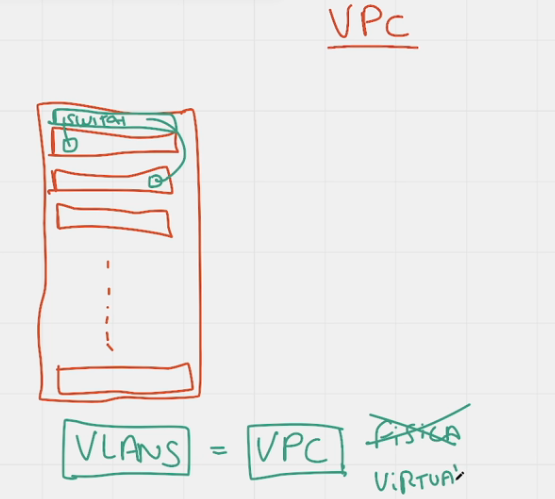
Introdução ao VPC

terça-feira, 13 de junho de 2023

19:29



O VPC funciona como ligação entre uma EC2 e outra que estejam em servidores diferentes, passando por um tipo de switch para fazer esta ligação.

Normalmente conhecida como Vlans mas pela AWS é conhecida como VPC - Virtual Private Cloud, é uma segmentação virtual.

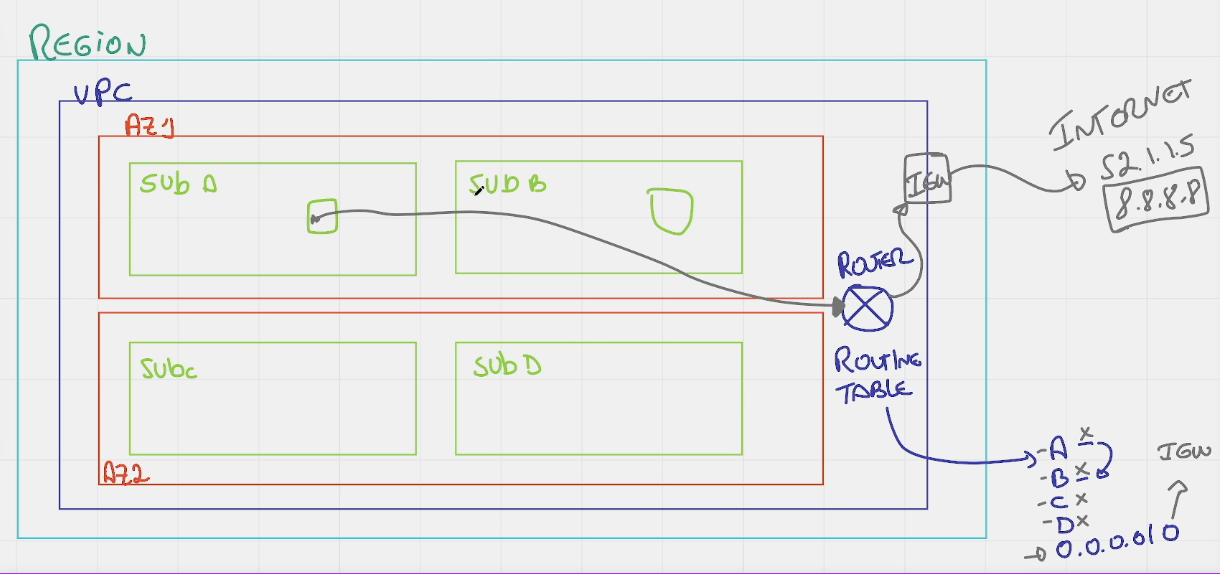
Quem cria e gerencia as vpc's é o usuário porém não é possível se comunicar com a Vpc de outro cliente amazon.

O que é uma VPC ?

terça-feira, 13 de junho de 2023

19:33

* VPC é criada por região
  + As Zonas de disponibilidades estão dentro da VPC
  + Dentro das Zonas de disponibilidades podemos criamos as subnets
  + As VPC são criadas para isolar o seu conteúdo de outro conteúdo em uma mesma região
  + REGION > VPC > AZ > Subnet
  + Dentro de uma VPC existe um roteador
  + Você visualiza a routing table ( Tabela de roteamento ) - Enxerga todas as redes



* As subnets utilizam o roteador para se comunicar com a internet indo até o IGW ( Internet Gateway ), porém se não estiver disponível o ip para saída de internet o roteador não se comunica com o IGW.

Criando uma VPC

quarta-feira, 14 de junho de 2023

13:51

Pesquise por VPC no AWS > Selecione Minha VPC > Criar VPC

**Passo 1** - Somente VPC para criar apenas a VPC

**Passo 2** - Nomear a VPC

**Passo 3** - Escolher se o endereçamento IP tem um grupo ou não, se não tiver deve informar com um tamanho entre /16 e /28.

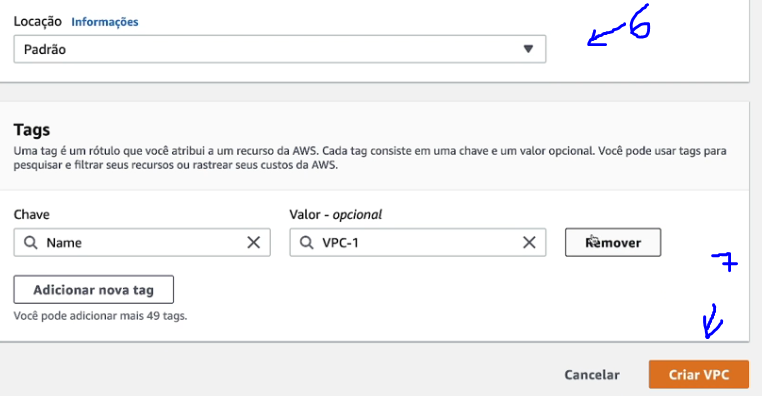
**Passo 4** - Escreva manualmente o seu CIDR IPv4

**Passo 5** - Selecione se o IP Também é IPv6

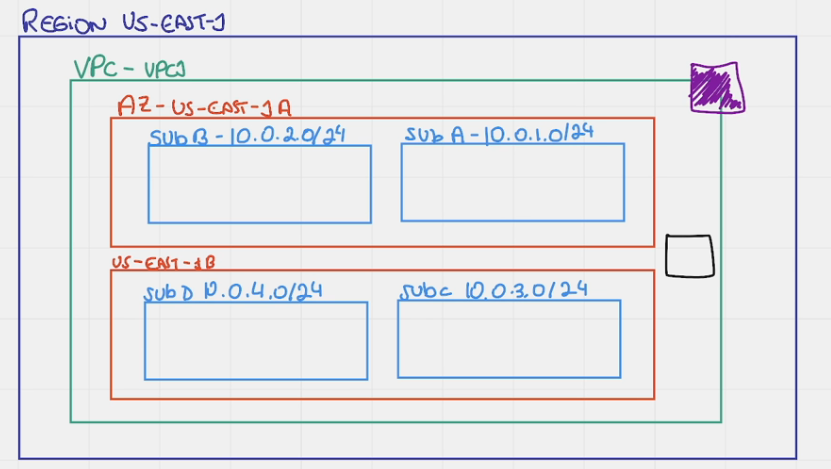
**Passo 6** - Selecionar a locação Padrão ( Mais barato ) ou Dedicada ( Mais Caro )

**Passo 7** - Criar VPC



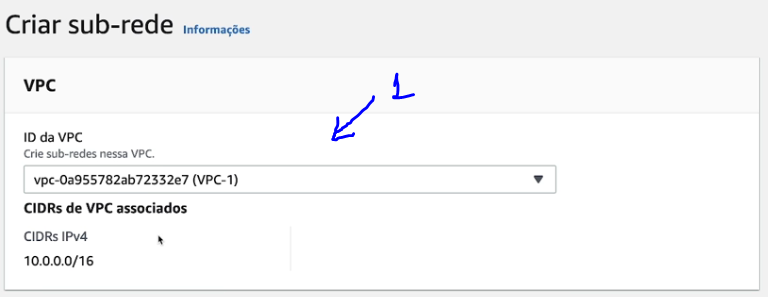


**A locação deve ser padrão por motivos de valores, as opções são padrão e dedicada ( mais cara )**

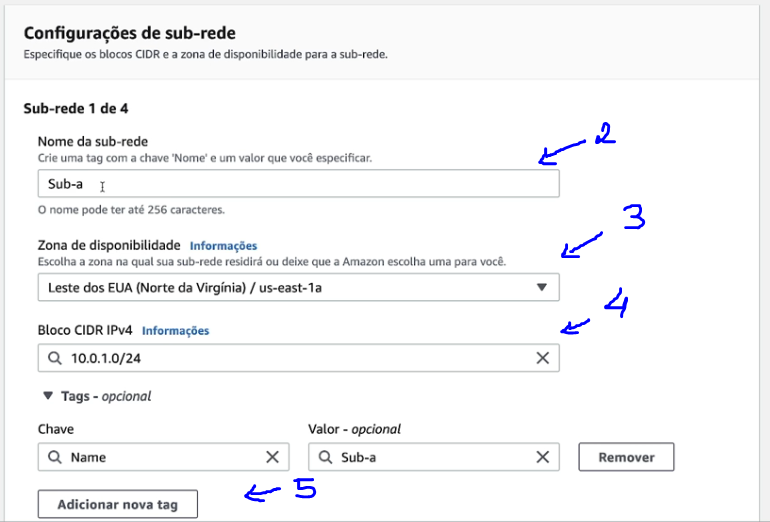


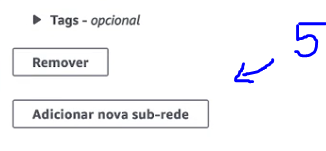
**Criando subredes**

* **Passo 1 - Selecione a VPC**



* **Passo 2 - Crie o nome da sub-rede**
* **Passo 3 - Selecione a zona de disponibilidade**
* **Passo 4 - Digite o endereçamento IP**
* **Passo 5 ( Abaixo ) - Crie uma nova sub-rede após finalizar**

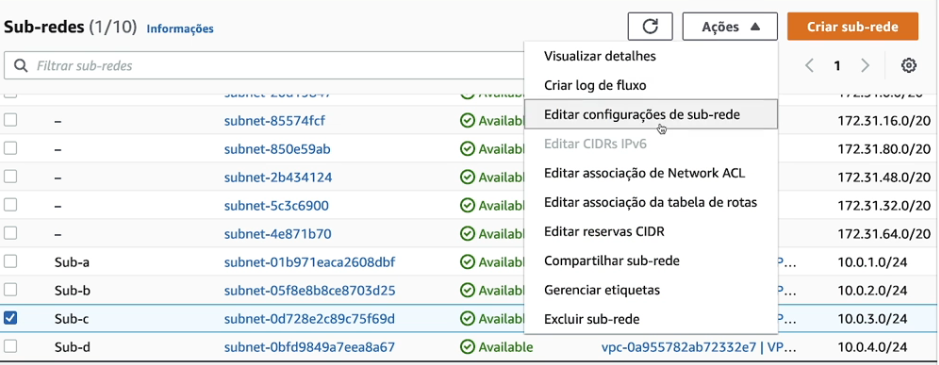




Segmentando as Tabelas de Roteamento

quarta-feira, 14 de junho de 2023

14:43



Transformando subnet em pública

Selecione a Subnet > Editar configurações de sub-rede > Habilitar endereço IPv4 publico de atribuição automática



Nessa aba de sub-redes conseguimos verificar se ela tem ip público

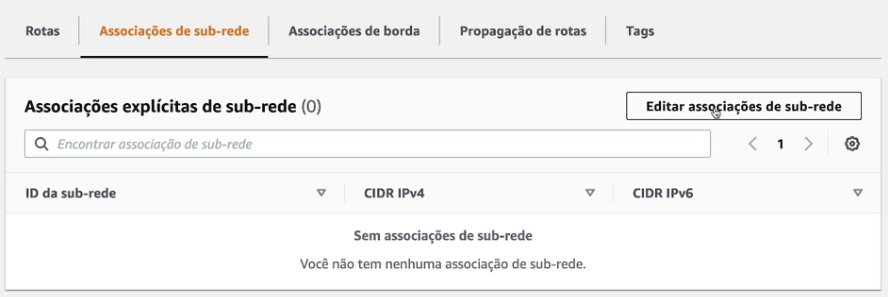
A tabela de roteamento é quem leva informação para o Internet Gateway logo apenas devemos associar a Tabela de roteamento as sub-redes públicas.



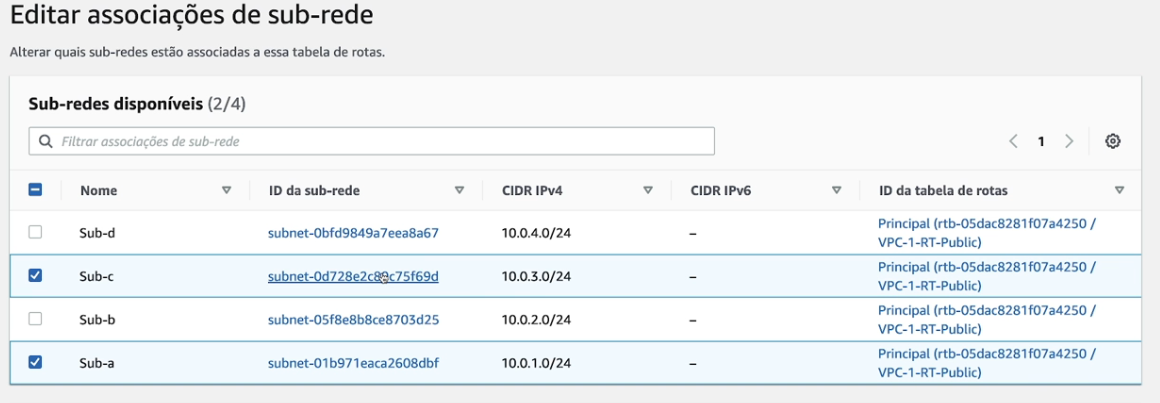
Podemos criar uma tabela de roteamento para associar as nossas sub-redes privadas

**Associando tabela de roteamento as sub-redes**

**Selecione a tabela de roteamento > Associações de sub-rede > Editar associações de sub-rede**



**Associe as sub-redes que contem ip públicos a tabela de roteamento que foi selecionada para associar elas**



**O mesmo serve para as tabelas de roteamento para as sub-redes privadas**

Criando um Internet Gateway e adicionando roteamento

quarta-feira, 14 de junho de 2023

15:05

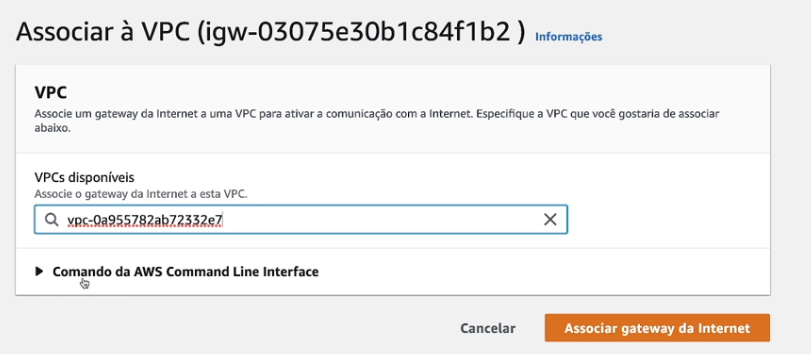
Passo a Passo:

VPC > Internet Gateways > Criar gateway da internet

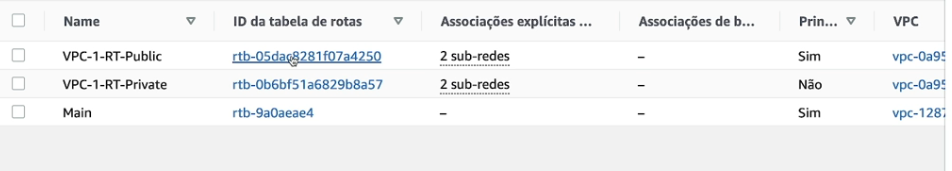


**Conectando a tabela de roteamento ao IGW ( Internet Gateway )**



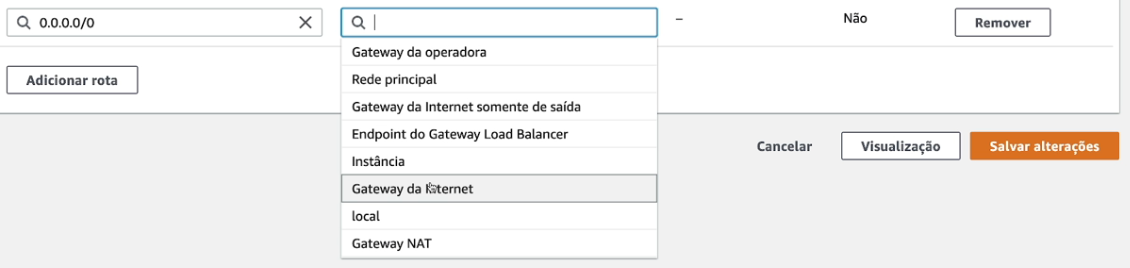


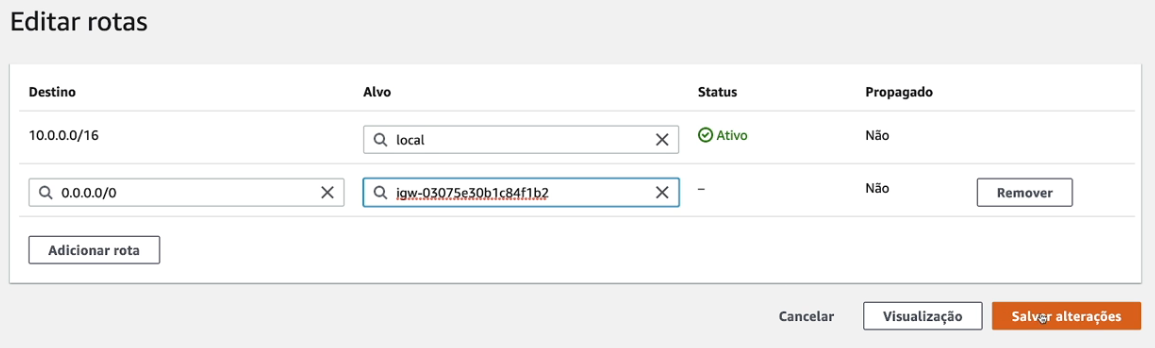
**Selecione a tabela de roteamento pública**



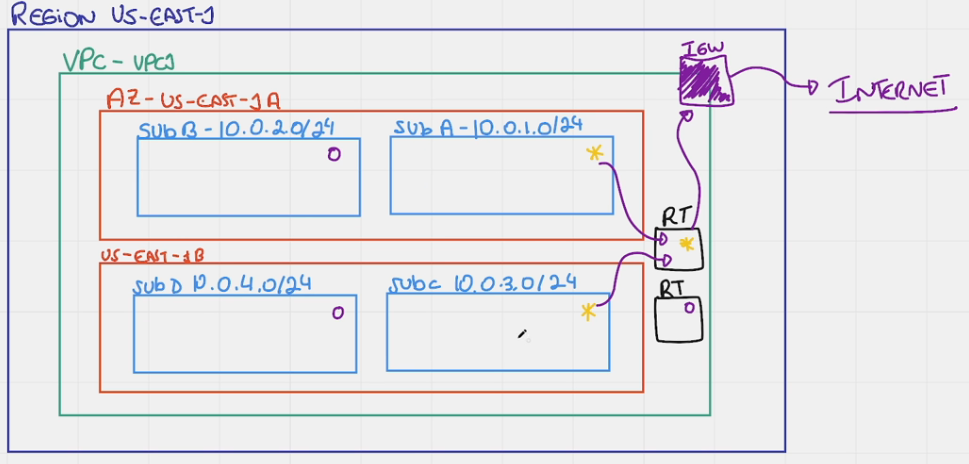
**Adicionando rota para internet pela tabela de roteamento para o IGW**







**Dessa forma já está assim**



A sub-rede está associada a tabela de roteamento que também está associada ao internet gateway com o ip para internet.

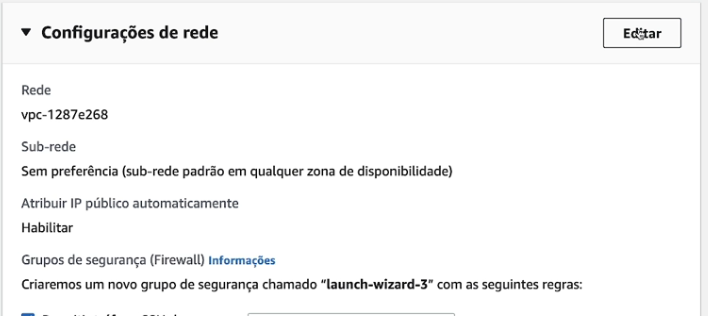
Adicionando as instancias publicas a EC2

quarta-feira, 14 de junho de 2023

15:16

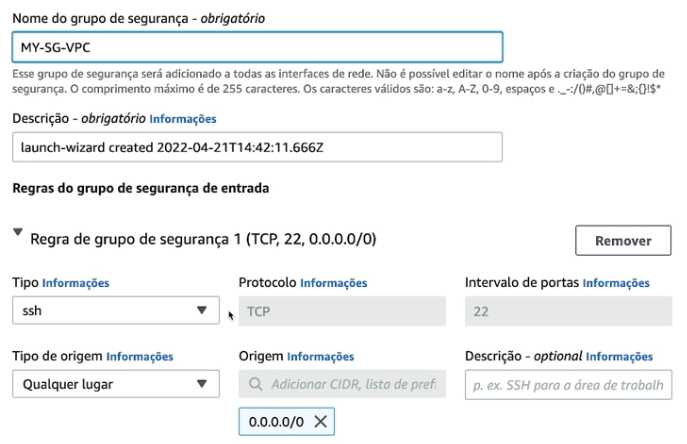
Criando instancia e configurando para VPC

O que muda na criação da EC2 dessa vez é a configuração de rede onde devemos implementar o VPC criado e a subrede





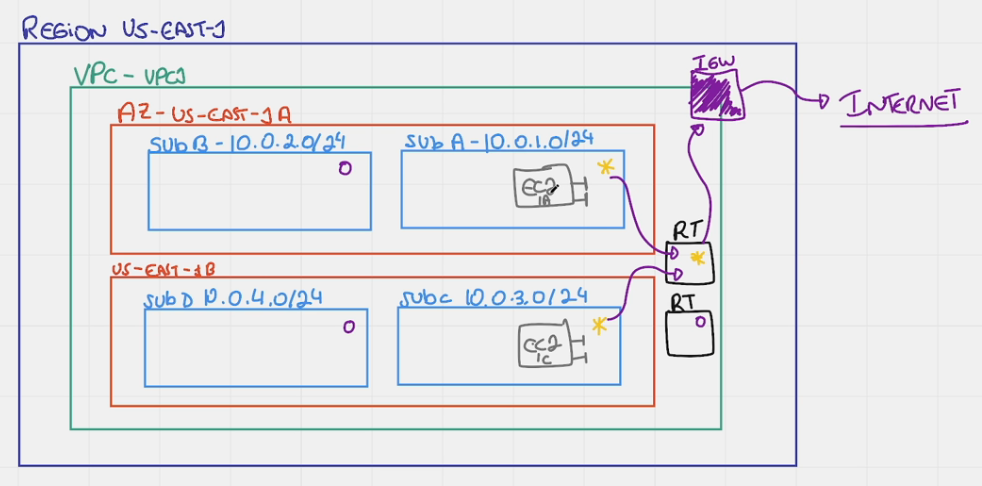
**Criar um grupo de segurança**



**O tipo deve ser atribuido da forma que você preferir mas por convenção para teste podemos trocar o ssd por todo o trafego**

**A partir da criação da instancia ela terá acesso a internet**

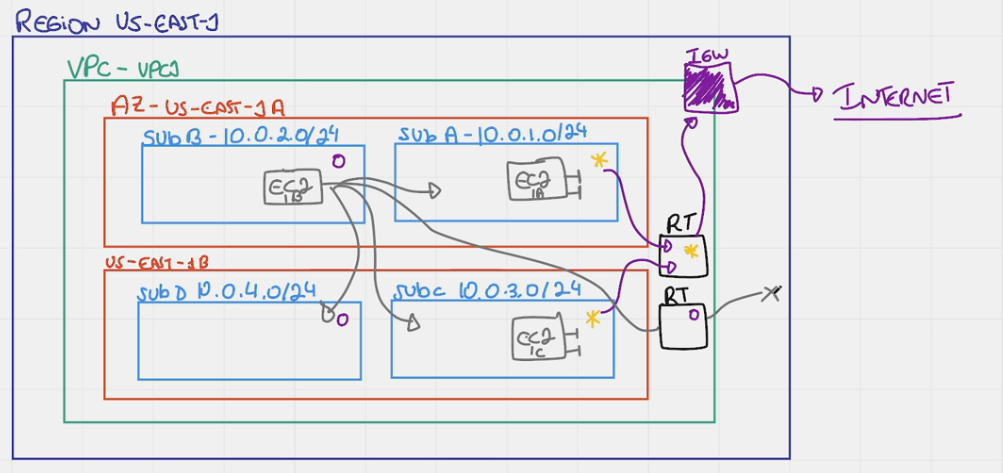
**Quando criamos as instancias e conectamos ao VPC e subredes diferentes quando elas estão na mesma VPC e a tabela de roteamento associadas, elas se comunicam entre si.**



Adicionando Instancias privadas EC2

quarta-feira, 14 de junho de 2023

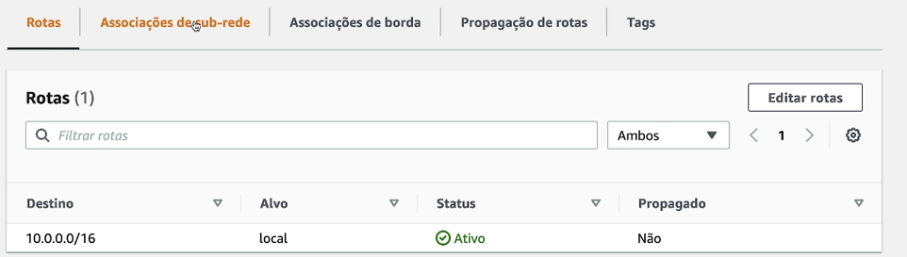
17:51



As instancias EC2 privadas se comunicam entre si e com as outras públicas porém não tem acesso para comunicação com a internet

Contudo as instancias que não tem ip público não conseguem se conectar, a não ser usando o bastion hosts

As tabelas de roteamento em uma mesma VPC se conectam entre sim



As sub-redes privadas se conectam através da VPC por que elas tem acesso local porém não tem acesso a internet

É possível acessar uma instancia privada atraves de uma instancia pública porém é necessário a key pair para permitir esse acesso.

Configurando um bastion host

quinta-feira, 15 de junho de 2023

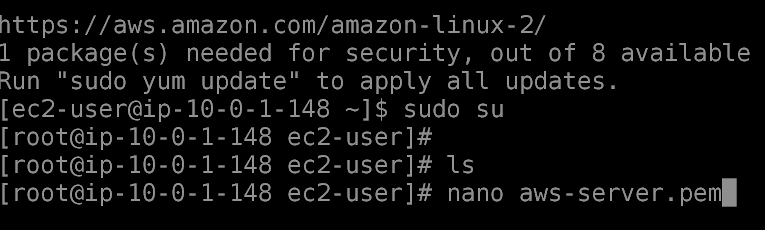
17:29

* **Acessando a máquina com a chave key pair**

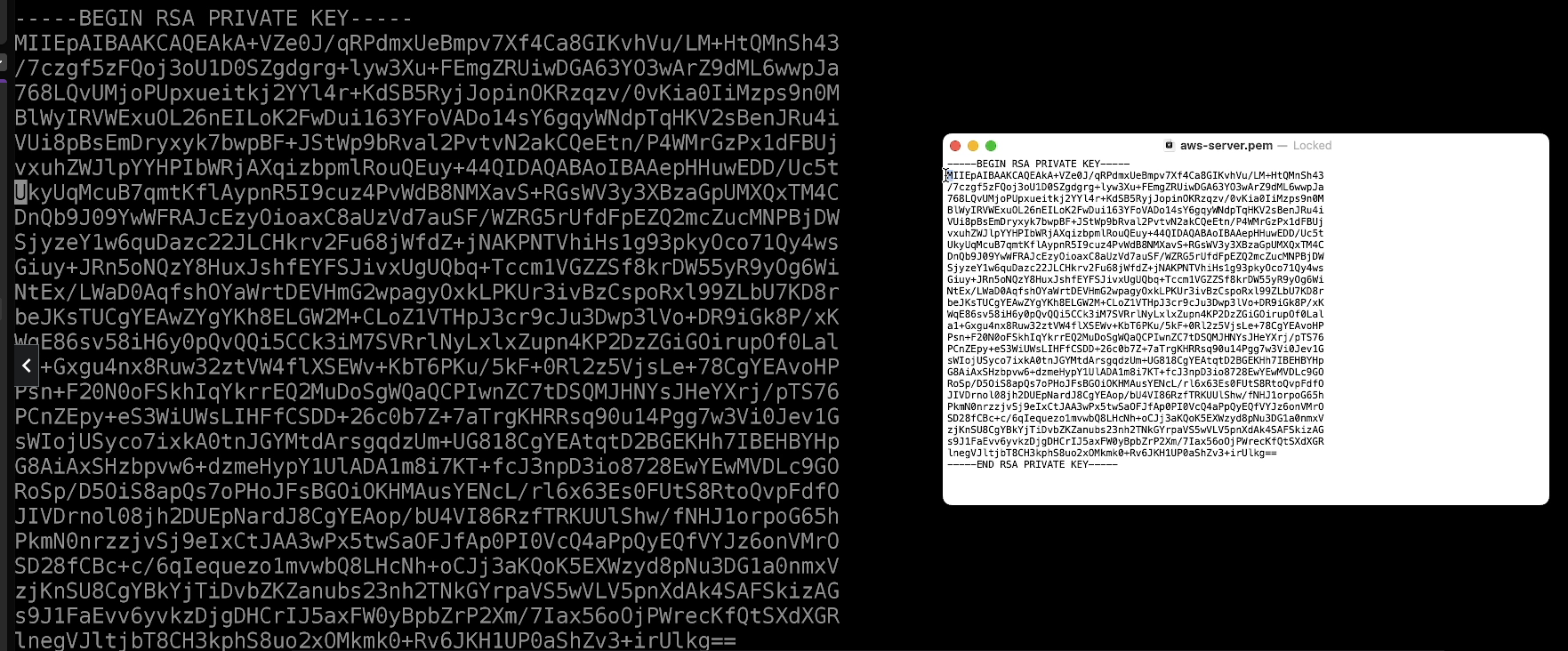
* Formato .pem

Passo:

* Conectamos uma EC2 pública
* Terminal digite:
  + **Sudo su** - Se tornar admin
  + **Nano aws-server.pem** - Criando um arquivo ( Key pair )

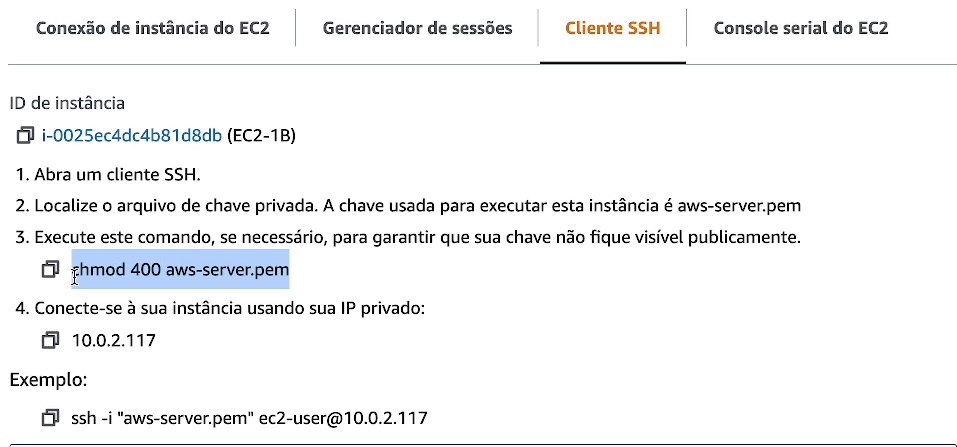


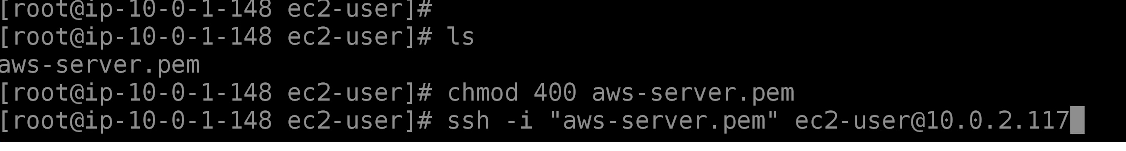
* Copie o que está dentro da key pair e cole dentro da criação do arquivo na instancia linux
* Apague os espaços e deixe identico ao key pair dentro do .pem, caso existe uma diferença mínima que seja a conexão não será permitida



* **Conectando instancia diferente na instancia com o arquivo .pem**

* Selecione a instancia que deseja conectar > Conectar > Cliente SSH > Copie os endereços e cole na instancia bastion host

* 



* A partir disso a instancia está conectada a outra instancia que está funcionando como bastion host
* Qualquer que seja a instancia criada se se estiver dentro do VPC e tenha a mesma key pair, consegue usar a instancia que contem o arquivo .pem.
* Sair da instancia basta usar exit

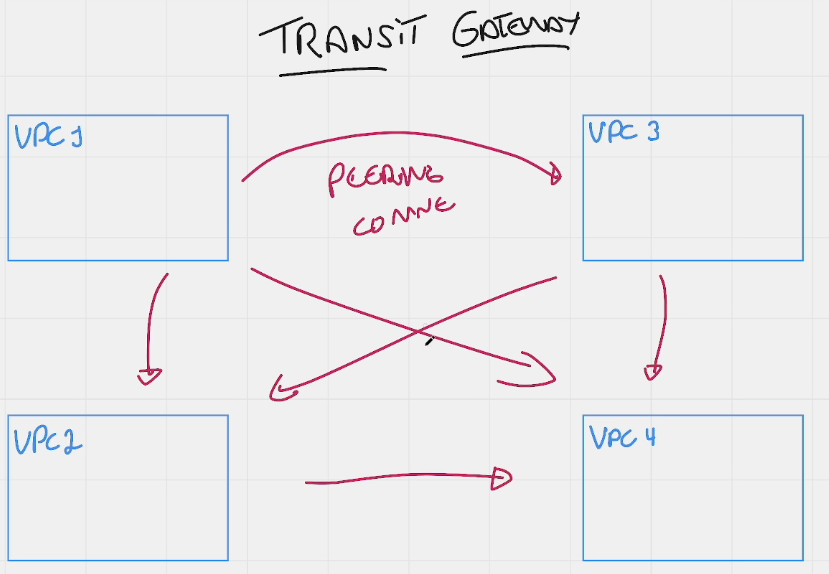
AWS Transit Gateway

quinta-feira, 15 de junho de 2023

17:47

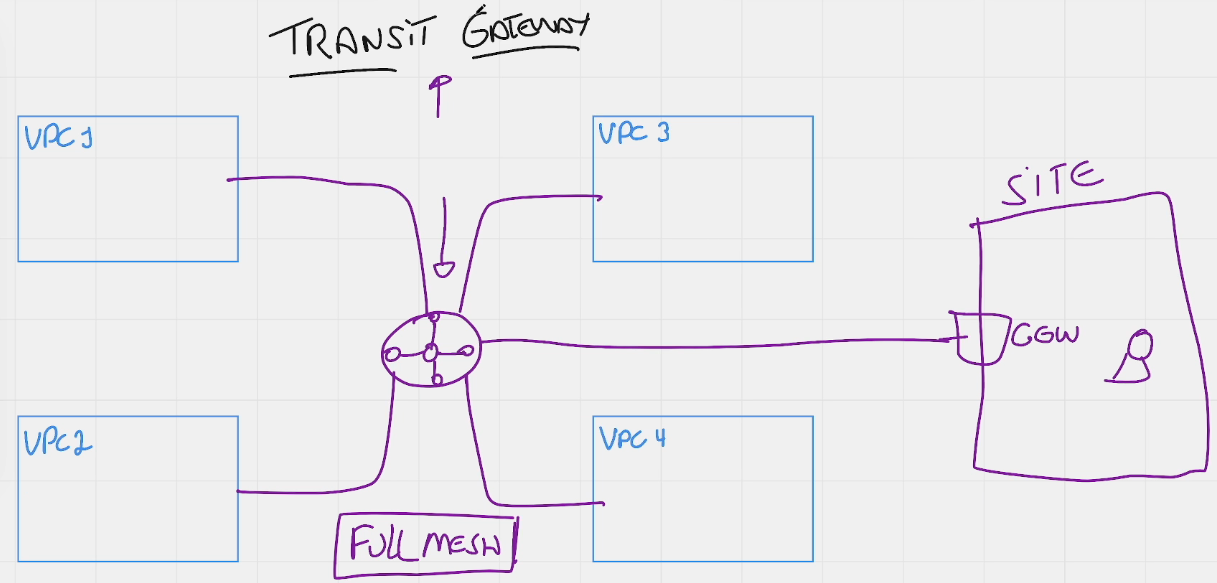
Melhorando conexões entre VPC

A partir do crescimento da empresa é necessário a conexão entre várias VPC



* A conexão simples de 1 para 1 é um peering connect

Uma quantidade maior ex: 20 VPC's fica um pouco mais complicado



O Transit Gateway serve como um roteador onde faz conexão entre diversas VPC's e também consegue receber um tráfego e repassar para diversas VPC's

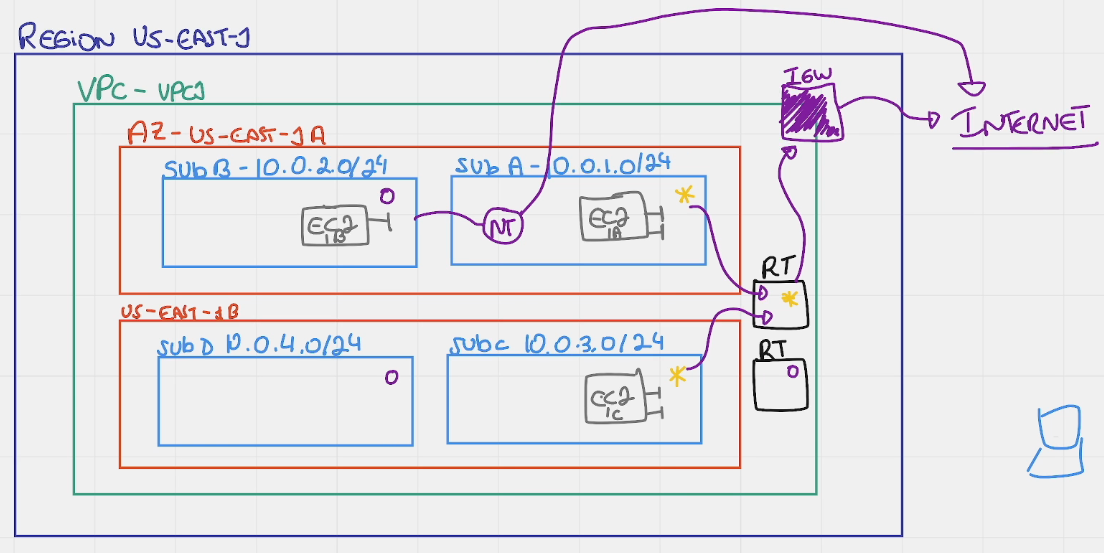
* Essa Conexão é chamada de Fullmesh

Configurando o NAT Gateway

quinta-feira, 15 de junho de 2023

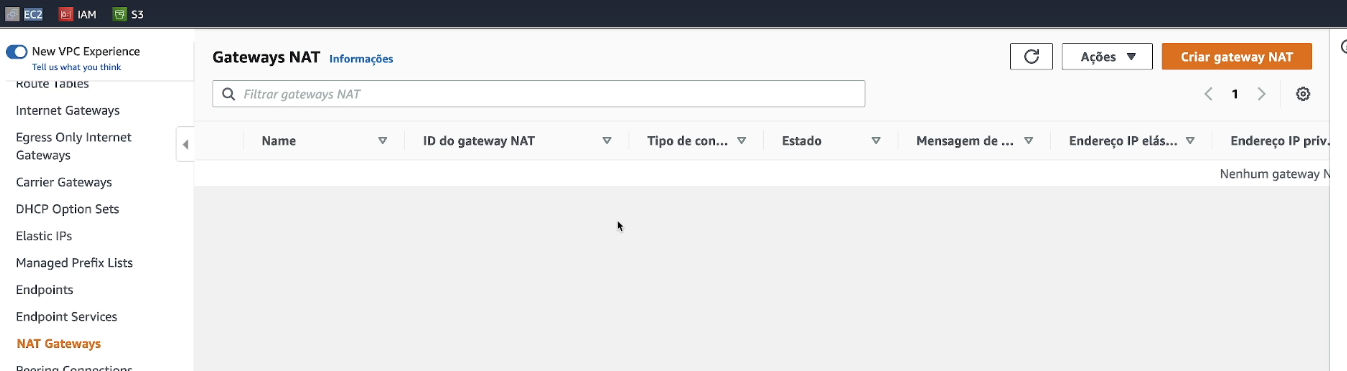
17:53

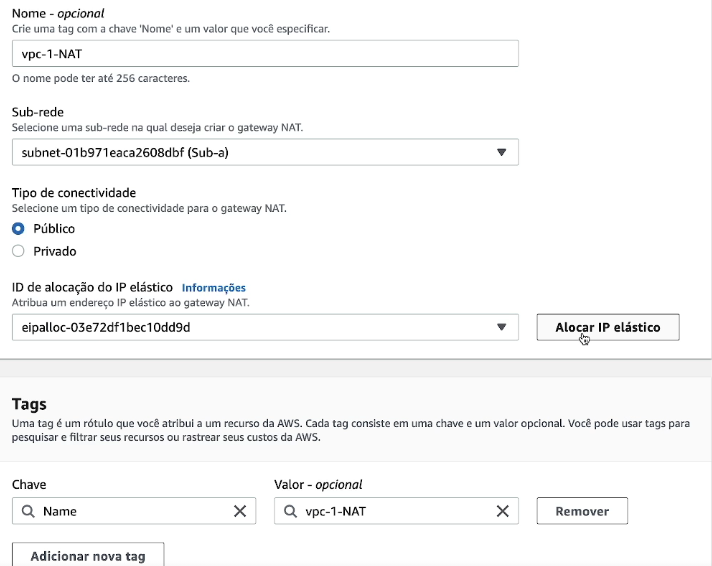
Quero que minha instancia que não tem acesso a internet usando o bastion host consiga acessar a internet com o NAT Gateway - A máquina consiga acesso a internet porém a internet não tenha acesso a minha maquina para manter a segurança.



* A sigla NT simboliza Networking adress transaction que tem acesso a internet e precisamos conectar uma instancia EC2 de uma subnet privada a outra EC2 que está em outra subnet que é pública para ter acesso a internet através do NAT.

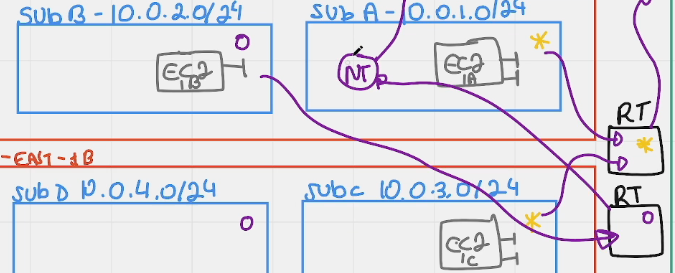
* **Criando uma NAT**





* A partir disso precisamos usar a tabela de roteamento privada para conectar via NAT Gateway

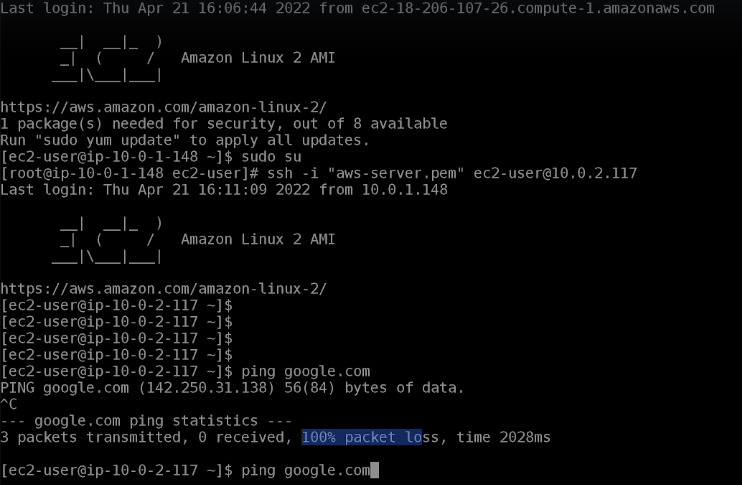
* **Conectando Tabela de roteamento para internet**



* Passo :

* Route Tables > Selecione a Tabela de roteamento privada > Editar rotas > adicionar rota > ip 0.0.0.0/0 > Gateway NAT > concluir

* A partir disso a instancia privada terá acesso a internet porém apenas a instancia terá acesso a internet, nenhum usuário consegue acessar a máquina de fora mantendo a segurança da máquina.



* Sempre utilize NAT Gateway para Subnet privadas, porém não é preciso deixar constantemente habilitado o NAT Gateway, pode ser habilitado apenas quando for ser utilizado.

* Sempre utiliza Internet Gateway para Subnet públicas

Diferença entre Stateful e Stateless

quinta-feira, 15 de junho de 2023

18:14

* Camada de seguranças - Stateful e Stateless

* Security Group - Placa de Rede virtual ( Elastic Networking interface )
* Network ACL - NACL