

1. Objetivo

Estabelecer uma VPN site-to-site entre Microsoft Azure e Amazon Web Services (AWS), permitindo comunicação entre máquinas virtuais em sub-redes privadas usando exclusivamente endereços IP privados.

2. Ambiente

- Rede Virtual Azure: 10.0.0.0/16
 - Sub-rede GatewaySubnet (Azure): 10.0.255.0/27
 - VPC AWS: 172.16.0.0/16
 - Sub-rede privada AWS: 172.16.1.0/24
-

3. Passo a passo da Configuração VPN Site-to-Site

3.1 Criar Rede Virtual e Sub-rede no Azure

- No portal Azure, crie uma Virtual Network com endereço 10.0.0.0/16.
- Crie a sub-rede obrigatória GatewaySubnet com o intervalo 10.0.255.0/27.

3.2 Criar VPN Gateway no Azure

- Configure o VPN Gateway na mesma região da VNet.
- Escolha tipo VPN, SKU conforme necessidade (exemplo: VpnGw1), VPN baseado em rota (Route-based).
- Aguarde a criação (tempo aproximado: 30 minutos).

3.3 Criar Gateway de Rede Local no Azure

- Defina o endereço IP público do VPN Gateway da AWS.

- Configure o espaço de endereço da rede AWS, `172.16.0.0/16`.

3.4 Criar Conexão VPN no Azure

- Configure a conexão site-to-site utilizando o Gateway de rede virtual e Gateway de rede local.
- Configure a chave pré-compartilhada (PSK), deve ser idêntica na AWS.

3.5 Criar VPC e Sub-rede na AWS

- No console AWS, crie uma VPC com CIDR `172.16.0.0/16`.
- Crie uma sub-rede privada na VPC, por exemplo, `172.16.1.0/24`.

3.6 Criar Virtual Private Gateway (VGW) na AWS

- Crie o VGW e associe à VPC.

3.7 Criar Customer Gateway (CGW) na AWS

- Defina o IP público do VPN Gateway do Azure.
- Configure o roteamento estático.

3.8 Criar VPN Connection na AWS

- Associe o CGW e VGW criados.
- Configure rotas estáticas apontando para a rede Azure (`10.0.0.0/16`).
- Configure a chave pré-compartilhada (igual ao Azure).

3.9 Configuração de Rotas e Security Groups

- Configure tabelas de rotas na AWS e no Azure para direcionar tráfego via VPN.
- Ajuste regras nos grupos de segurança para permitir ICMP, SSH e RDP entre as sub-redes.

3.10 Testes de Conectividade

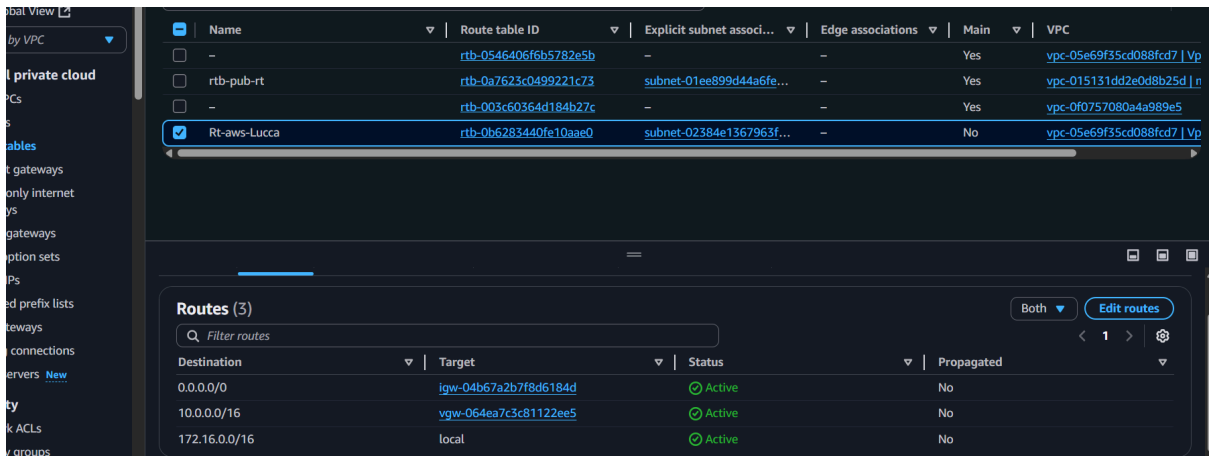
- Realize ping entre máquinas virtuais usando IP privado.
- Teste acesso via SSH ou RDP conforme o sistema operacional.

4. Tabela de Endereços IP e Sub-redes

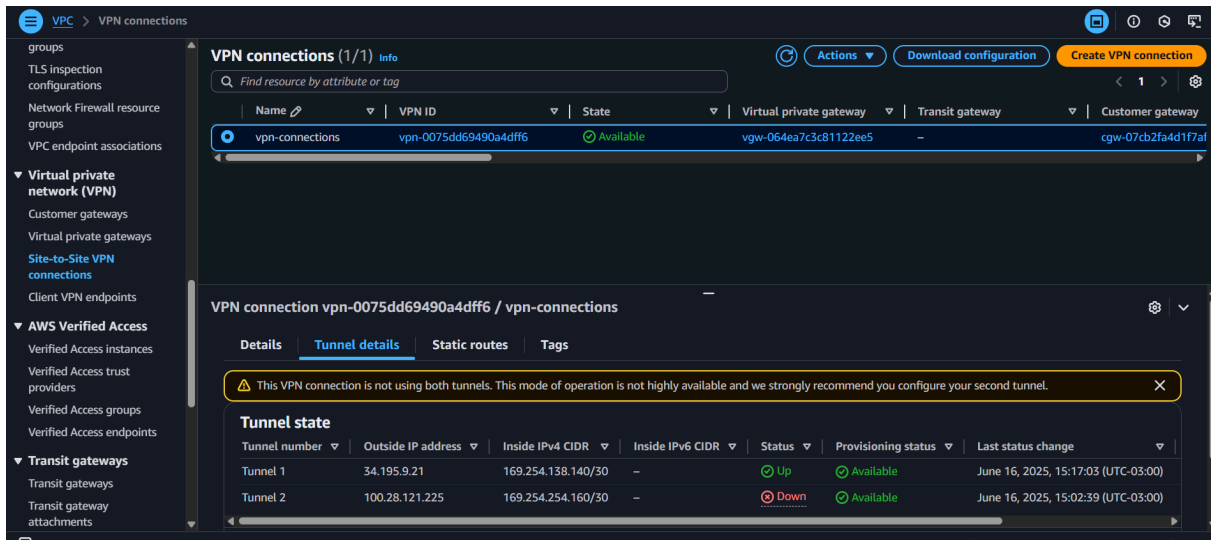
Recurso	Endereço IP / CIDR
Rede Virtual Azure	10.0.0.0/16
Sub-rede GatewaySubnet	10.0.255.0/27
VM Azure (exemplo)	10.0.1.5 (privado)
VPC AWS	172.16.0.0/16
Sub-rede AWS	172.16.1.0/24
VM AWS (exemplo)	172.16.1.208 (privado)

5. Prints e Evidências

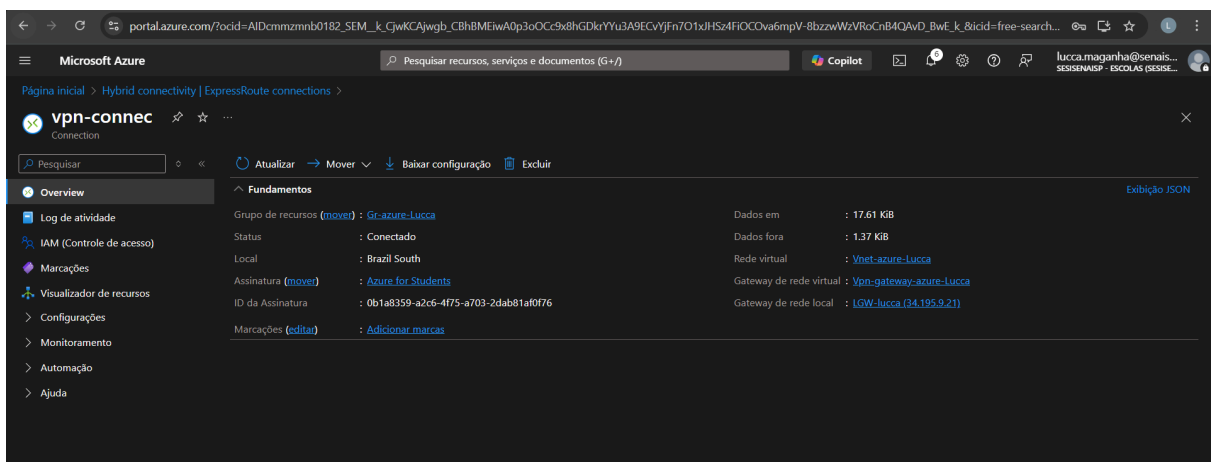
aws route table



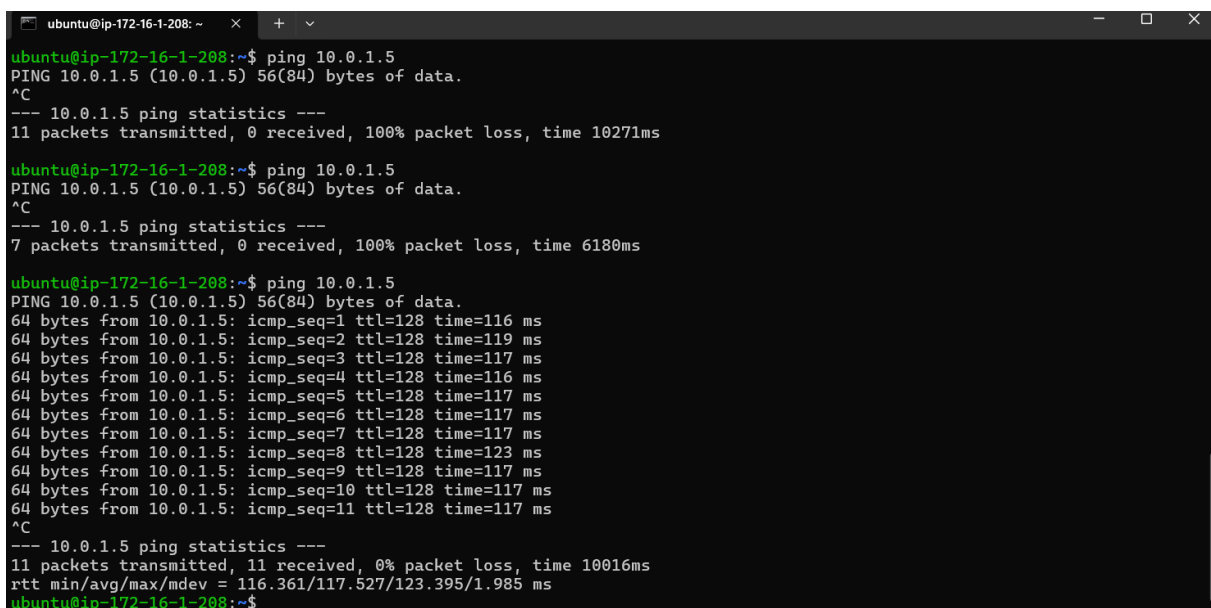
vpn connections tunnel 1 principal UP



vpn-connection da azure mostrando conectado



aws (ip privado- 172.16.1.208) pingando azure privado (10.0.1.5)



dentro do windows(azure) pingando aws

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.3807]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lucca>ping 172.16.1.208

Pinging 172.16.1.208 with 32 bytes of data:
Reply from 172.16.1.208: bytes=32 time=116ms TTL=64
Reply from 172.16.1.208: bytes=32 time=120ms TTL=64
Reply from 172.16.1.208: bytes=32 time=116ms TTL=64
Reply from 172.16.1.208: bytes=32 time=116ms TTL=64

Ping statistics for 172.16.1.208:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 116ms, Maximum = 120ms, Average = 117ms

C:\Users\lucca>
```

ips da instancia aws

instance-ec2-lucca

i-042b54ad5975926f8

Running

t2.micro

2/2 checks passed

View alarms

us-east-1a

i-042b54ad5975926f8 (instance-ec2-lucca)

DetailsStatus and alarmsMonitoringSecurityNetworkingStorageTags

▼ Instance summary Info

Instance ID

i-042b54ad5975926f8

IPv6 address

-

Public IPv4 address

44.204.40.75 | open address

Instance state

Running

Private IPv4 addresses

172.16.1.208

Public DNS

-

grupos de segurança e nsg

Todos os serviços > Grupos de segurança de rede >

Vm-azure-Lucca-nsg

Grupo de segurança de rede

Pesquisar

MoverExcluirAtualizarEnviar 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

Fundamentos

Grupo de recursos (move): Gr-azure-lucca

Local: Brazil South

Assinatura (move): Azure for Students

ID da Assinatura: 0b1a8359-a2c6-4f75-a703-2dab81a0f76

Marcações (editar): Adicionar marcas

Regras de segurança per...: 3 de entrada, 0 de saída

Associado a: 1 sub-redes, 2 interfaces de rede

Exibição JSON

Filtrar por nome

Porta == tudoProtocolo == tudoOrigem == tudoDestino == tudoAção == tudo

Prioridade	Nome	Porta	Protocolo	Origem	Destino	Ação
▼ Regras de Segurança de Entrada						
100	default-allow-ssh	22	TCP	0.0.0.0/0	Qualquer	Allow
1021	AllowAnyRDPInbound	3389	TCP	Qualquer	Qualquer	Allow
1031	AllowAnyCustomAnyInbound	Qualquer	ICMP	172.16.0.0/16	Qualquer	Allow
65000	AllowVnetInbound	Qualquer	Qualquer	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Qualquer	Qualquer	AzureLoadBalancer	Qualquer	Allow

<input checked="" type="checkbox"/>	-	sg-0f30de2e76ec557a6	default	vpc-05e69f35cd088fcd7	default VPC
<input type="checkbox"/>	-	sg-0e470e2e8548ab183	node-exporter-sg	vpc-015131dd2e0d8b25d	launch-wizard-2
<input type="checkbox"/>	-	sg-01ab10747e35bb2ea	launch-wizard-2	vpc-015131dd2e0d8b25d	launch-wizard-2

sg-0f30de2e76ec557a6 - default

Inbound rules (4)

Search

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-083658f4b09cee90b	IPv4	RDP	TCP	3389
<input type="checkbox"/>	-	sgr-0bedf460ac00e7d63	-	All traffic	All	All
<input type="checkbox"/>	-	sgr-01fbc17ea5a8bb5af	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-0d80c78bbc2ce65c6	IPv4	All ICMP - IPv4	ICMP	All

ips da vm azure

Microsoft Azure

Todos os serviços > Infraestrutura de computação | Máquinas virtuais >

vm-azure-lucca

Máquina virtual

Pesquisar

Assistente (1 de 3): Use Azure Capacity Reservation for virtual machine (VM) →

Ajude-me a copiar essa VM em qualquer região

Conectar Iniciar Reiniciar Parar Hibernar Capturar Excluir Atualizar Abrir no celular Comentários CLI / PS

Local : Brazil South

Assinatura (move) : Azure for Students

ID da Assinatura : 0b1a8359-a2c6-4f75-a703-2dab81af076

Endereço IP público : 4.201.200.56

Rede virtual/sub-rede : Vnet-azure-Lucca/Subnet-priv-azure-Lucca

Nome DNS : Não configurado

Estado de integridade : -

Horário criado : 16/06/2025, 18:55 UTC

Marcações (edita) : Adicionar marcas

Propriedades Monitoramento Funcionalidades (8) Recomendações (3) Tutoriais

Máquina virtual

Nome do computador : vm-azure-lucca

Sistema operacional : Windows (Windows Server 2022 Datacenter Azure Edition)

Geração de VM : V2

Arquitetura de VM : x64

Status do agente : Ready

Versão do agente : 2.7.41491.1149

Rede

Endereço IP público : 4.201.200.56 (Interface de rede vm-azure-lucca111)

Endereço IP público (IPv6) : -

Endereço IP privado : 10.0.1.5

Endereço IP privado (IPv6) : -

Rede virtual/sub-rede : Vnet-azure-Lucca/Subnet-priv-azure-Lucca

Nome DNS : Configurar