWS (Services: EC2, S3, StorageStorage)

network intance

Từ internet mà muốn vào được con 1 thì dùng public IP

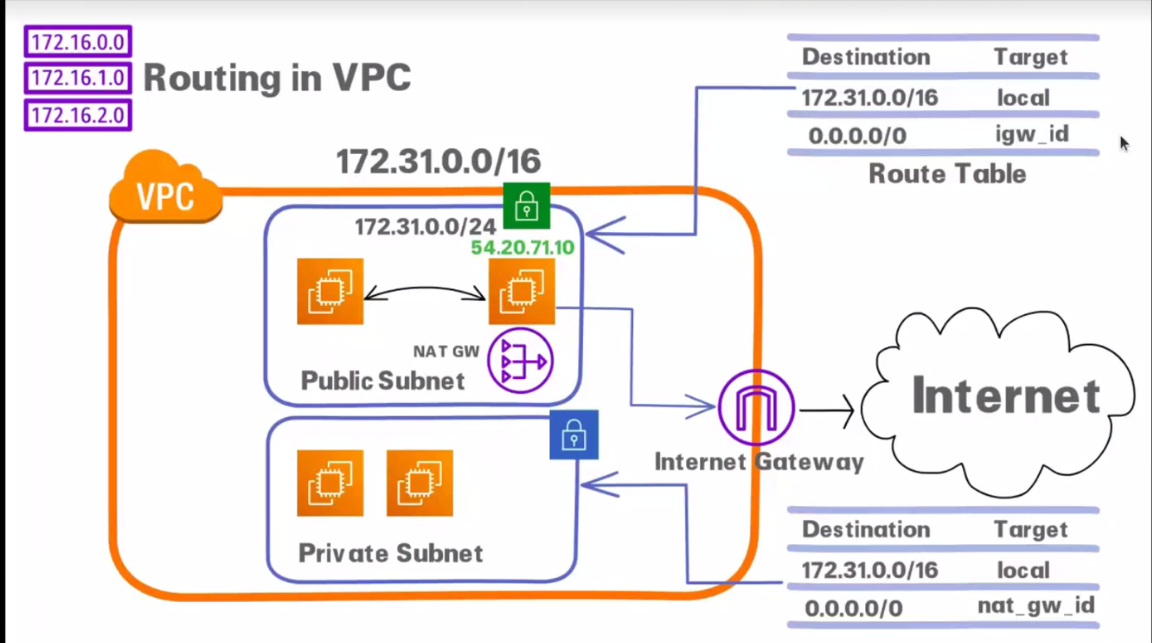
còn muốn ra internet thì phải qua internet gateway

- EBS: ổ cứng gắn qua internet, giống kiểu NFS



1 VPC có 1 internet GW, vào nó cho phép resource trong VPC ra được internet nhờ internet GW

phân biệt public subnet và private subnet

Route Target là local : tức là để các intance trong subnet đấy nói chuyện với nhau

tức là để đi đến Destination: 172.31.0.0/16 thì nó sẽ sử dụng là mạng local (tức là nội bộ)

còn muốn ra internet (destination: 0.0.0.0/0) thì sẽ sử dụng cái igw\_id (internet gateway)

để 1 intance ra được internetnhau

- có 1 IP public

- đươc gắn vs public subnet (có route table trỏ đến internet GW)

2 subnet

- public subnet

- Routing to 1 internet GW

- intance in public subnet can access internet via ipv4 (or EIP)

- private subnet

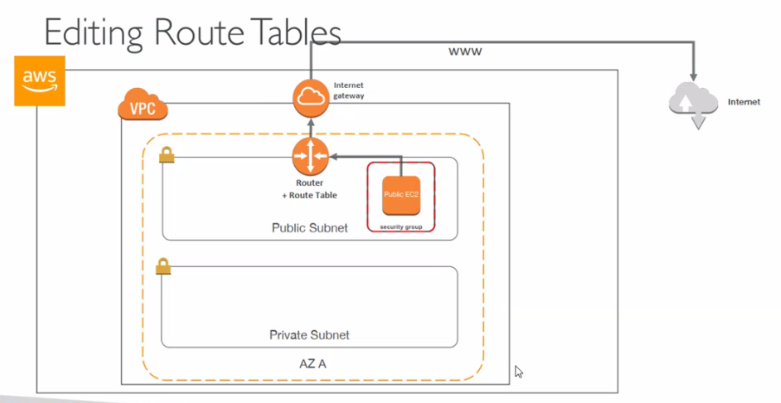
- dont routing to internet gateway

Bài 1: VPC – subnet

- Tạo 1 VPC

- Tạo subnet public và private

- tạo intance trên subnet publet và intantce này kết nối được internet



- Bài làm:

bước 1. Tạo VPC: 10.0.0.0/16

Bước 2: tạo và gắn intenet GW vào VPC

Bước 3: tạo public subnet, private subnet, với CIDR là VPC vừa tạo

public subnet: 10.0.0.0/24

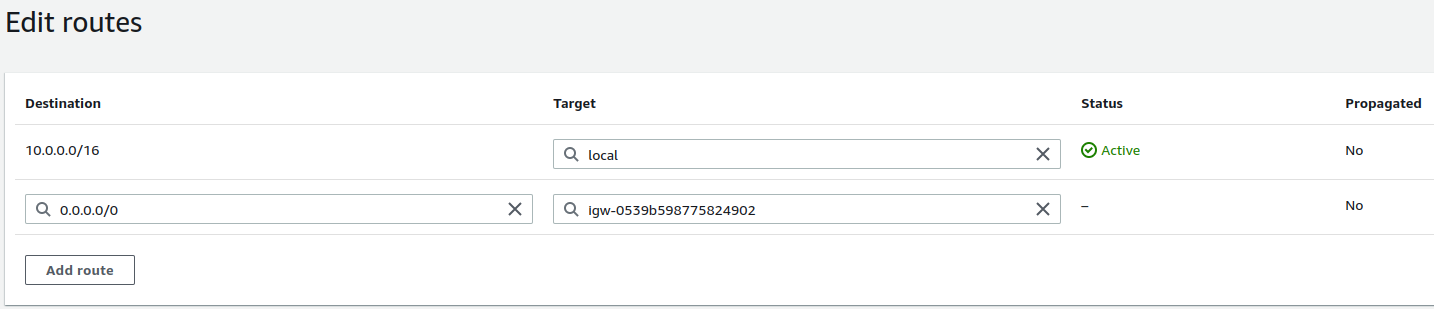
private subnet: 10.0.1.0/24

- làm sao để phân biệt public subnet và private subnet

Bước 4: check route table trên public subnet đã có ra internet (destiantion: 0.0.0.0/0) target internet GW chưa

nếu chưa, tạo route table và assign route table và public subnet

1 subnet chỉ có 1 route table, nhưng 1 route table có nhiều subnet



Bước 5. Tạo intance trên public subnet

lưu ý là khi tạo chọn subnet public

- tôi sẽ tạo 1 intance trên public subnet enable IP public và 1 intance trên public subnet và ko có IP public xem cả 2 đều ra được internet ko

- tôi tạo 1 intance trên private subnet xem 2 intance trên public subnet và private subnet có kết nối dk vs nhau ko

=> kết luận

1 intance để có kết nối internet

- assign IP public

- nằm trong public subnet

=> kết luận 2

2 intance khác subnet ko có kết nối

mà 1 intance nằm trong private subnet có gắn IP public thì cũng ko ssh vào được nó, vì ko có internet GW để phi vào nó

Bài 2: làm thế nào để 1 intance trong private subnet có kết nối internet

dùng NAT

bài này sẽ demo ở dưới

NAT là gì, NAT là phương thức để ánh xạ 1 hoặc nhiều đại chỉ IP sang IP khác (ip public)

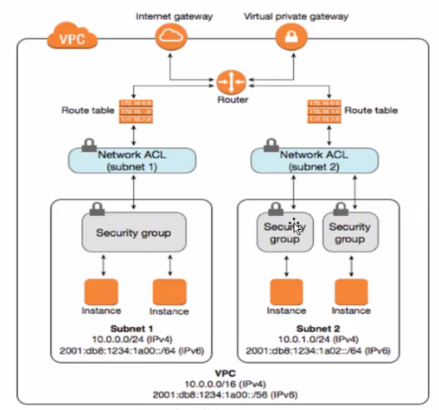
ví dụ mình đang dùng wifi ở nhà, địa chỉ máy tính mình đang là IP private,

thì ngoài internet nó ko hiểu IP private bạn là gì, nên bạn cần 1 moden nhà mạng, bạn ra ngoài intenet nhờ modern đấy bằng 1 địa chỉ IP public

=> vì vậy tương tự như trong AWS, NAT GW trong AWS được sử dụng để các intance trong private subnet có kết nối ra ngoài internet nhưng ngoài internet sẽ ko có kết nối đến các intance này

Nat GW sẽ giúp cho intance ra ngoài internet nhưng vẫn được bảo vệ ko cho thằng khác phi được vào con intance

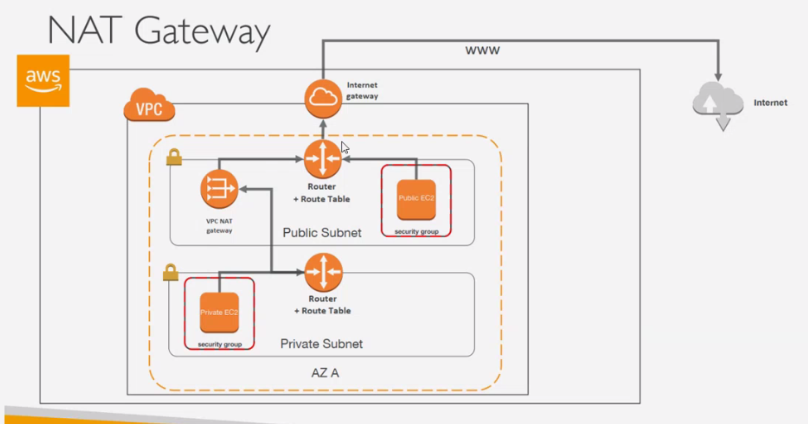
Network Access controller List



ACL bảo vệ subnet, có deny

SG bảo vệ intance, ko deny

NAT GatewayGateway



nat gateway giúp cho intance trong private subnet có thể đi ra được ngoài internet

Bài tập: làm thế nào để 1 intance private subnet ra được internet

- các intance trong cùng 1 VPC nói chuyện được vs nhau

Bước 0: tạo VPC, private, public subnet, route table, internet gateway như ở bài trên

- tạo VPC

- tạo igw attach VPC

- tạo subnet

- route table assign cho subnet (route table quyết định subnet public hay private)

- route table: cũng có route table ra public, route table private

- gắn tới subnet

- thêm rule ra internet gắn vs internet GW hoặc NAT GW

=> check kết nối từ intance public ra internet, nếu được thì các config đã oke

Bước 1: tạo 1 intance ở subnet public có IP public

Bước 2: tạo 1 intance ở Private subnet, ko có IP public

Bước 3:

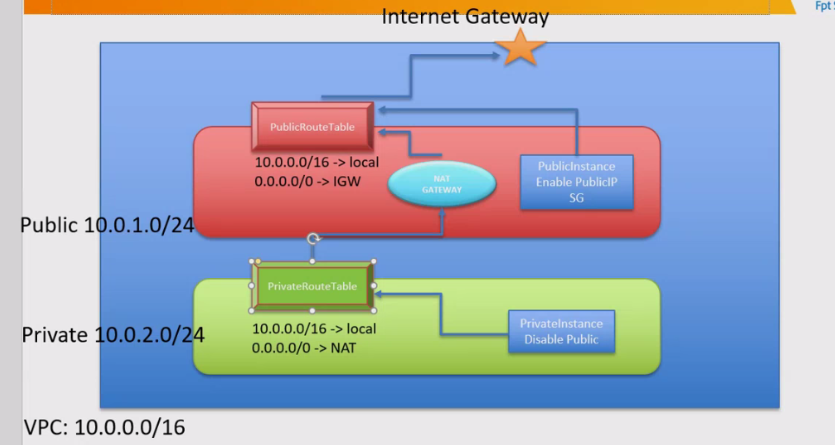
- check kết nối internet ở intance public ra internet

- check kết nối giữa 2 intance

Bước 4: tạo NAT gateway, nat gateway phải ở public subnet, assign luôn EIP

chek route table của private subnet trỏ ra internet qua natGW

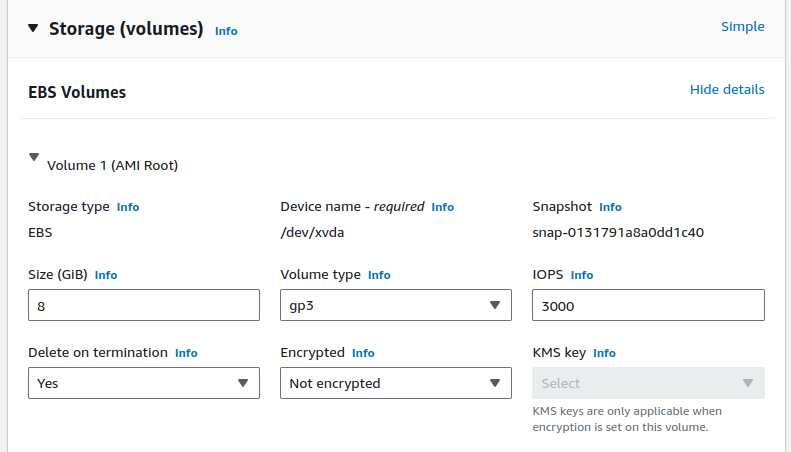
và thế là oke



kết thúc phần network

Volume

EBS volume: tạo để gắn với 1 intance, nó là ổ đĩa gắn qua mạng, kiểu như USB



gp2, gp3 là SSD

snapshot EBS