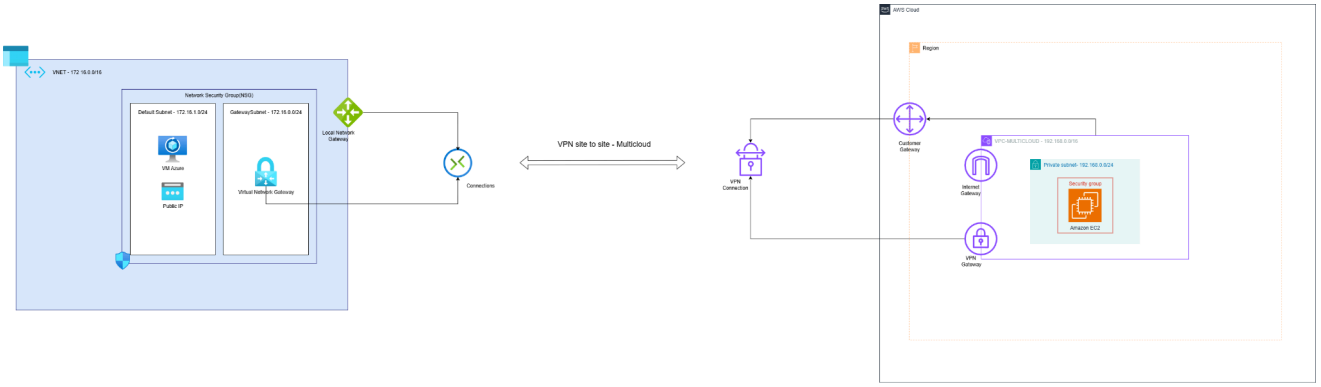
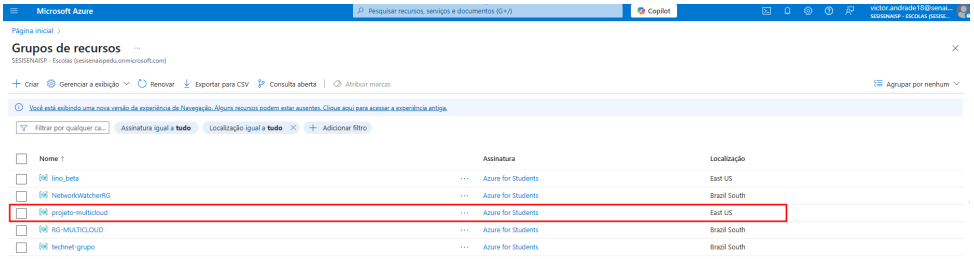
Multicloud AZURE x AWS

TOPOLOGIA



Lado AZURE

1) *Criando Grupo de recursos(projeto-multicloud) - organização dos recursos da azure*



2) Criando VNET + Subnet default e Subnet de gateway

- subnet de gateway vai ter a função de funcionamento para o VNG

- subnet default para criação da VM

Criar rede virtual ...

Básicos | Segurança | Endereços IP | Rótulos | **Revisar + criar**

Exibir modelo de automação

Básicos

Assinatura	Azure for Students
Grupo de Recursos	lino_beta
Nome	VNET-MULTICLOUD
Região	East US

Segurança

Azure Bastion	Desabilitado
Firewall do Azure	Desabilitado
Proteção de Rede do DDoS do Azure	Desabilitado

Endereços IP

Espaço de endereço	172.16.0.0/16 (65.536 endereços)
Sub-rede	GatewaySubnet (172.16.0.0/24) (256 endereços)
Sub-rede	default (172.16.1.0/24) (256 endereços)

Rótulos

3)*Criação do VNG(Virtual Network Gateway)*

- *sku: vpngw1*
- *geração: generation1*
- *geração de novo public IP*

Criar gateway de rede virtual ...

Validação aprovada

Básico | Marcas | **Revisar + criar**

Básico

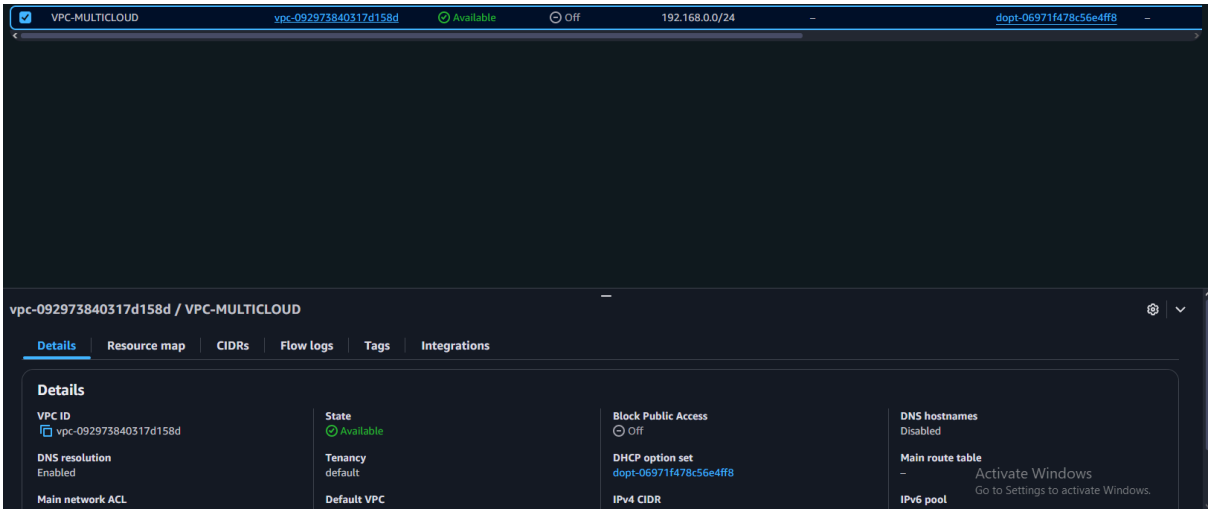
Assinatura	Azure for Students
Grupo de recursos	projeto-multicloud
Nome	VGN-multicloud
Região	East US
SKU	VpnGw1
Geração	Generation1
Rede virtual	VNET-MULTICLOUD
Sub-rede	GatewaySubnet (172.16.0.0/24)
Tipo de gateway	Vpn
Tipo de VPN	RouteBased
Habilitar o modo ativo-ativo	Desabilitado
Habilitar Conectividade Avançada	Desabilitado
Configurar BGP	Desabilitado
Endereço IP público	public-ip-multicloud

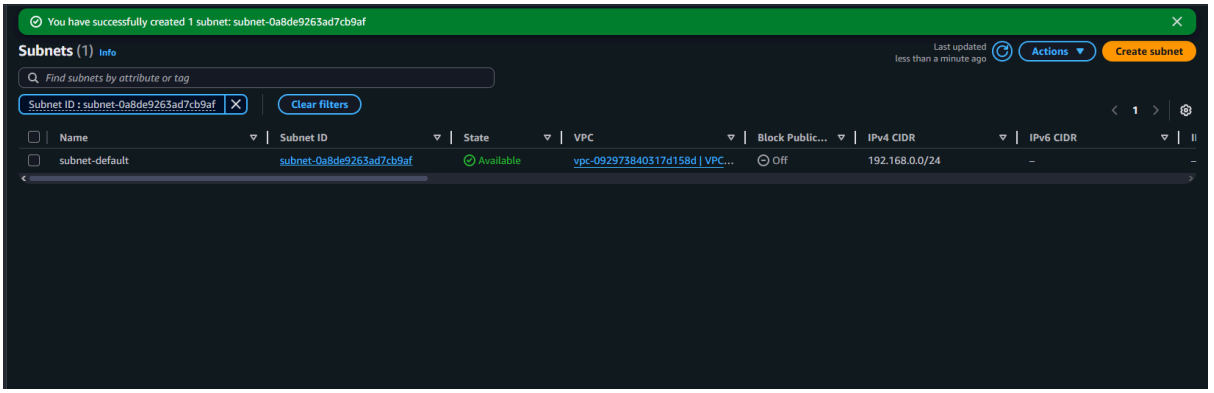
Marcas

Nenhum

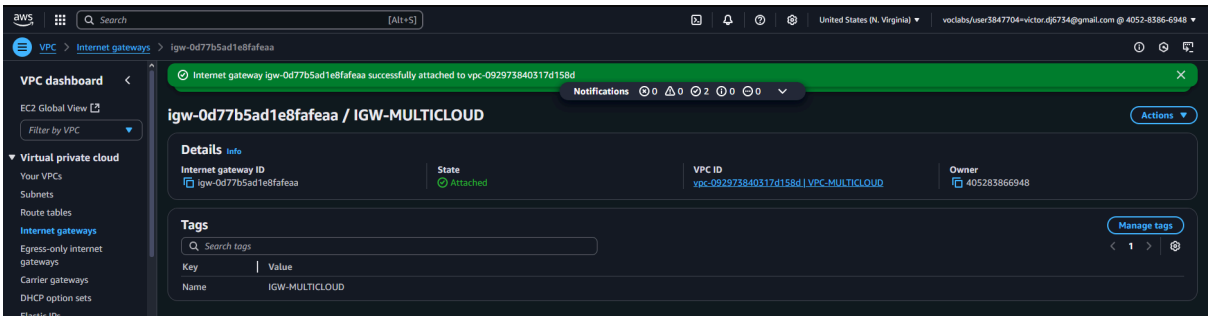
Lado da AWS

4) Criação de VPC e subnets

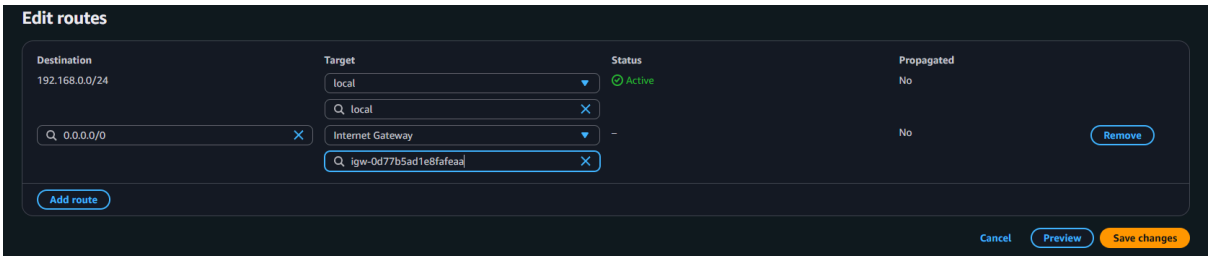


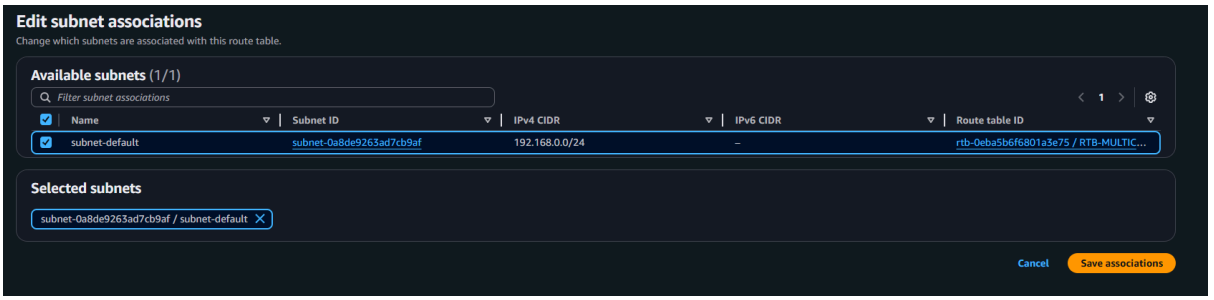


5)Criação do INTERNET Gateway e atracar na VPC



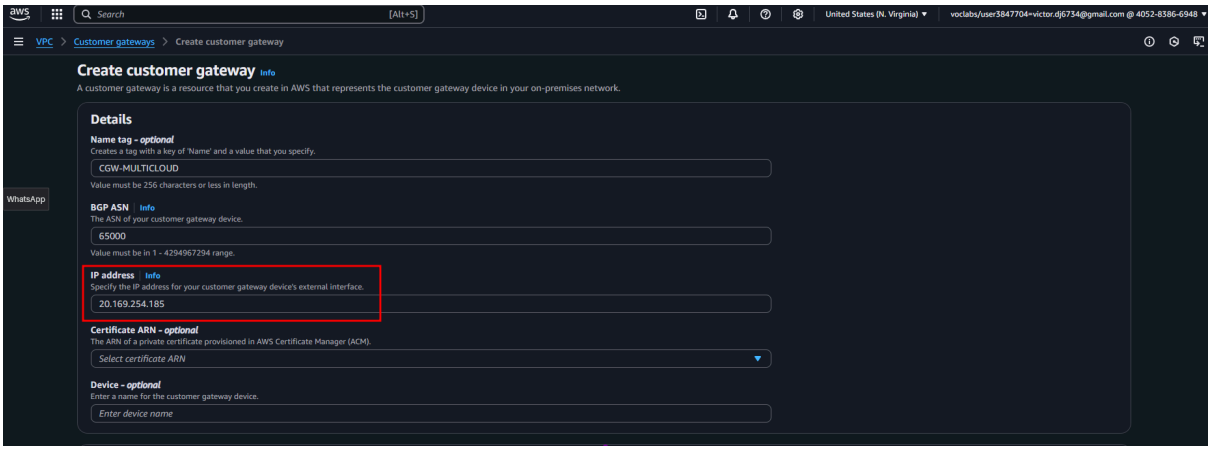
6) Criando route table, associando a subnet e criando rota apontando para um internet gateway

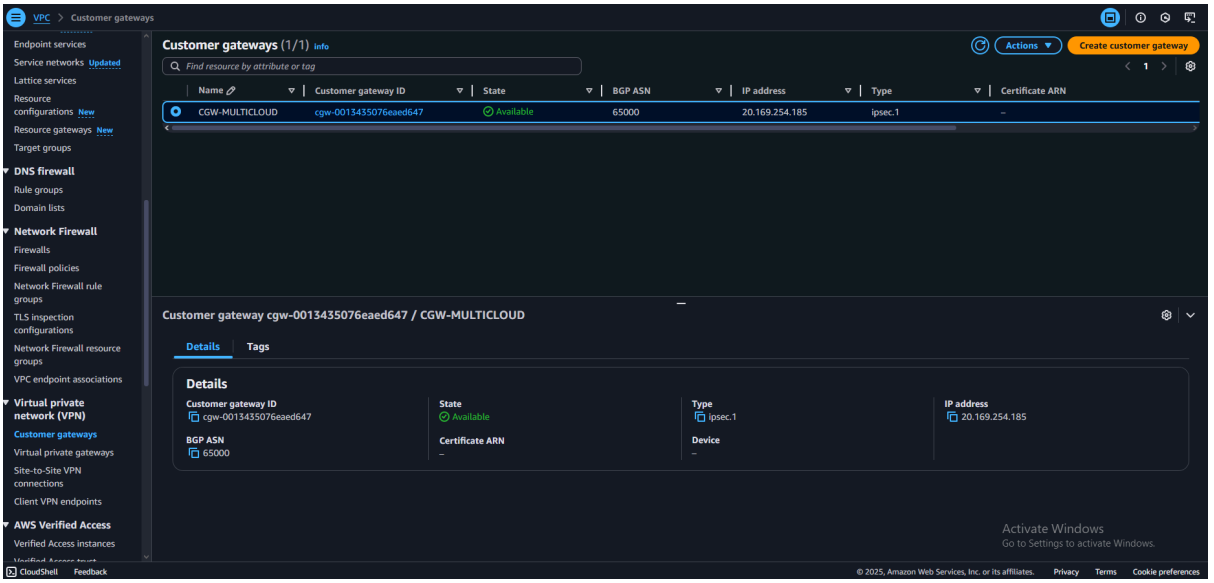




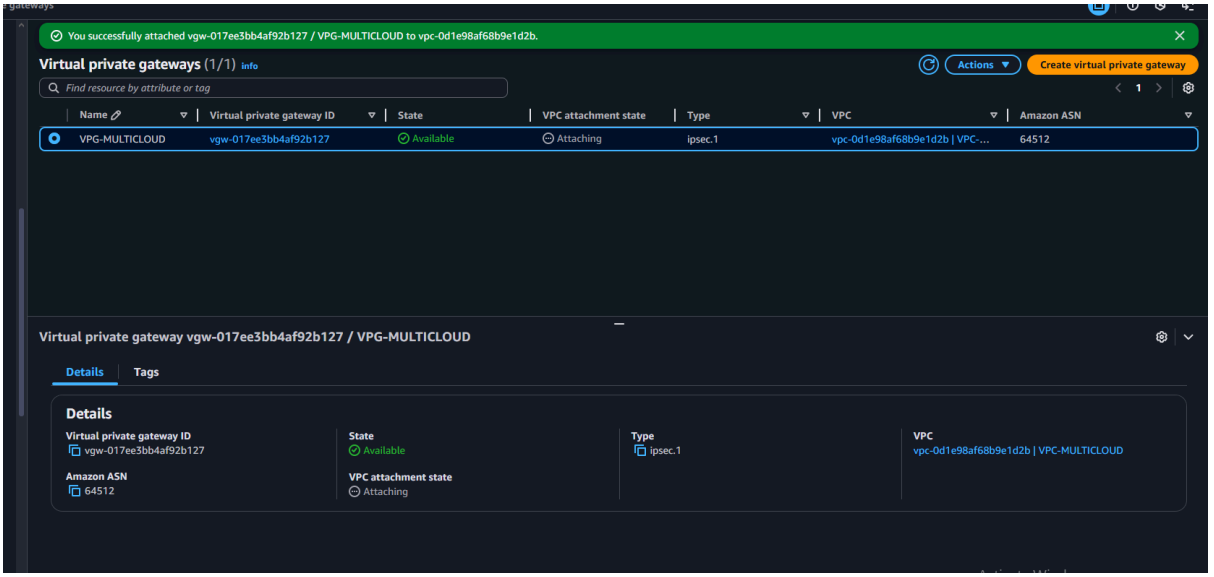
7) Criação do customer gateway (VPC > Customer gateway)

. em " Ip address " inserir o IP publico do virtual network gateway gerado no passo 3 do lado azure .

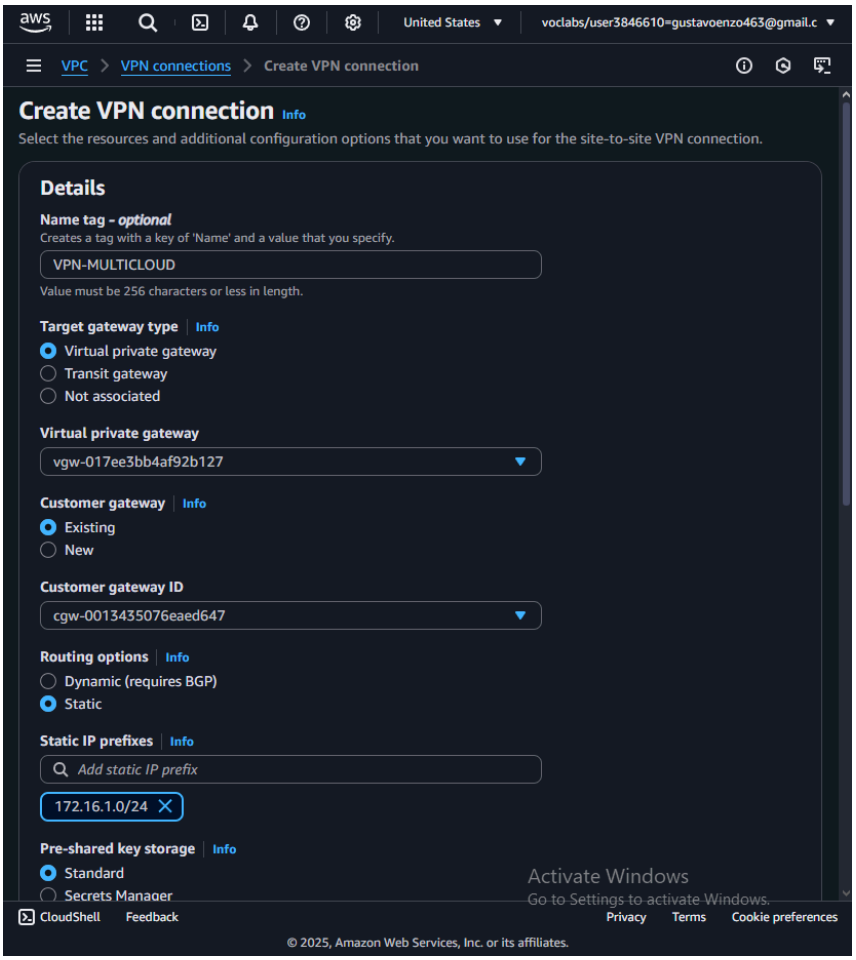




8) Criação do VPG(Virtual private gateway) e atraca-lo na VPC

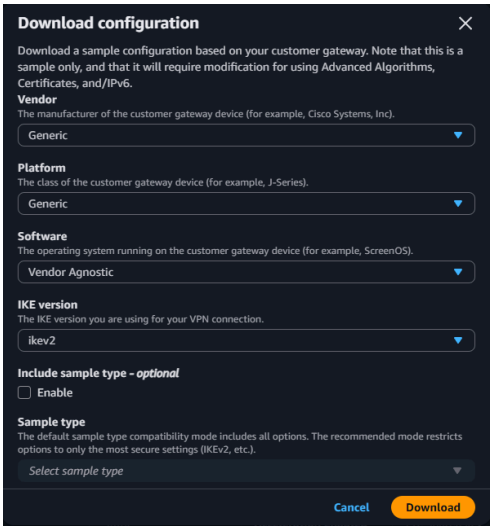


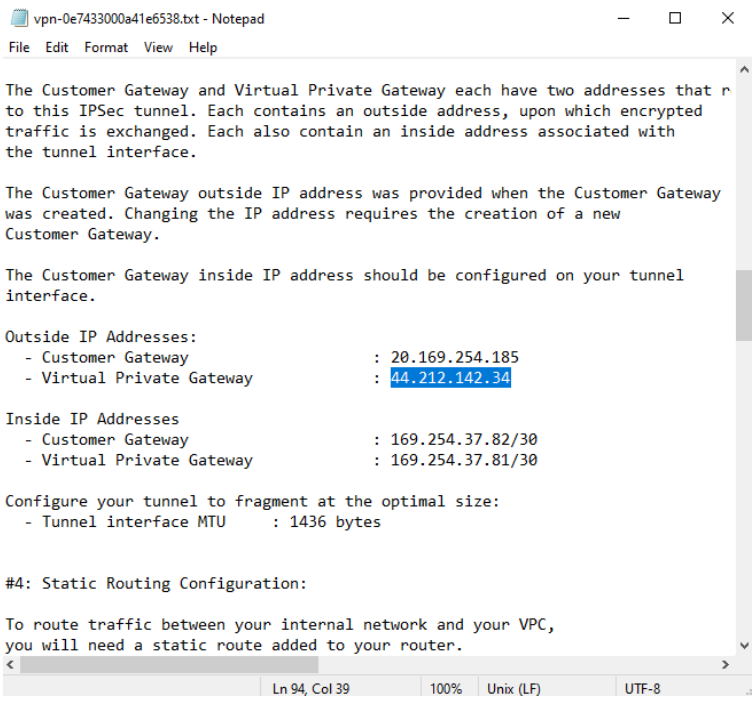
9)Criando VPN CONNECTIONS (site to site vpn connections)
Routing options - static indicar o escopo da rede da sub-rede onde serão alocadas suas maquinas na azure , nesse caso : 172.16.1.0/24



10) Baixar o arquivo de configuração da VPN

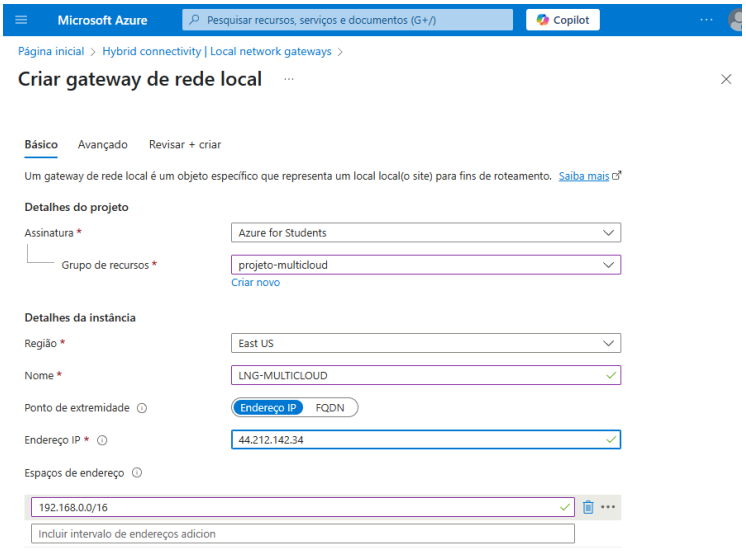
- *generic*
- *generic*
- *vendor*
- *agnostic*
- *ikev2*





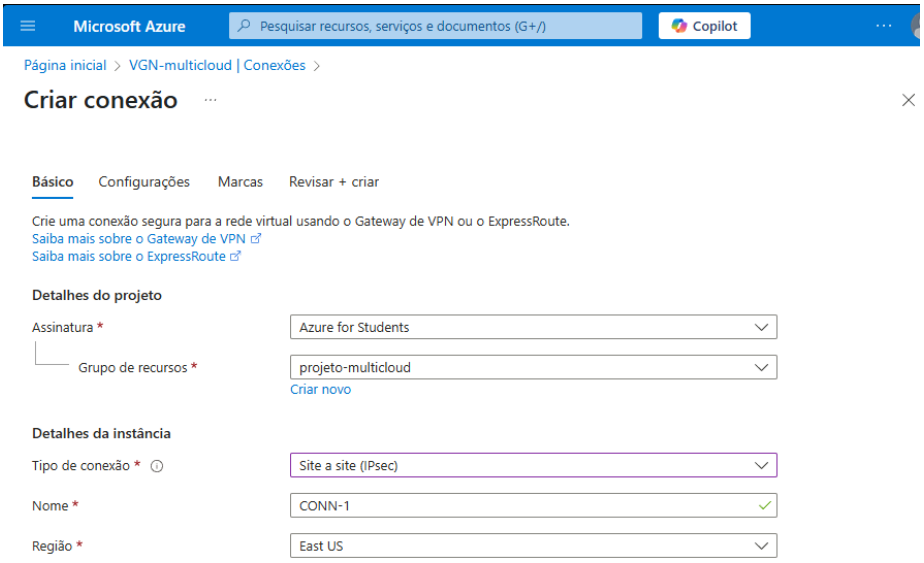
Pegue o IP do túnel criado no documento do VPG e adicione no LNG

11)Criando Local network gateway(LNG)



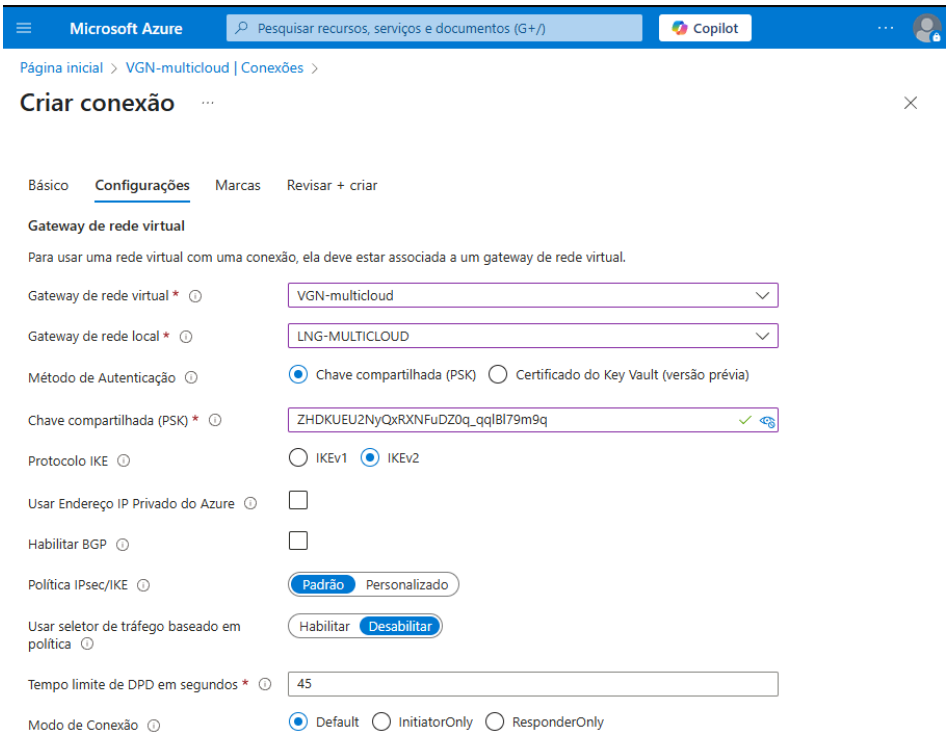
<u>obs - podem ser feitos até dois tuneis (recomendado). ao criar o outro LNG, colocar o IP do segundo tunel na doc do VPG na AWS</u>

12) criando conexões no virtual private gateway (virtual network gateway > conexões > adicionar)Tipo de conexão : site a site (ipsec)



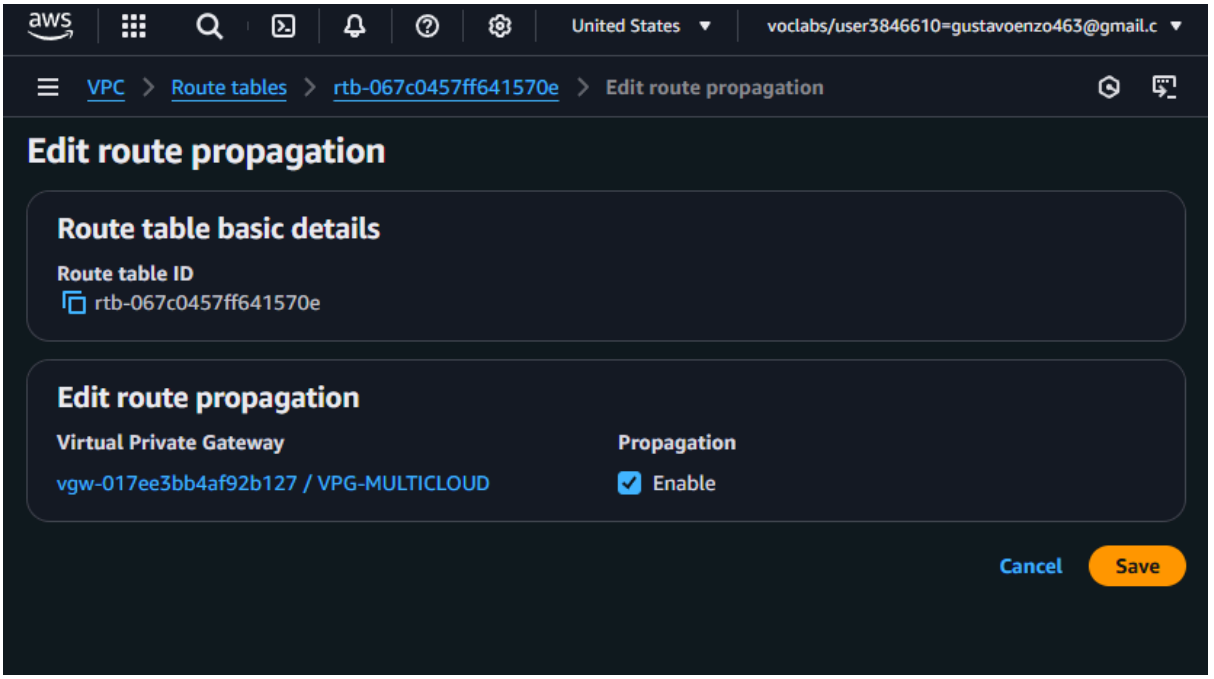
13) PSK : selecionar a PSK do primeiro tunel ,presente no arquivo de configuração e adcione na criação das conexões(gerado no passo 10).
protocolo ike : ikev2

```
IPSec Tunnel #2
================================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum requirement of AES
Category "VPN" connections in the GovCloud region have a minimum requirement of
You will need to modify these sample configuration files to take advantage of A
NOTE: If you customized tunnel options when creating or modifying your VPN conn

Higher parameters are only available for VPNs of category "VPN," and not for "V
The address of the external interface for your customer gateway must be a stati
Your customer gateway may reside behind a device performing network address tra
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewal
If not behind NAT, and you are not using an Accelerated VPN, we recommend disab
  - IKE version              : IKEv2
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : ZHDKUEU2NyQxRXNFuDZ0q_qq1Bl79m9q
  - Authentication Algorithm : sha1
  - Encryption Algorithm     : aes-128-cbc
  - Lifetime                 : 28800 seconds
  - Phase 1 Negotiation Mode : main
  - Diffie-Hellman           : Group 2

#2: IPSec Configuration

Configure the IPSec SA as follows:
Category "VPN" connections in the GovCloud region have a minimum requirement of
```

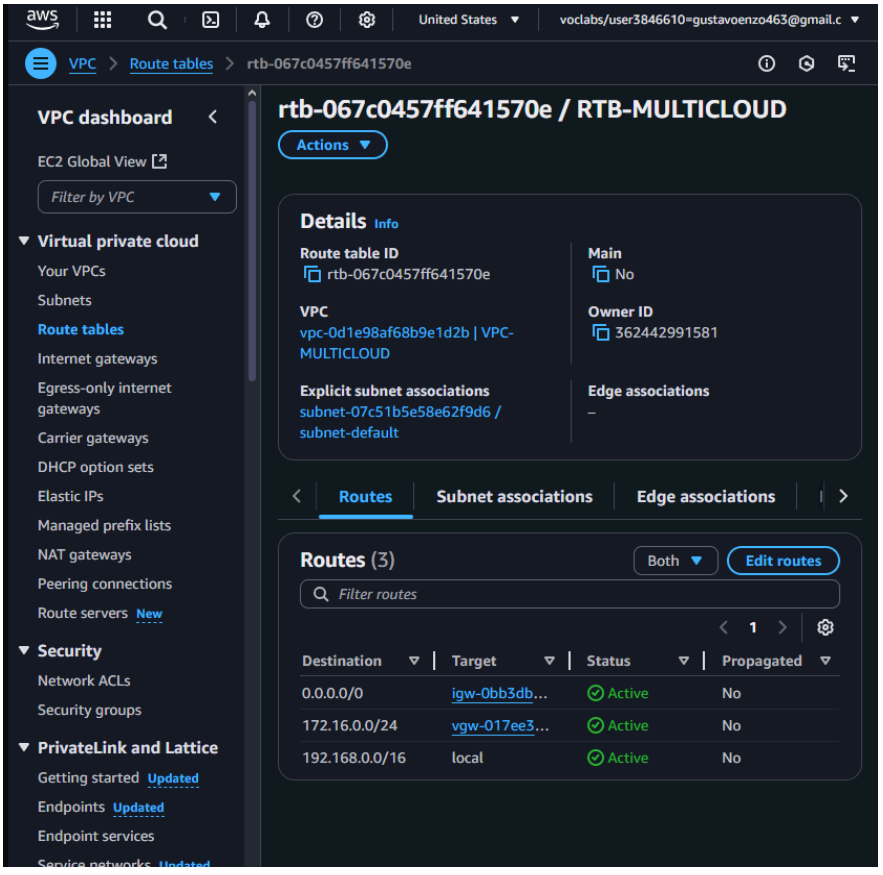


obs - é possível (recomendado) criar até duas conexões . Para isso é necessário ter dois local network gateway (criado no passo 11) . Ao criar uma segunda conexão, forneça como PSK o valor da PSK do segundo túnel disponível no arquivo de configuração gerado no passo 10 . Também aponte para o segundo local network gateway em " gateway de rede local "

Criar rota na route table para o virtual-private gateway (vpc > route tables > route propagation > edit routepropagation > enable)



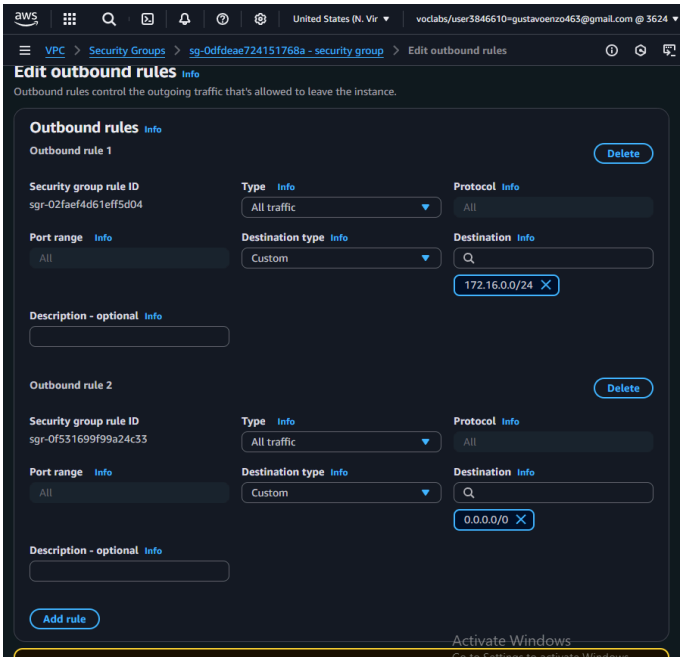
também é possivel adicionar a rota manualmente : destination : rede da azure (no caso , 172.16.0.0/24) target : virtual private gateway



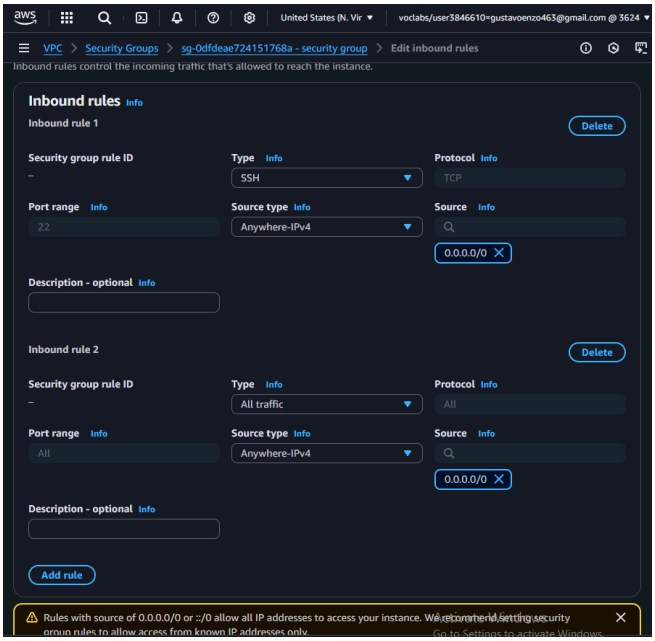
Validações finais e criação de instâncias Nesse ponto, ambos os tuneis de ambos os lados deveram estar conectados e estáveis Seguiremos estabelecendo regras de uma rede interna para outra ————> importante !!!

14) Security Group AWS

Outbound Rule - Liberando todo o tipo de tráfego para qualquer rede , e todo tipo de tráfego para a rede azure

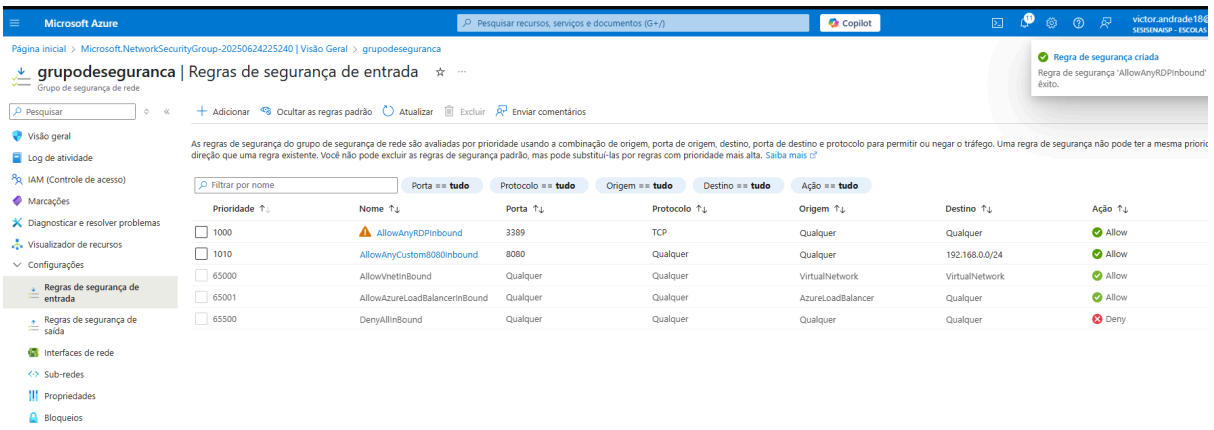


Inbound Rule - Liberando todo o tráfego com origem da rede azure, e liberando acesso via SSH para acessar á maquina da AWS

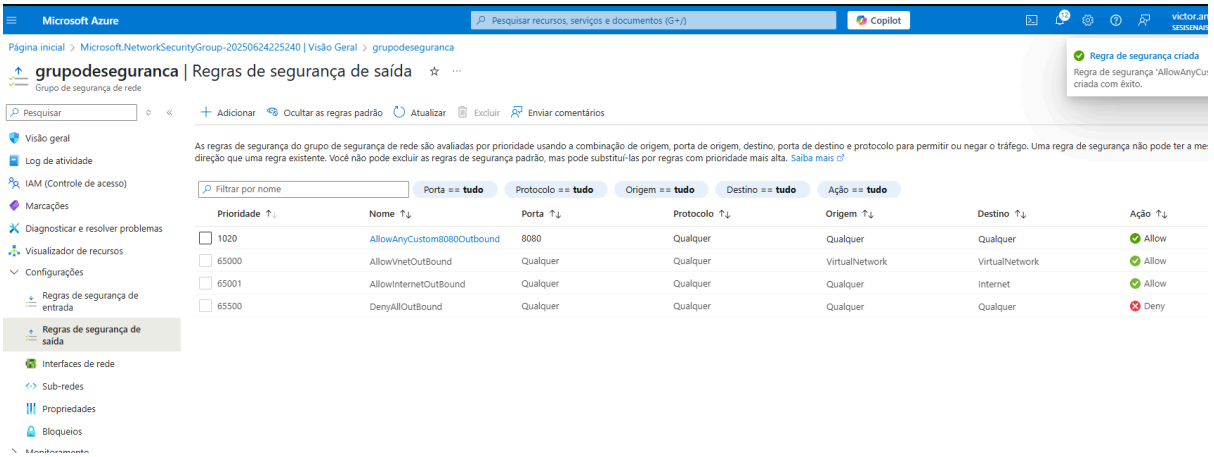


15) Security Group AZURE

Inbound Rule - Liberar todo tráfego para a AWS e liberar o RDP para acesso da máquina

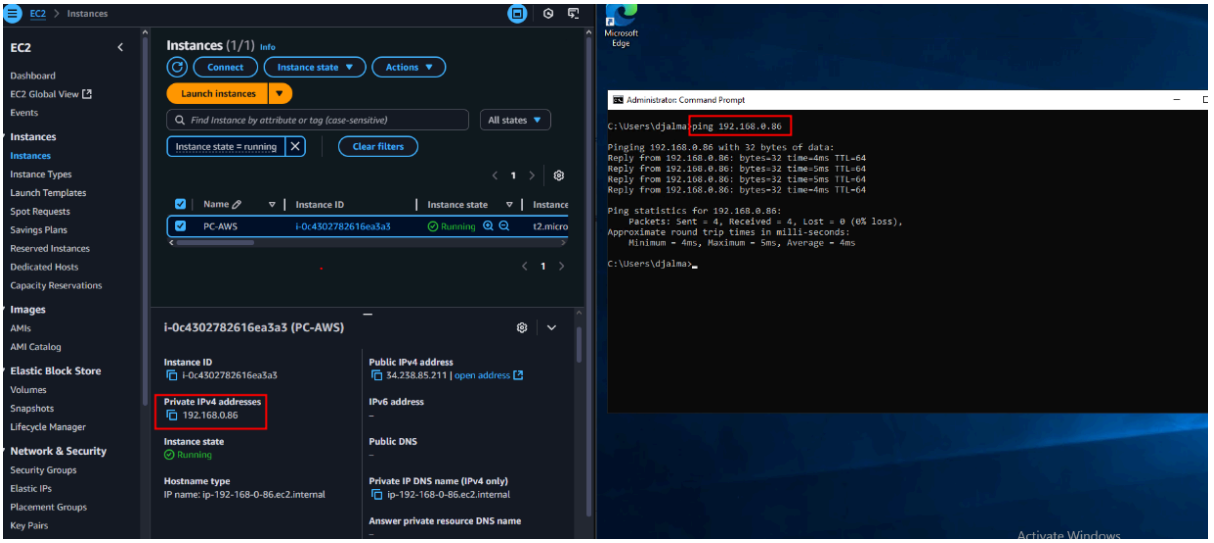


Outbound Rule - Liberar todo tráfego de saída



PING DE MÁQUINA- TESTE FINAL DA VPN ENTRE NUVENS

Máquina da Azure pingando máquina da AWS



Máquina da AWS pingando máquina da AZURE