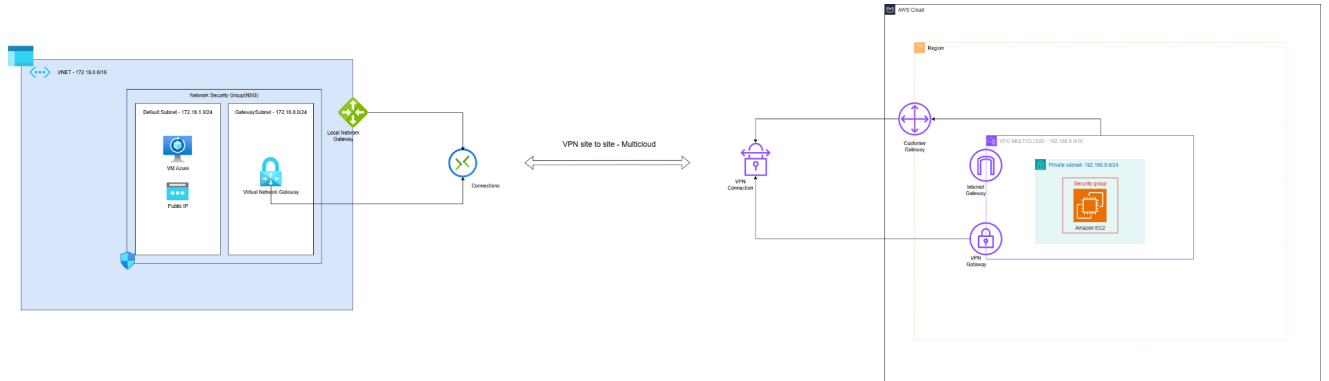


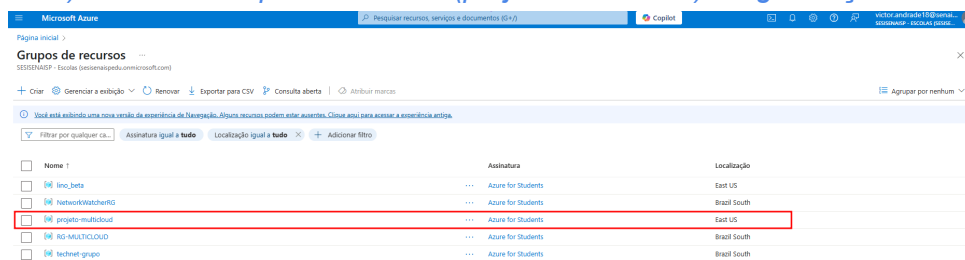
Multicloud AZURE x AWS

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

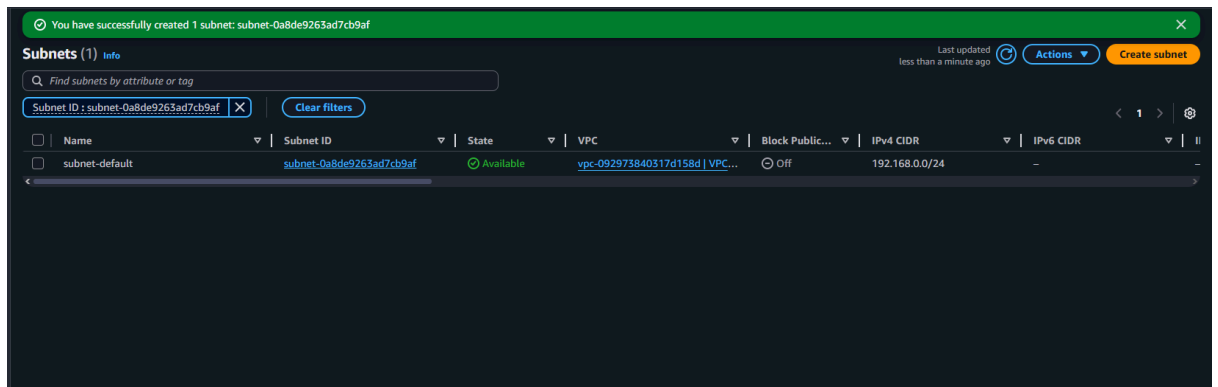
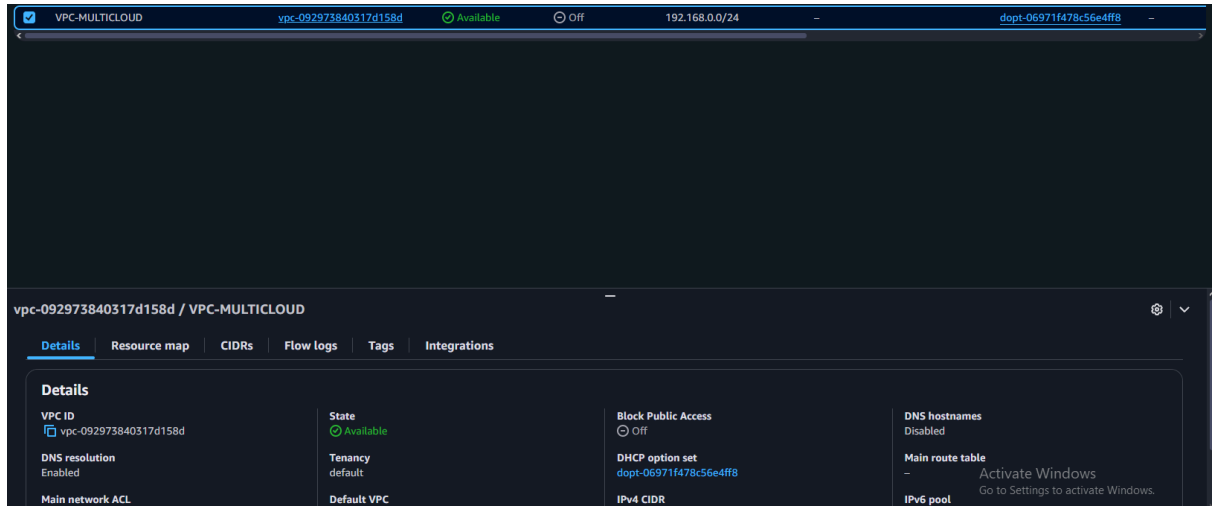
Assinatura	Azure for Students
Grupo de recursos	projeto-multicloud
Nome	VGN-multicloud
Região	East US
SKU	VpnGw1
Geração	Generation1
Rede virtual	VNET-MULTICLOUD
Sub-rede	GatewaySubnet (172.16.0.0/24)
Tipo de gateway	Vpn
Tipo de VPN	RouteBased
Habilitar o modo ativo-ativo	Desabilitado
Habilitar Conectividade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

Marcas

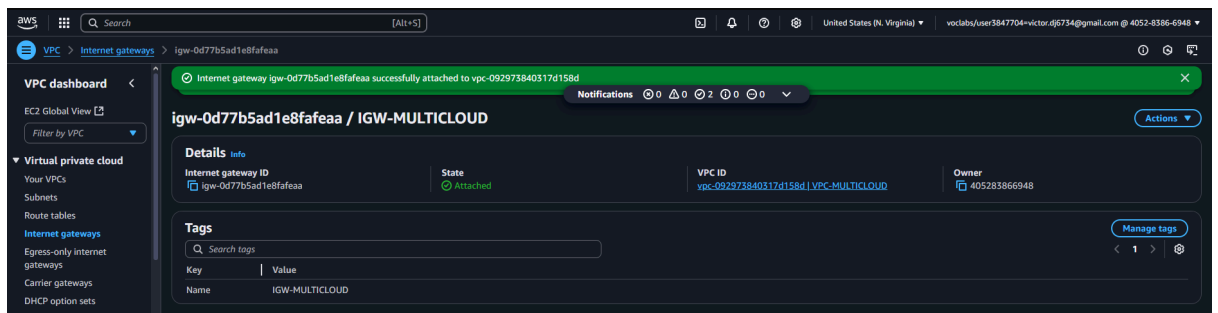
Nenhum

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

Edit routes

Destination	Target	Status	Propagated
192.168.0.0/24	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

[Add route](#) [Cancel](#) [Preview](#) [Save changes](#)

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
subnet-default	subnet-0a8de9263ad7cb9af	192.168.0.0/24	-	rtb-0eba5b6f6801a3e75 / RTB-MULTIC...

Selected subnets

subnet-0a8de9263ad7cb9af / subnet-default

[Cancel](#) [Save associations](#)

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 .

Create customer gateway

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.

Details

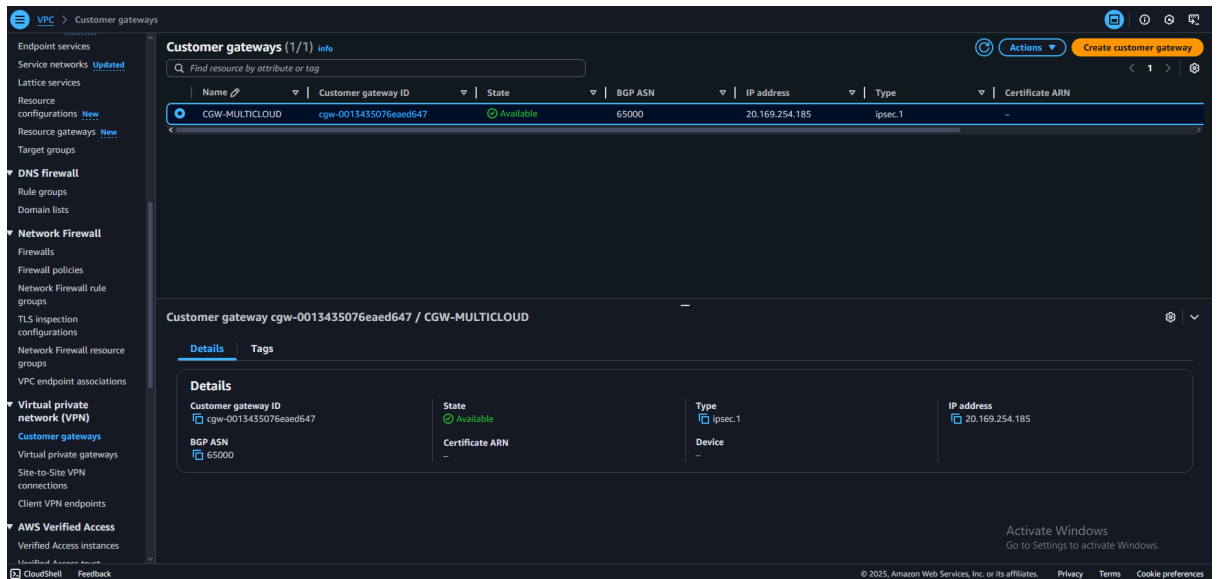
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
CGW-MULTICLOUD

BGP ASN - info
The ASN of your customer gateway device.
65000

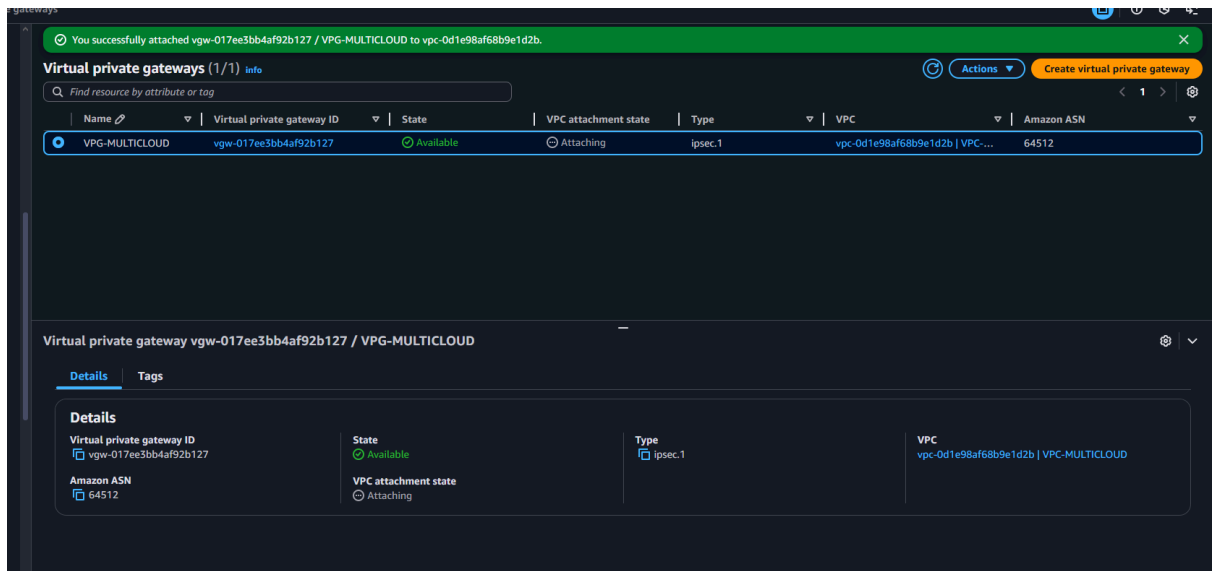
IP address - info
Specify the IP address for your customer gateway device's external interface.
20.169.254.185

Certificate ARN - optional
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).
Select certificate ARN

Device - optional
Enter a name for the customer gateway device.
Enter device name



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

Create VPN connection [Info](#)

Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

Details

Name tag - optional [Info](#)
Creates a tag with a key of 'Name' and a value that you specify.

Value must be 256 characters or less in length.

Target gateway type [Info](#)
☒ Virtual private gateway
☐ Transit gateway
☐ Not associated

Virtual private gateway

Customer gateway [Info](#)
☒ Existing
☐ New

Customer gateway ID

Routing options [Info](#)
☐ Dynamic (requires BGP)
☒ Static

Static IP prefixes [Info](#)

Pre-shared key storage [Info](#)
☒ Standard
☐ Secrets Manager

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback Privacy Terms Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.

10) Baixar o arquivo de configuração da VPN

- generic
- generic
- vendor
- agnostic
- ikev2

Download configuration ✕

Download a sample configuration based on your customer gateway. Note that this is a sample only, and that it will require modification for using Advanced Algorithms, Certificates, and IPv6.

Vendor
The manufacturer of the customer gateway device (for example, Cisco Systems, Inc.).

Generic ▾

Platform
The class of the customer gateway device (for example, J-Series).

Generic ▾

Software
The operating system running on the customer gateway device (for example, ScreenOS).

Vendor Agnostic ▾

IKE version
The IKE version you are using for your VPN connection.

ikev2 ▾

Include sample type - optional
☐ Enable

Sample type
The default sample type compatibility mode includes all options. The recommended mode restricts options to only the most secure settings (IKEv2, etc.).

Select sample type ▾

Cancel Download

vpn-0e7433000a41e6538.txt - Notepad

File Edit Format View Help

```
The Customer Gateway and Virtual Private Gateway each have two addresses that r
to this IPSec tunnel. Each contains an outside address, upon which encrypted
traffic is exchanged. Each also contain an inside address associated with
the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway
was created. Changing the IP address requires the creation of a new
Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel
interface.

Outside IP Addresses:
- Customer Gateway           : 20.169.254.185
- Virtual Private Gateway    : 44.212.142.34

Inside IP Addresses
- Customer Gateway           : 169.254.37.82/30
- Virtual Private Gateway    : 169.254.37.81/30

Configure your tunnel to fragment at the optimal size:
- Tunnel interface MTU      : 1436 bytes

#4: Static Routing Configuration:

To route traffic between your internal network and your VPC,
you will need a static route added to your router.
```

Ln 94, Col 39 100% Unix (LF) UTF-8

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

11) Criando Local network gateway(LNG)

Microsoft Azure | Pesquisar recursos, serviços e documentos (G+/I) | Copilot

Página inicial > Hybrid connectivity | Local network gateways >

Criar gateway de rede local

Básico | Avançado | Revisar + criar

Um gateway de rede local é um objeto específico que representa um local local(o site) para fins de roteamento. [Saiba mais](#)

Detalhes do projeto

Assinatura *

Grupo de recursos * [Criar novo](#)

Detalhes da instância

Região *

Nome *

Ponto de extremidade ☐ Endereço IP ☐ FQDN

Endereço IP *

Espaços de endereço ☐

[Incluir intervalo de endereços adicional](#)

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

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

Microsoft Azure | Pesquisar recursos, serviços e documentos (G+/I) | Copilot

Página inicial > VGN-multicloud | Conexões >

Criar conexão

Básico | Configurações | Marcas | Revisar + criar

Crie uma conexão segura para a rede virtual usando o Gateway de VPN ou o ExpressRoute. [Saiba mais sobre o Gateway de VPN](#) [Saiba mais sobre o ExpressRoute](#)

Detalhes do projeto

Assinatura *

Grupo de recursos * [Criar novo](#)

Detalhes da instância

Tipo de conexão *

Nome *

Região *

13) PSK : selecionar a PSK do primeiro tunel ,presente no arquivo de configuração e adicione 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 firewall
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        : ZHDKUEU2NyQxRXNFBuZDZ0q_qq1B179m9q
- 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
< >
```

Microsoft Azure | Pesquisar recursos, serviços e documentos (G+ /) | Copilot

Página inicial > VGN-multicloud | Conexões >

Criar conexão

Básico | **Configurações** | Marcas | Revisar + criar

Gateway de rede virtual

Para usar uma rede virtual com uma conexão, ela deve estar associada a um gateway de rede virtual.

Gateway de rede virtual *

Gateway de rede local *

Método de Autenticação ☒ Chave compartilhada (PSK) ☐ Certificado do Key Vault (versão prévia)

Chave compartilhada (PSK) *

Protocolo IKE ☐ IKEv1 ☒ IKEv2

Usar Endereço IP Privado do Azure ☐

Habilitar BGP ☐

Política IPsec/IKE ☒ Padrão ☐ Personalizado

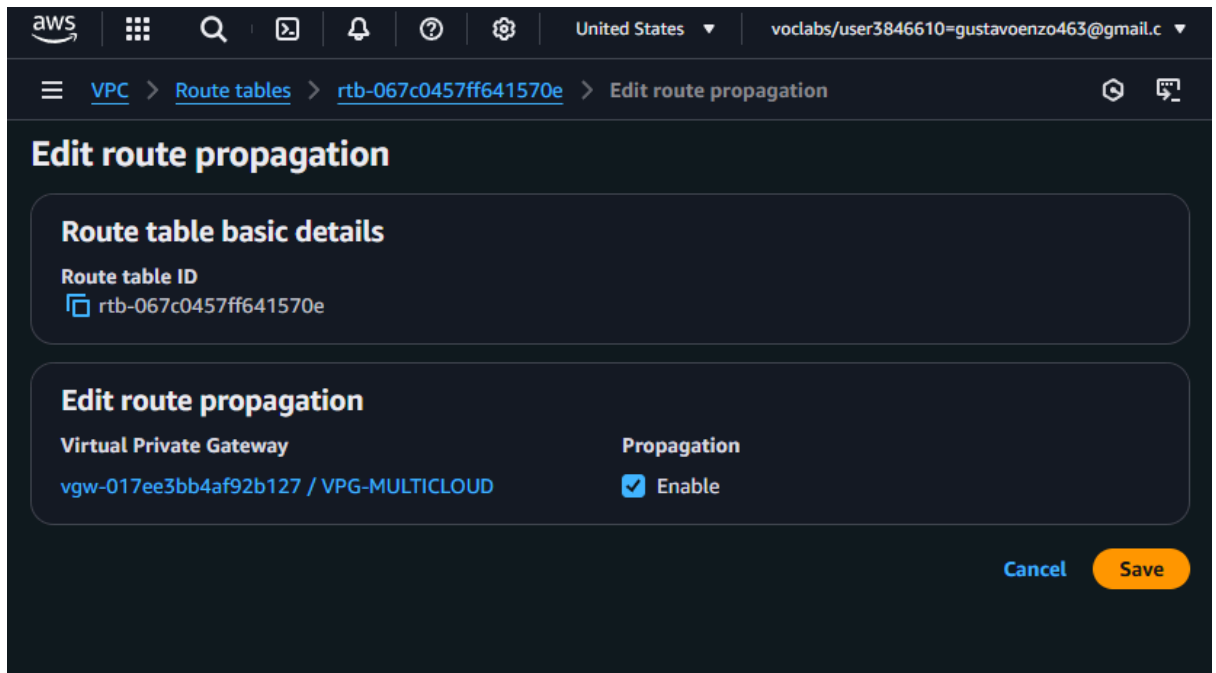
Usar seletor de tráfego baseado em política ☐ Habilitar ☒ Desabilitar

Tempo limite de DPD em segundos *

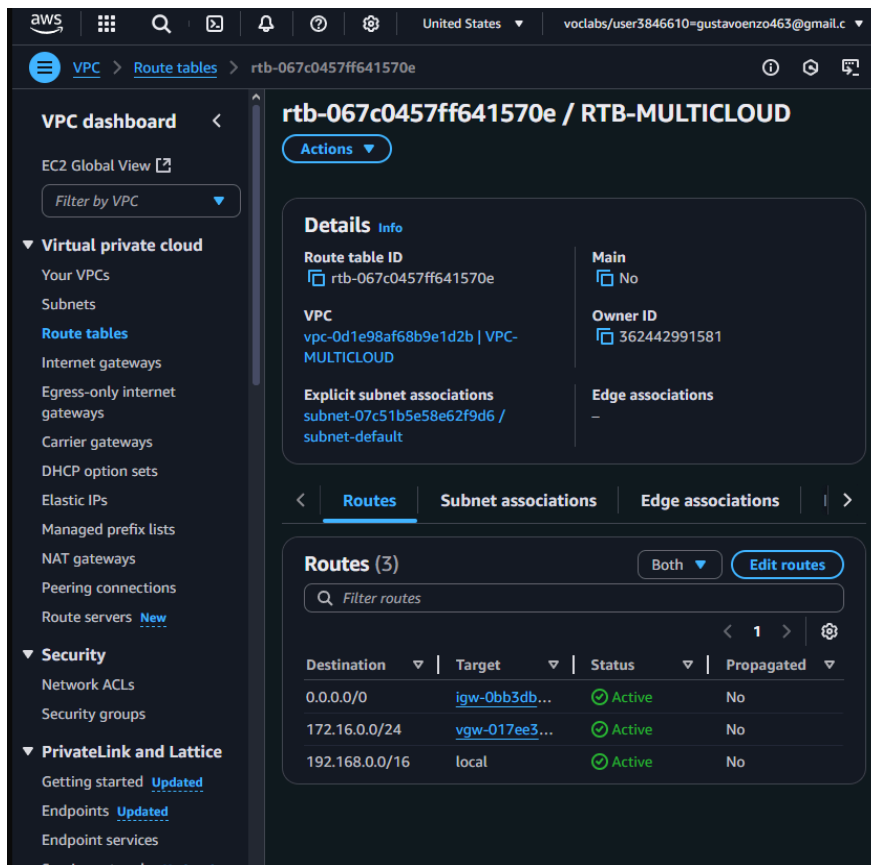
Modo de Conexão ☒ Default ☐ InitiatorOnly ☐ ResponderOnly

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 route propagation > enable)



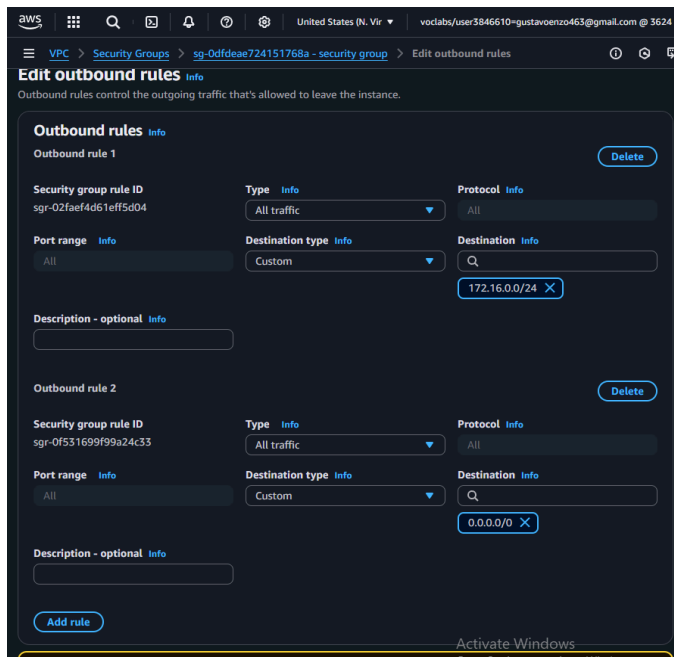
também é possível adicionar a rota manualmente : destination : rede da azure (no caso , 172.16.0.0/24) target : virtual private gateway



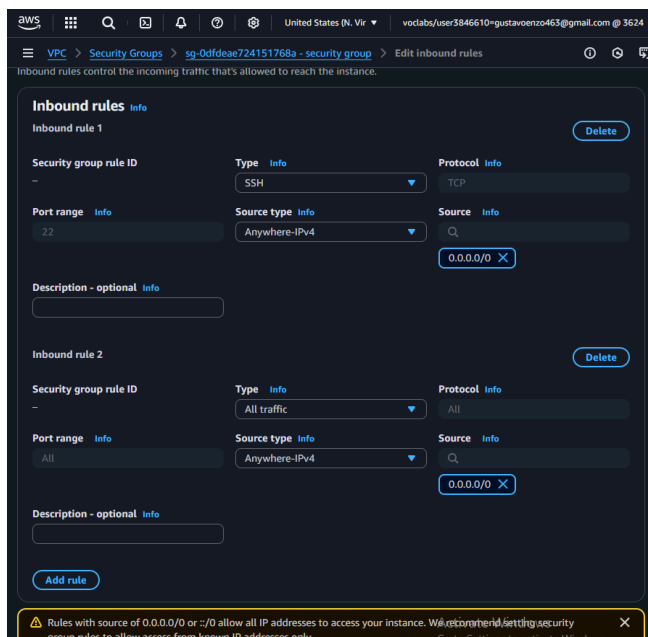
Validações finais e criação de instâncias Nesse ponto, ambos os tuneis de ambos os lados deveram estar conectados e estáveis Seguiremos estabelecendo regras de uma rede interna para outra —————> importante !!!

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

Microsoft Azure

Página inicial > Microsoft.NetworkSecurityGroup-2025062425240 | Visão Geral > grupodesequilíbrio

grupodesequilíbrio | Regras de segurança de entrada

Grupo de segurança de rede

Pesquisar Adicionar Ocultar as regras padrão Atualizar Excluir Enviar comentários

Visão geral Log de atividade IAM (Controle de acesso) Marcações Diagnosticar e resolver problemas Visualizador de recursos Configurações

Regras de segurança de entrada

Regras de segurança de saída Interfaces de rede Sub-redes Propriedades Bloqueios

As regras de segurança do grupo de segurança de rede são avaliadas por prioridade usando uma combinação de origem, porta de origem, destino, porta de destino e protocolo para permitir ou negar o tráfego. Uma regra de segurança não pode ter a mesma prioridade que uma regra existente. Você não pode excluir as regras de segurança padrão, mas pode substituí-las por regras com prioridade mais alta. Saiba mais

Prioridade ↑↓	Nome ↑↓	Porta ↑↓	Protocolo ↑↓	Origem ↑↓	Destino ↑↓	Ação ↑↓
1000	AllowAnyRDPEndbound	3389	TCP	Qualquer	Qualquer	Allow
1010	AllowAnyCustom8080Inbound	8080	Qualquer	Qualquer	192.168.0.0/24	Allow
65000	AllowVnetInBound	Qualquer	Qualquer	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Qualquer	Qualquer	AzureLoadBalancer	Qualquer	Allow
65500	DenyAllInBound	Qualquer	Qualquer	Qualquer	Qualquer	Deny

Outbound Rule - Liberar todo tráfico de saída

Microsoft Azure

Página inicial > Microsoft.NetworkSecurityGroup-20250624225240 | Visão Geral > grupodeseguranca

grupodeseguranca | Regras de segurança de saída

Grupo de segurança de rede

Pesquisar

+ Adicionar

Ocultar as regras padrão

Atualizar

Excluir

Enviar comentários

Visão geral

Log de atividade

IAM (Controle de acesso)

Marcações

Diagnosticar e resolver problemas

Visualizador de recursos

Configurações

Regras de segurança de entrada

Regras de segurança de saída

Interfaces de rede

Sub-redes

Propriedades

Bloqueios

Regra de segurança criada

Regra de segurança 'AllowAnyCus...
criada com êxito.

As regras de segurança do grupo de segurança de rede são avaliadas por prioridade usando a combinação de origem, porta de origem, destino, porta de destino e protocolo para permitir ou negar o tráfego. Uma regra de segurança não pode ter a mesma direção que uma regra existente. Você não pode excluir as regras de segurança padrão, mas pode substituí-las por regras com prioridade mais alta. [Saiba mais](#)

Filtrar por nome

Porta == tudo

Protocolo == tudo

Origem == tudo

Destino == tudo

Ação == tudo

Prioridade ↑↓	Nome ↑↓	Porta ↑↓	Protocolo ↑↓	Origem ↑↓	Destino ↑↓	Ação ↑↓
<input type="checkbox"/> 1020	AllowAnyCustom8080Outbound	8080	Qualquer	Qualquer	Qualquer	Allow
<input type="checkbox"/> 65000	AllowVnetOutBound	Qualquer	Qualquer	VirtualNetwork	VirtualNetwork	Allow
<input type="checkbox"/> 65001	AllowInternetOutBound	Qualquer	Qualquer	Qualquer	Internet	Allow
<input type="checkbox"/> 65500	DenyAllOutBound	Qualquer	Qualquer	Qualquer	Qualquer	Deny

PING DE MÁQUINA- TESTE FINAL DA VPN ENTRE NUVENS

Máquina da Azure pingando máquina da AWS

The screenshot displays the AWS Management Console on the left and a Windows Command Prompt on the right. In the console, the 'Instances' page shows a single instance named 'PC-AWS' with ID 'i-0c4302782616ea3a3', which is in the 'Running' state. The 'Private IPv4 addresses' section is highlighted, showing the address '192.168.0.86'. The Command Prompt shows the command 'ping 192.168.0.86' being executed, resulting in four successful replies from 192.168.0.86 with 32 bytes of data and a 4ms round trip time.

Máquina da AWS pingando máquina da AZURE

The screenshot displays the Azure portal on the left and a Windows Command Prompt on the right. In the portal, the 'PC-MULTICLOUD' virtual machine is shown with its network configuration. The 'Endereço IP privado' (Private IP address) is highlighted as '172.16.1.4'. The Command Prompt shows the command 'ping 172.16.1.4' being executed, resulting in nine successful replies from 172.16.1.4 with 64 bytes of data and a round trip time between 4.67 ms and 5.23 ms.