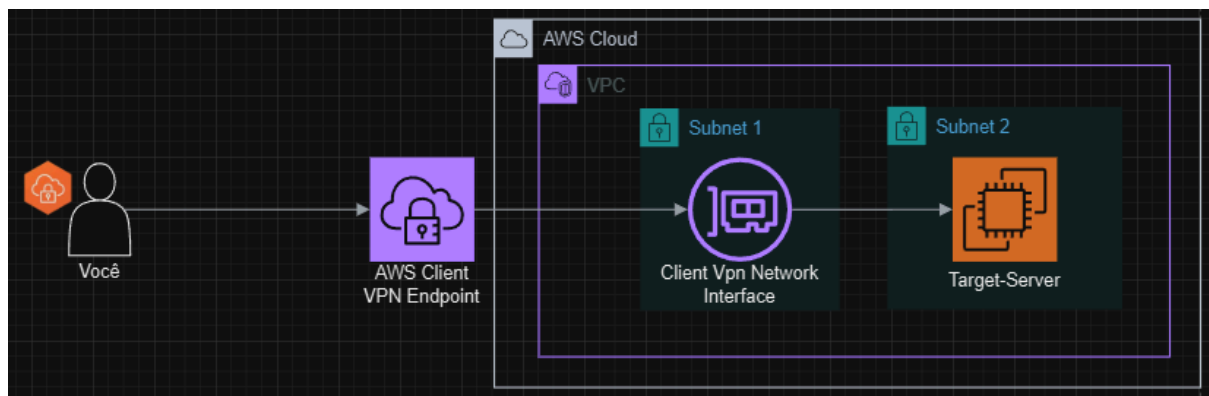


## AWS VPN: Conectividade Segura com a Nuvem

O **AWS VPN** oferece soluções seguras para conectar redes locais, escritórios remotos e dispositivos à infraestrutura global da AWS. Ele inclui dois serviços principais:

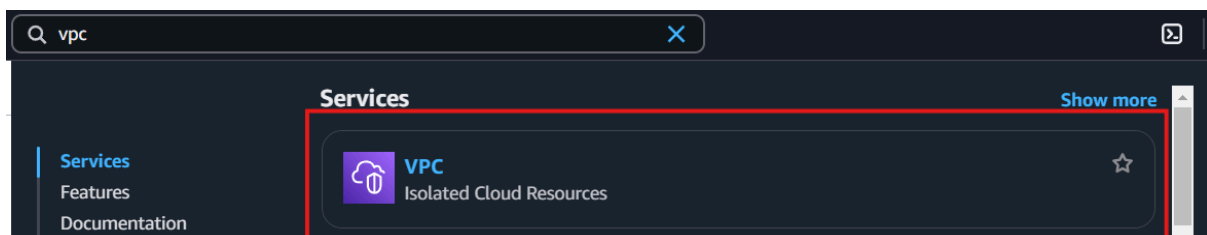
- **AWS Site-to-Site VPN:** ideal para conexões seguras entre redes locais e a AWS.
- **AWS Client VPN:** permite que usuários se conectem a recursos na AWS ou on-premises usando um cliente de software VPN.

Essas soluções são gerenciadas, altamente disponíveis e escaláveis, garantindo segurança e simplicidade no tráfego de rede.



### Configurando uma VPC para a VPN.

Para criar uma VPN Client na AWS, você precisa configurar uma **Virtual Private Cloud (VPC)**. Siga as etapas abaixo:



Agora dentro do console da VPC vamos criar uma rede virtual para servir de acesso para nossa VPN.

Your VPCs (1) <a href="#">Info</a>							
<div> <div>Search</div> <div> <div>Last updated 1 minute ago</div> <div>Actions</div> <div>Create VPC</div> </div> </div>							
<input type="checkbox"/>	Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option
<input type="checkbox"/>	-	<a href="#">vpc-02311a76cae395b91</a>	Available	Off	172.31.0.0/16	-	<a href="#">dopt-0d9f86t</a>

Dentro do console clique **Create VPC** e deixe selecionado como **VPC only**, agora dentro da parte do VPC settings colocar:

- **Nome:** vpc\_vpn
- **IPv4 Cidr:** 10.1.0.0/16

### VPC settings

Resources to create [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only
 ☐ VPC and more

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

[vpc\\_vpn](#)

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.1.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block  
☐ IPAM-allocated IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block  
☐ IPv6 CIDR owned by me

Com isso, temos que criar duas subnets para utilizar no ambiente, ainda dentro do console em baixo de **Suas VPCs** e clicar em **Subnets**.

VPC dashboard ×

EC2 Global View [↗](#)

Filter by VPC ▼

Virtual private cloud

Your VPCs  
**Subnets**  
 Route tables

Dentro do console clique **Create Subnet**, agora dentro do **VPC ID** selecionar a **VPC** criada anteriormente, e em subnet configurar ela assim:

- **Nome:** Subnet01
- **IPv4 Cidr:** 10.1.1.0/24
- **Availability Zone:** us-east-1a

#### Subnet 1 of 2

##### Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

##### Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

##### IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

##### IPv4 subnet CIDR block

256 IPs

##### ▼ Tags - optional

Key

Value - optional



Remove

Add new tag

You can add 49 more tags.

Remove

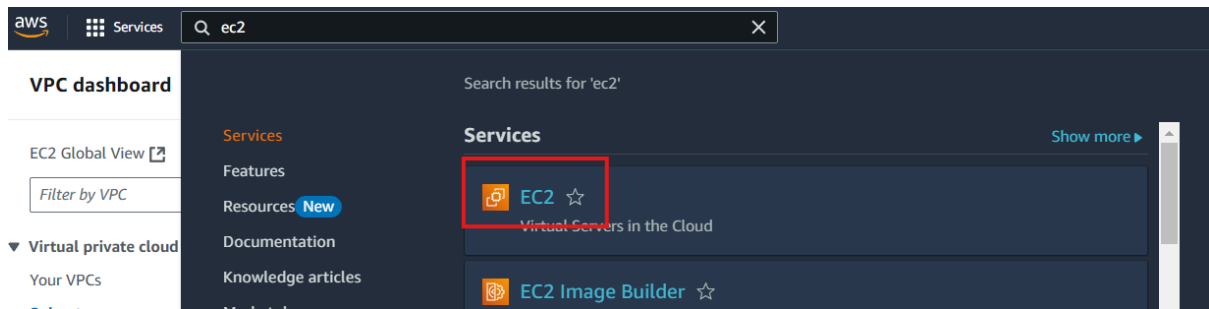
Repita esse processo para uma outra Subnet:

- **Nome:** Subnet02
- **IPv4 Cidr:** 10.1.2.0/24
- **Availability Zone:** us-east-1b

Agora no total temos uma VPC já configurada e duas Subnets em duas zonas diferentes.

## Configurando a EC2 Target-Server.

No console da AWS procure por EC2 e clique nela.



Já dentro do console procure por Instâncias e clique em **Executar instâncias**, já dentro da configuração siga os passos abaixo:

- **Nome:** TargetServerVPN
- **Imagem:** Amazon Linux 2023
- **Tipo de instância:** t2.micro

### Nome e tags [Informações](#)

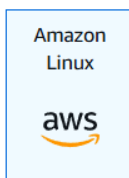
Nome

[Adicionar mais tags](#)

### ▼ Imagens de aplicação e de sistema operacional (imagem de máquina da Amazon)

[Informações](#)

Uma AMI é um modelo que contém a configuração do software (sistema operacional, servidor de aplicações e aplicações) necessária para executar a instância. Pesquise ou navegue pelas AMIs se você não estiver vendo o que está buscando abaixo

[Minhas AMIs](#)[Início rápido](#)

macOS



Ubuntu



Windows



Red Hat



SUSE Linux



[Procurar mais AMIs](#)

Incluindo AMIs da AWS, do Marketplace e da comunidade

### Imagem de máquina da Amazon (AMI)

Amazon Linux 2023 AMI

ami-0453ec754f44f9a4a (64 bits (x86), uefi-preferred) / ami-0ed83e7a78a23014e (64 bits (Arm), uefi)

Virtualização: hvm ENA habilitado: true Tipo de dispositivo raiz: ebs

Qualificado para o nível gratuito



Em Par de chaves crie uma para sua instância.

▼ **Par de chaves (login)** [Informações](#)

Você pode usar um par de chaves para se conectar com segurança à sua instância. Certifique-se de ter acesso ao par de chaves selecionado antes de executar a instância.

Nome do par de chaves - *obrigatório*

Selecionar



[Criar novo par de chaves](#)

Na parte da configuração da chave, coloque:

- **Nome:** pairkey
- **Tipo da chave:** .pem

Na parte de Configurações de rede selecionar a vpc criar anteriormente e a Subnet02.

▼ **Configurações de rede** [Informações](#)

VPC - *obrigatório* | [Informações](#)

vpc-04024ccb5cfed6c67 (vpc\_vpn)  
10.1.0.0/16



Sub-rede | [Informações](#)

subnet-098a328afbce979e6 Subnet02  
VPC: vpc-04024ccb5cfed6c67 Proprietário: 058264191091  
Zona de disponibilidade: us-east-1b Tipo de zona: Zona de disponibilidade  
Endereços IP disponíveis: 251 CIDR: 10.1.2.0/24



[Criar nova sub-rede](#) [↗](#)

Atribuir IP público automaticamente | [Informações](#)

Desabilitar

Na configuração do SG coloque **Criar grupo de segurança** e coloque as seguintes configurações:

- **Nome:** vpn-sg
- **Descrição:** Habilitando SSH e ICMP
- **Regras:** SSH e ICMP

#### Firewall (grupos de segurança) | [Informações](#)

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

☒ Criar grupo de segurança

☐ Selecionar grupo de segurança existente

Nome do grupo de segurança - *obrigatório*

vpn-sg

Esse grupo de segurança será adicionado a todas as interfaces de rede. Não é possível editar o nome após a criação do grupo de segurança. O comprimento máximo é de 255 caracteres. Os caracteres válidos são: a-z, A-Z, 0-9, espaços e .\_-:/()#,@[]+=&;{}!\$\*

Descrição - *obrigatório* | [Informações](#)

Habilitando SSH e ICMP

Tipo | [Informações](#)

ssh ▼

Protocolo | [Informações](#)

TCP

Intervalo de portas | [Informações](#)

22

Tipo de origem | [Informações](#)

Qualquer lugar ▼

Origem | [Informações](#)

🔍 Adicionar CIDR, lista de prefixos c

0.0.0.0/0 ✕

Descrição (*opcional*) | [Informações](#)

p. ex. SSH para a área de trabalho do

▼ Regra de grupo de segurança 2 (ICMP, Todos, 0.0.0.0/0)

Remover

Tipo | [Informações](#)

Todos os ICMPs - IPv4 ▼

Protocolo | [Informações](#)

ICMP

Intervalo de portas | [Informações](#)

Todos

Tipo de origem | [Informações](#)

Qualquer lugar ▼

Origem | [Informações](#)

🔍 Adicionar CIDR, lista de prefixos c

0.0.0.0/0 ✕

Descrição (*opcional*) | [Informações](#)

p. ex. SSH para a área de trabalho do

E clique em executar as instâncias.

▼ Configurar armazenamento Informações

Avançado

1x  GiB  Volume raiz (Criptografado)

Os clientes qualificados para o nível gratuito podem obter até 30 GB de armazenamento de uso geral (SSD) ou armazenamento magnético do EBS

Adicionar novo volume

Clique em atualizar para visualizar as informações de backup

As tags que você atribui determinam se o backup da instância será feito por alguma política do Data Lifecycle Manager.

0 x Sistemas de arquivos

Editar

► Detalhes avançados Informações

Firewall (grupo de segurança)

Novo grupo de segurança

Armazenamento (volumes)

1 volume(s) - 8 GiB

Nível gratuito: No primeiro ano, inclui 750 horas de uso de instâncias t2.micro (ou t3.micro nas regiões em que o t2.micro está indisponível) em AMIs de nível gratuito por mês, 750 horas de uso de endereço IPv4 público por mês, 30 GiB de armazenamento do EBS, 2 milhões de E/S, 1 GB de snapshots e 100 GB de largura de banda para a Internet.

Cancelar

Executar instância

Visualizar código

## Certificados



Agora vamos precisar de um certificado para o cliente e um para o server que vamos ter que usar para criar nossa vpn.

New Contributors

@NathanBaulch made their first contribution in #1169









Full Changelog: [v3.2.0...v3.2.1](#)



Contributors



NathanBaulch and TinCanTech

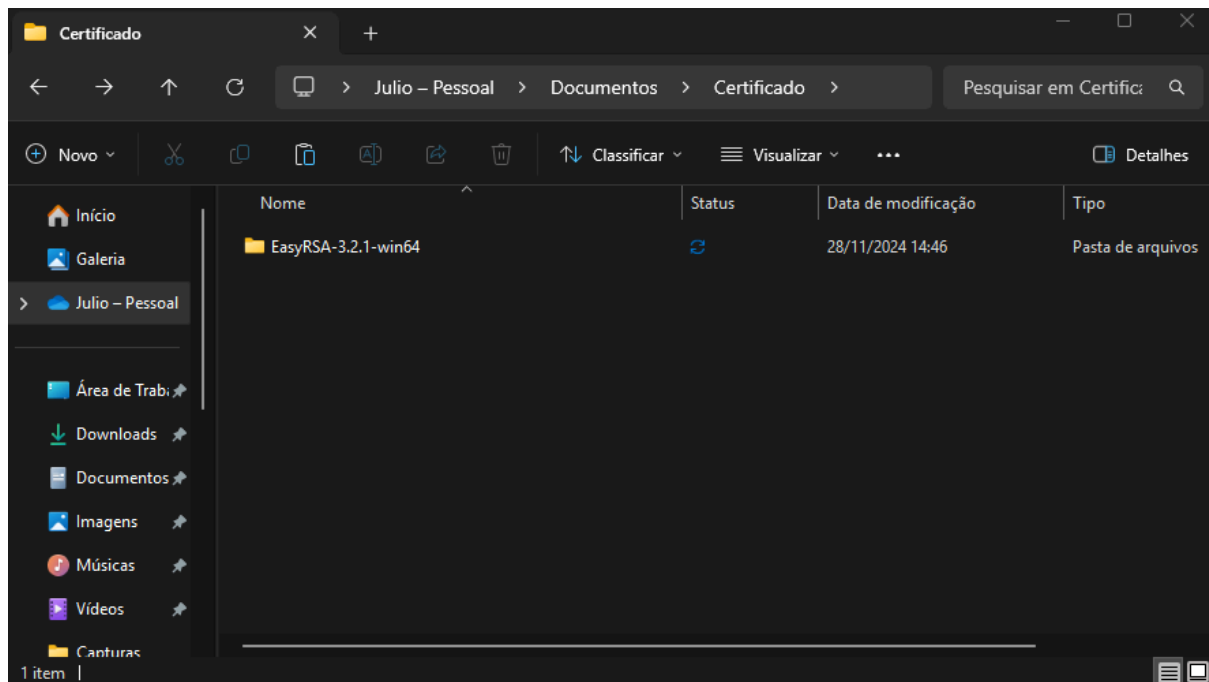
▼ Assets 8

 EasyRSA-3.2.1-win32.zip	3.55 MB	Sep 13
 EasyRSA-3.2.1-win32.zip.sig	310 Bytes	Sep 13
 EasyRSA-3.2.1-win64.zip	3.85 MB	Sep 13
 EasyRSA-3.2.1-win64.zip.sig	310 Bytes	Sep 13
 EasyRSA-3.2.1.tgz	78 KB	Sep 13
 EasyRSA-3.2.1.tgz.sig	310 Bytes	Sep 13
 Source code (zip)		Sep 5
 Source code (tar.gz)		Sep 5



6 people reacted

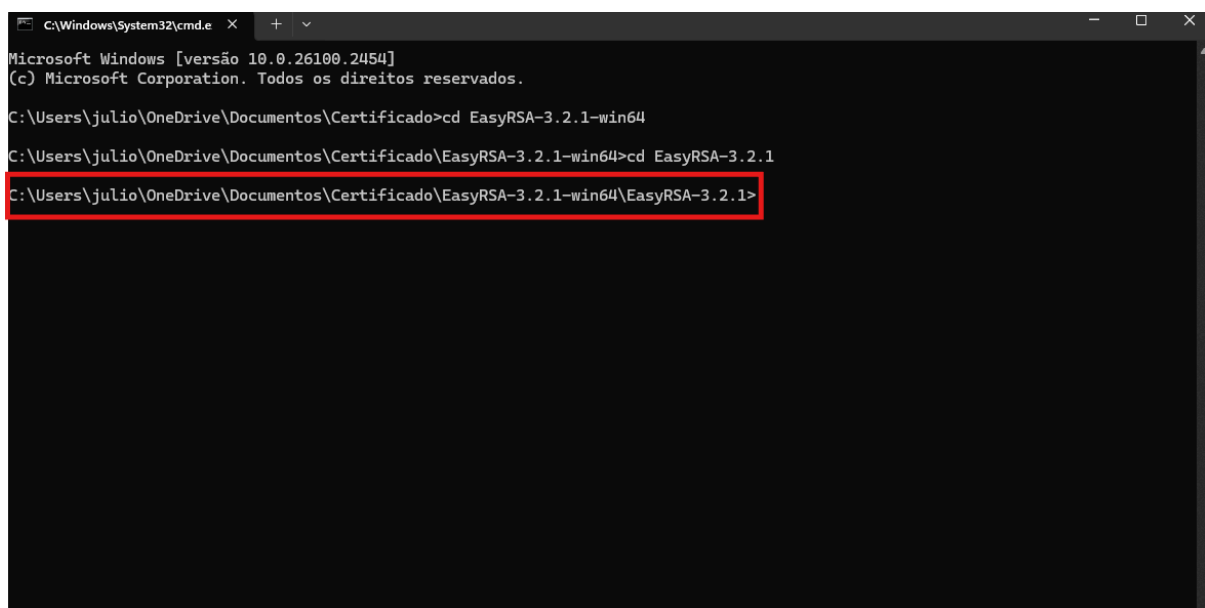
Com isso precisamos criar uma pasta localmente para servir de armazenamento para nosso certificado e precisamos colocar o arquivo já **extraído** da instalação do nosso certificado.



agora com o arquivo da rsa precisamos executar esse arquivo vamos seguir esse caminho para achar o arquivo. ( no meu caso foi:

**C:\Users\Julio\OneDrive\Documentos\Certificado\EasyRSA-3.2.1-win64\EasyRSA-3.2.1.)**

Mas fique livre para criar uma pasta da sua escolha em qualquer lugar, a única coisa importante é ter o arquivo EasyRSA descompactado dentro dessa pasta.





Com isso agora podemos executar o arquivo a seguir segue o comando para executar o arquivo dentro da pasta:

`.\EasyRSA-Start.bat`

Com isso agora já dentro do software precisamos colocar esse comando para iniciar nosso software:

`./easyrsa init-pki`

```
C:\Users\julio\OneDrive\Documentos\Certificado\EasyRSA-3.2.1-win64\EasyRSA-3.2.1> .\EasyRSA-Start.bat
Easy-RSA starting..

Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke 'easyrsa' to call the program. Without commands, help is displayed.

Using directory: C:/Users/julio/OneDrive/Documentos/Certificado/EasyRSA-3.2.1-win64/EasyRSA-3.2.1

EasyRSA Shell
# ./easyrsa init-pki

Notice
-----
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* C:/Users/julio/OneDrive/Documentos/Certificado/EasyRSA-3.2.1-win64/EasyRSA-3.2.1/pki

Using Easy-RSA configuration:
* undefined

EasyRSA Shell
#
```

Agora gerando a rsa:

`./easyrsa build-ca nopass`

Na parte do Common Name podemos seguir deixando ele em branco mesmo.

## Notice

```
* C:/Users/julio/Documents/Certificate/EasyRSA-3.2.1/pki/ca.crt
```

```
Build-ca completed successfully.
```

#

```
Using directory: C:/Users/julio/OneDrive/Documentos/Certificado/EasyRSA-3.2.1-win64/EasyRSA-3.2.1
```

```
# ./easysrsa build-server-full server nopass
```

## Notice

```
Private-Key and Public-Certificate-Request files created.
```

Your files are:

```
* req: C:/Users/julio/OneDrive/Documentos/Certificado/EasyRSA-3.2.1-win64/EasyRSA-3.2.1/pki/reqs/server.req
```

```
* key: C:/Users/julio/OneDrive/Documentos/Certificado/EasyRSA-3.2.1-win64/EasyRSA-3.2.1/pki/private/server.key
```

You are about to sign the following certificate:

```
Requested CN:      'server'
```

```
Requested type: 'server'
```

Valid for: '825' days

subject=

```
commonName = server
```

```
Type the word 'yes' to continue, or any other input to abort.
```

Confirm requested details: yes

Continuando para o último comando:

```
./easysrsa build-client-full client1.domain.tld nopass
```

No prompt colocar **yes**.

[illegible]

## Comandos:

.\EasyRSA-Start.bat

```
./easysrsa init-pki
```

```
./easyrsa build-ca nopass
```

```
./easysrsa --san=DNS:server build-server-full server nopass
```

```
./easysrsa build-client-full client1.domain.tld nopass
```

exit

Agora dentro o diretório podemos colocar esses comandos para organização dos nossos certificados:

### Comandos:

```
mkdir vpncert
```

```
copy pki\ca.crt vpncert
```

```
copy pki\issued\server.crt vpncert
```

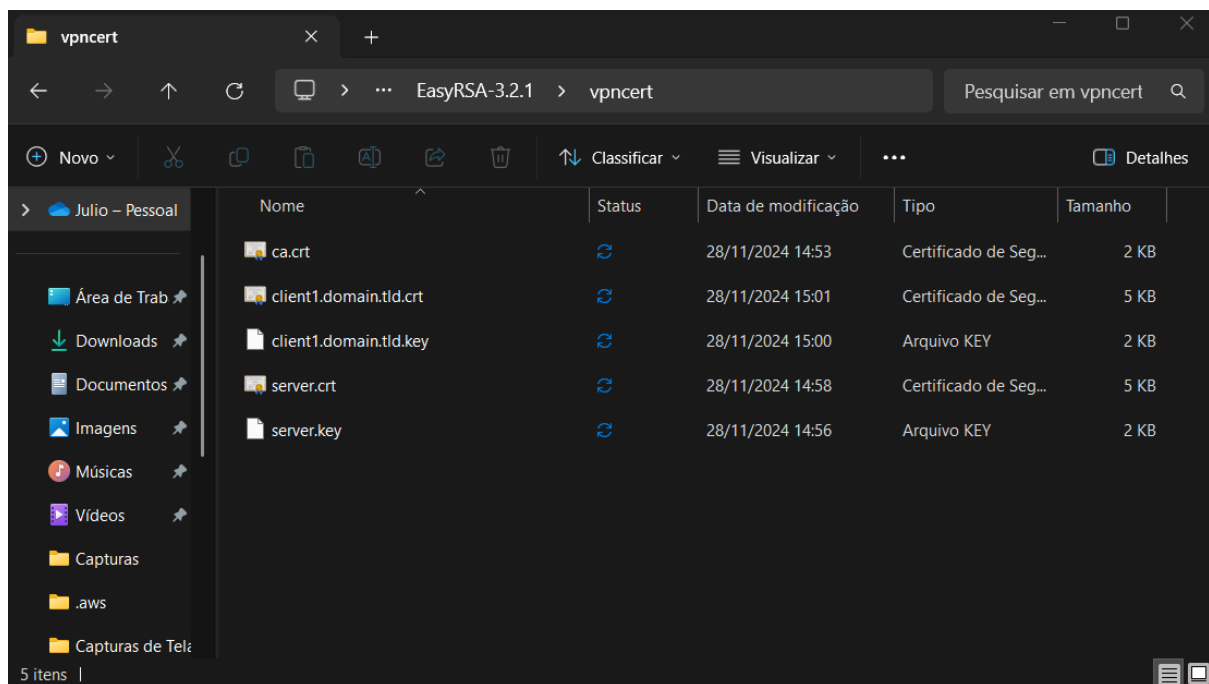
```
copy pki\private\server.key vpncert
```

```
copy pki\issued\client1.domain.tld.crt vpncert
```

```
copy pki\private\client1.domain.tld.key vpncert
```

```
cd vpncert
```

Agora dentro da pasta podemos ver nossos certificados que usaremos dentro da nossa vpn.



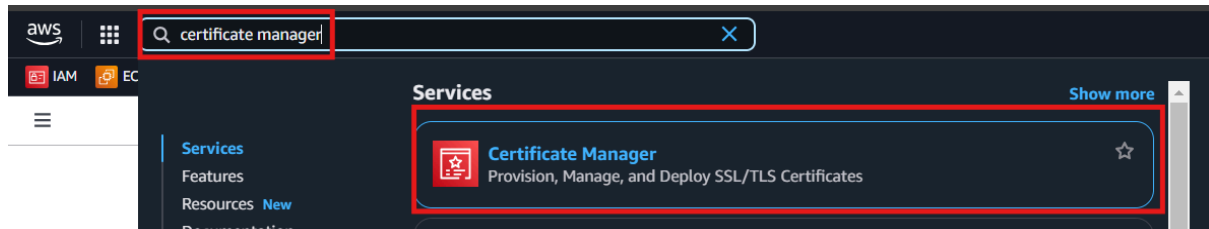
Voltando para dentro da aws precisamos utilizar o certificate manager para importar esse certificado, na aba da aws precisamos procurar pelo certificate manager.

obs: podemos também importar os certificados pela aws cli ficando bem mais fácil, só iremos precisar que a aws cli esteja configurada e conectada a sua aws.

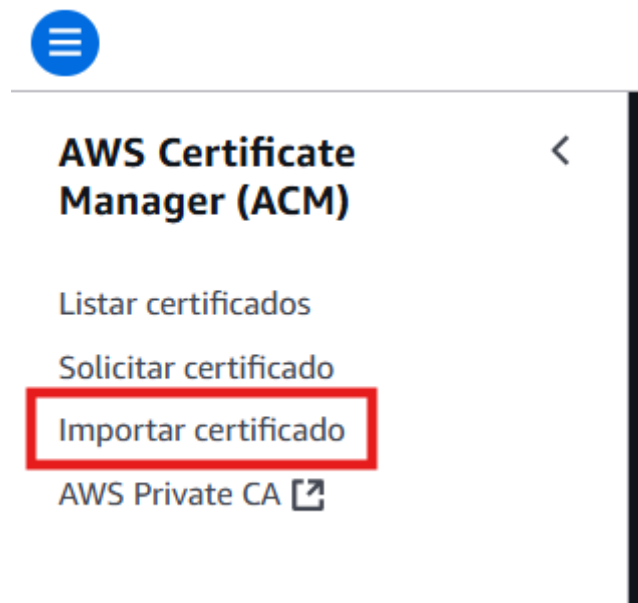
## Comandos:

```
aws acm import-certificate --certificate fileb://server.crt --private-key fileb://server.key  
--certificate-chain fileb://ca.crt
```

```
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-key  
fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```



agora já dentro do acm vamos importar nosso certificado



Agora dentro da pasta vpncert pegar o conteúdo dos arquivos **ca.cert** e colocar na cadeia de certificados.

## Importar certificado

### Detalhes do certificado [Informações](#)

#### Corpo do certificado

Cole o corpo do certificado codificado por PEM abaixo.

#### Chave privada do certificado

Cole a chave privada do certificado codificado por PEM abaixo.

#### Cadeia de certificados - *opcional* [Informações](#)

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAISgAwIBAgIUOTyMELvTf4ki7mDwCqm/zOAiQUwwDQYJKoZIhvcNAQEL
BQAwETEPMA0GA1UEAwGc2VydmlVYMB4XDTI0MTEyODE3NTM1N1oxDTM0MTEyNjE3
NTM1N1owETEPMA0GA1UEAwGc2VydmlVYMB4XDTI0MTEyODE3NTM1N1oxDTM0MTEyNjE3
MIIBCAQCAQEAAlvXOq72ZDe7jxw/WjZGgb9/nJHgk7mBOAEHvqN33wTFYjXKmYu
qkY86ohSpHrm4ac3zFNRkWW57e/N/ZfKrGyc42vmnaHr9yZc7xlr/qCdKHu3uunV
b8YF1FLXvrhYh6GGE1TTQ7Hz4ZXE42NrwJQGY+IC68YFTzXzkMYthDOoaM8AeEOd
oAE7IADHMeLo4butMTb5v8Aa/biFE3CaoudEM8uYOMOTiiQYIINBECF3uoCEKsEW/
```

Agora precisamos pegar o **server.cert** e precisamos colocar ele dentro do corpo do certificado.

### Detalhes do certificado [Informações](#)

#### Corpo do certificado

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
9caabbbf1c1d4bca9:43:ef9f:fe:fc:ae:83:a6  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: CN=server  
Validity  
Not Before: Nov 28 17:58:40 2024 GMT  
Not After : Mar 3 17:58:40 2027 GMT  
Subject: CN=server  
Subject Public Key Info:

#### Chave privada do certificado

Cole a chave privada do certificado codificado por PEM abaixo.

#### Cadeia de certificados - *opcional* [Informações](#)

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAISgAwIBAgIUOTyMELvTf4ki7mDwCqm/zOAiQUwwDQYJKoZIhvcNAQEL
BQAwETEPMA0GA1UEAwGc2VydmlVYMB4XDTI0MTEyODE3NTM1N1oxDTM0MTEyNjE3
NTM1N1owETEPMA0GA1UEAwGc2VydmlVYMB4XDTI0MTEyODE3NTM1N1oxDTM0MTEyNjE3
MIIBCAQCAQEAAlvXOq72ZDe7jxw/WjZGgb9/nJHgk7mBOAEHvqN33wTFYjXKmYu
qkY86ohSpHrm4ac3zFNRkWW57e/N/ZfKrGyc42vmnaHr9yZc7xlr/qCdKHu3uunV
b8YF1FLXvrhYh6GGE1TTQ7Hz4ZXE42NrwJQGY+IC68YFTzXzkMYthDOoaM8AeEOd
oAE7IADHMeLo4butMTb5v8Aa/biFE3CaoudEM8uYOMOTiiQYIINBECF3uoCEKsEW/
```

E no final precisamos colocar a **server.key** dentro desse certificado, depois disso daí podemos clicar em importar certificado.

## Importar certificado

### Detalhes do certificado [Informações](#)

#### Corpo do certificado

```
mmzPYfCjKzr75kGRwkFBlidIP/TnpX07z/P76YaQ==  
-----END CERTIFICATE-----
```

#### Chave privada do certificado

```
a8WThjic2CkqhfEBY1S8CZy  
-----END PRIVATE KEY-----
```

#### Cadeia de certificados - opcional [Informações](#)

```
vaZmQ/maYZhWii8snBNsA==  
-----END CERTIFICATE-----
```

### Etiquetas [Informações](#)

Nenhuma tag associada ao recurso.





[Adicionar nova tag](#)

Você pode adicionar até 50 tags.

[Cancelar](#)

[Importar certificado](#)

Depois disso vamos ter que importar outro certificado para dentro do certificate manager de novo em importar certificado, e vamos adicionar esses dois arquivos respectivamente o **client1.domain.tld.cert** como corpo do certificado e **client1.domain.tld.key** como chave privada do certificado dentro do certificado.

 client1.domain.tld.crt		28/11/2024 15:01	Certificado de Seg...	5 KB
 client1.domain.tld.key		28/11/2024 15:00	Arquivo KEY	2 KB

Ficando assim e já podemos importar esse certificado:

## Importar certificado

### Detalhes do certificado [Informações](#)

#### Corpo do certificado

```
Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
78:ea:44:fd:f8:3d:b7:5b:73:96:a0:a5:96:89:7b:f7  
Signature Algorithm: sha256WithRSAEncryption
```

#### Chave privada do certificado

```
-----BEGIN PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAkwggSkAgEAAoIBAQQDDot9GoAsAbqvj  
EU2xk62eliFNPxSIt75Xm+BXh5g8Urk+C3eehoVJK/tUy4wnwhlyGFbk8CybW3n  
/AFOccBMbcy6k2nHeMP8E6utwo5A71jGndRn0VUF1zLeJL6sz9WwGaRTWgsWmKSx  
M30bZGYKP99ek1RWcXfleU7KlyTgtGHuOrqF3NaMIWYXizXNDc6C6dSTJGWLIZ  
jtGSaHvM4TF5pIOA1xLhFimNK6ms0MBOJ59XAcc3kXjeO/9bSmfu6WzgCvVMSPz
```

#### Cadeia de certificados - opcional [Informações](#)

Cole a cadeia de certificados codificados por PEM abaixo.

### Etiquetas [Informações](#)

Nenhuma tag associada ao recurso.

[Adicionar nova tag](#)

Você pode adicionar até 50 tags.

[Cancelar](#)

[Importar certificado](#)

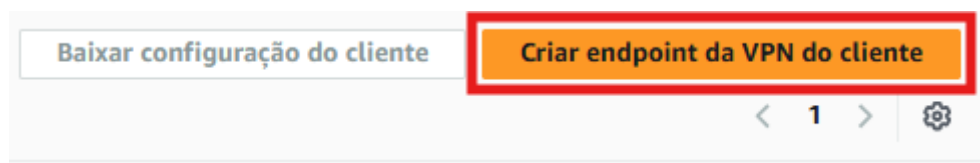
# VPN

Com isso já podemos criar nossa cliente vpn

Voltando para o console da VPC podemos acessar a aba de vpn para se criar uma vpn cliente para se utilizar como uma conexão ssh de nossa máquina local para a AWS.



Nele vamos clicar em criar um endpoint para a vpn



Agora na configuração vamos utilizar esses passo:

Nome: client-vpn

Client IPv4 CIDR: 192.168.0.0/16

Na parte dos Certificates habilitar o usar **autenticação mútua** depois disso colocar o server como primeiro certificado e o client como segundo.



## Criar endpoint da VPN do cliente [Informações](#)

Crie um endpoint de VPN do cliente para permitir o acesso a redes por meio de uma sessão de VPN TLS.

### Detalhes

#### Etiqueta de nome - *opcional*

Cria uma etiqueta com a chave definida como Nome e o valor definido como a string especificada.

O nome deve ter 255 caracteres ou menos.

#### Descrição - *opcional*

Uma breve descrição do endpoint de VPN do cliente.

#### CIDR IPv4 do cliente [Informações](#)

O intervalo de endereços IP, em notação CIDR, do qual os endereços IP do cliente são alocados.



O bloco CIDR não pode ser maior que /12 ou menor que /22.

### Informações de autenticação [Informações](#)

#### ARN do certificado do servidor

O certificado do servidor deve ser provisionado ou importado para o AWS Certificate Manager (ACM).



#### Opções de autenticação

Escolha um ou uma combinação de métodos de autenticação para usar.

- ☒ Usar autenticação mútua  
☐ Usar autenticação baseada em usuário

#### ARN do certificado do cliente [Informações](#)



Na aba de outros parâmetros vamos definir que nossa vpn use um **split-tunnel** e conectar ela a vpc criada anteriormente, depois escolher o grupo de segurança **vpn-sg** e habilitar a **Habilitar o portal de autoatendimento**.

### Outros parâmetros - *opcional*

#### Endereço IP do servidor DNS 1

O endereço IP do servidor DNS a ser usado. Não há servidores DNS padrão.

#### Endereço IP do servidor DNS 2

O endereço IP do servidor DNS a ser usado. Não há servidores DNS padrão.

#### Protocolo de transporte | [Informações](#)

Protocolo de transporte usado pelas sessões TLS.

☒ UDP☐ TCP☒ Habilitar split-tunnel [Informações](#)

#### ID da VPC

#### IDs de grupo de segurança

Grupos de segurança a serem aplicados ao endpoint.

Habilitando SSH e ICMP

#### Porta da VPN

A VPN do cliente da AWS oferece suporte às portas 443 e 1194 para TCP e UDP.

☒ Habilitar o portal de autoatendimento [Informações](#)

#### Horas de tempo-limite da sessão | [Informações](#)

☐ Habilitar banner de login do cliente [Informações](#)

Clicando nela podemos acessar as associações de rede de destino e podemos clicar em associar rede de destino.

Endpoints da VPN do cliente (1/1) [Informações](#)

Localizar cliente VPN por atributo ou tag

Name	ID do endpoint da VPN do cliente	Estado	CIDR do cliente
client-vpn	cvpn-endpoint-01ffdaacf19a1a9e5	Pending-associate	192.168.0.0/16

cvpn-endpoint-01ffdaacf19a1a9e5 / client-vpn

[Detalhes](#) [Associações de rede de destino](#) [Grupos de segurança](#) [Regras de autorização](#) [Tabela de rotas](#) [Conexões](#) [Tags](#)

Associações de rede de destino [Informações](#)

Localizar associações de rede de destino por atributo

ID da associação	Estado	ID da rede	Grupos de segurança	ID do endpoint	Descrição
Nenhuma rede de destino					
Você não tem redes de destino da VPN do cliente nessa região.					

[Associar rede de destino](#)

Nela vamos indicar nossa vpc e colocar a **Subnet01**.


[VPC](#) > [Endpoints da VPN do cliente](#) > [cvpn-endpoint-01ffdaacf19a1a9e5](#) > [Associar rede de destino](#)

## Associar rede de destino [Informações](#)

Uma rede de destino é uma sub-rede em uma VPC. Você associa uma sub-rede em uma zona de disponibilidade ao endpoint da VPN do cliente. É possível associar uma sub-rede por zona de disponibilidade. As sub-redes em uma VPC podem ser associadas a um endpoint de VPN do cliente.

**Detalhes**

ID do endpoint da VPN do cliente

 cvpn-endpoint-01ffdaacf19a1a9e5

VPC

vpc-076011bd2552c7944 (vpc\_vpn)

Escolha uma sub-rede para associar

subnet-0c358936f1660a160 (Subnet01)

[Cancelar](#) [Associar rede de destino](#)

Depois disso vamos criar uma autorização para nossa vpn.

Endpoints da VPN do cliente (1/1) [Informações](#)

Localizar cliente VPN por atributo ou tag

Name	ID do endpoint da VPN do cliente	Estado	CIDR do cliente
client-vpn	cvpn-endpoint-01ffdaacf19a1a9e5	Pending-associate	192.168.0.0/16

cvpn-endpoint-01ffdaacf19a1a9e5 / client-vpn

[Detalhes](#) [Associações de rede de destino](#) [Grupos de segurança](#) [Regras de autorização](#) [Tabela de rotas](#) [Conexões](#) [Tags](#)

Regras de autorização [Informações](#)

Localizar authorization rule por atributo ou tag

ID do endpoint	Estado	Descrição	ID do grupo	Acessar todos	CIDR de destino
Nenhuma authorization rule					
Você não tem nenhuma authorization rule nessa região.					

[Criar authorization rule](#)


Na configuração vamos colocar o cidr da nossa vpc e deixar permitir acesso a todos os usuários.

## Adicionar regra de autorização [Informações](#)

Adicione regras de autorização para conceder aos clientes acesso às redes.



### Detalhes

ID do endpoint da VPN do cliente

 cvpn-endpoint-01ffdaacf19a1a9e5

Rede de destino para permitir acesso

O endereço IP, em notação CIDR, da rede de destino.

 10.0.1.0/16 

Conceder acesso a:

- ☒ Permitir acesso a todos os usuários  
☐ Permitir acesso a usuários em um grupo de acesso específico

Descrição - *opcional*

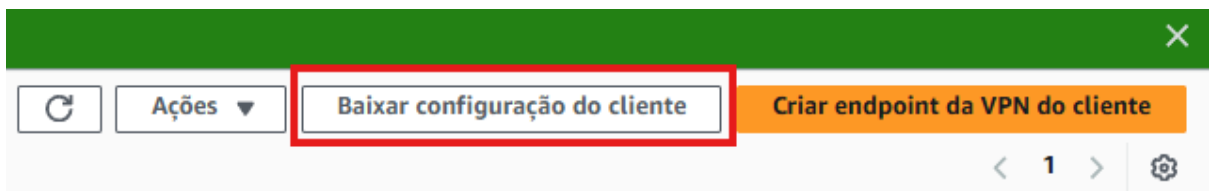
Uma breve descrição da regra de autorização.

Cancelar

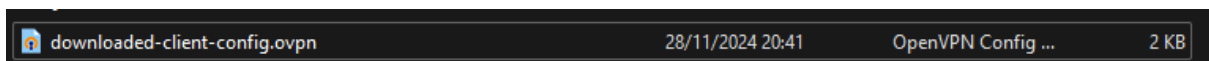
Adicionar regra de autorização

Depois disso nós vamos precisar esperar as regras e associações serem criadas.

Com isso do lado de Criar endpoint da VPN do cliente podemos baixar as configurações do client.



Com esse arquivo baixado vamos ter que editar ele como bloco de notas e ajustá-lo.



.Bem no final do arquivo vamos adicionar essas linhas:

<cert>

</cert>

<key>

</key>

```

remote-cert-tls server
cipher AES-256-GCM
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIDSzCCAjOgAwIBAgIUcNr8K6VXcWPYAlQE4nKlwKQ+XuIwDQYJKoZIhvcNAQEL
BQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjQxMTI4MjMxNzQ3WhcNMzQx
MTI2MjMxNzQ3WjAwMRQwEgYDVQQDDAtFYXN5LVJlTQSBDOQCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAJHpC+HbcsPc0n1zXOTKipq2krnmM5/3mAtYABwG
dDZ+5bz+5YIwpVgj2fKmZoHGjROVoy9ULG1CmRe0zwJbtt0lHG7O+XdnKQx6p7T+
4iqGrTz7c9EG71wP3bjSHMhWCD/hRzbLu9jZFHh1LJiFZR8FV7p5vkUKh5BEihX3
IH3KZTFKwC96HgOaaqr0RK62lLf93llidnQXMTcsRybAQVQeIA+jnxh/aNMa3jOX
onPnWBPSfnJi8iBEaD3/tYegqsm1CEXMBskLYG7PCV0agFhd/VKA2vcsLMVjujN0
A4hhXgn3iBxPFThjmdihb+A+71SJSJ3WvPhEJHuzdrnVR3ECAwEAAaOBkDCBjTAM
BgNVHRMEBTADAQH/MB0GA1UdDgQWBRR5V2iiwKe3Kb5CQnCKBb+9mlyvNTBRBgNV
HSMESjBIBR5V2iiwKe3Kb5CQnCKBb+9mlyvNaEapBgwFjEUMBIGA1UEAwwLRWFz
eS1SU0EgQ0GCFaja/CulV3Fj2AJUBOJypVpEP17iMAsGA1UdDwQEAwIBBjANBgkq
hkiG9w0BAQsFAAOCAQEAFtceemzbaxaoevRdTkOI1/DF94FhLYxqqzync3xrB9Ys
ugkmYwic4E85YD2ybdznmdBNtE7y+TaJ52Xg/ICTHPl6Z3DLkaSX+etzUv9G0VSS
6lZuro9dYeljs16zH+aXnglylw40oBYReok/EJNosmYm2xY0da7kSGzTp93/E5EC
rXyd0DflaJvk4QB9QHGU0i1+ZB1d3+E42TXZO1pDkHWeZkIce57LrwRmgVmH1Za9
pRsKtNmRrIa2GLiMJOGvn5YyQnF8FeflZJY90mcEq546wDZECILhLf50fA3Ged7a
iQlS5Sc/XwgVTTFZ4JZe2qY0DlAgRSdLLFcDKP5YAA==
-----END CERTIFICATE-----

</ca>

reneg-sec 0

verify-x509-name server name



<cert>

</cert>

<key>

```

Dentro delas vamos colocar o certificado e a key do client para acessar ele.

 client1.domain.tld.crt	28/11/2024 20:18	Certificado de Seg...	5 KB
 client1.domain.tld.key	28/11/2024 20:18	Arquivo KEY	2 KB

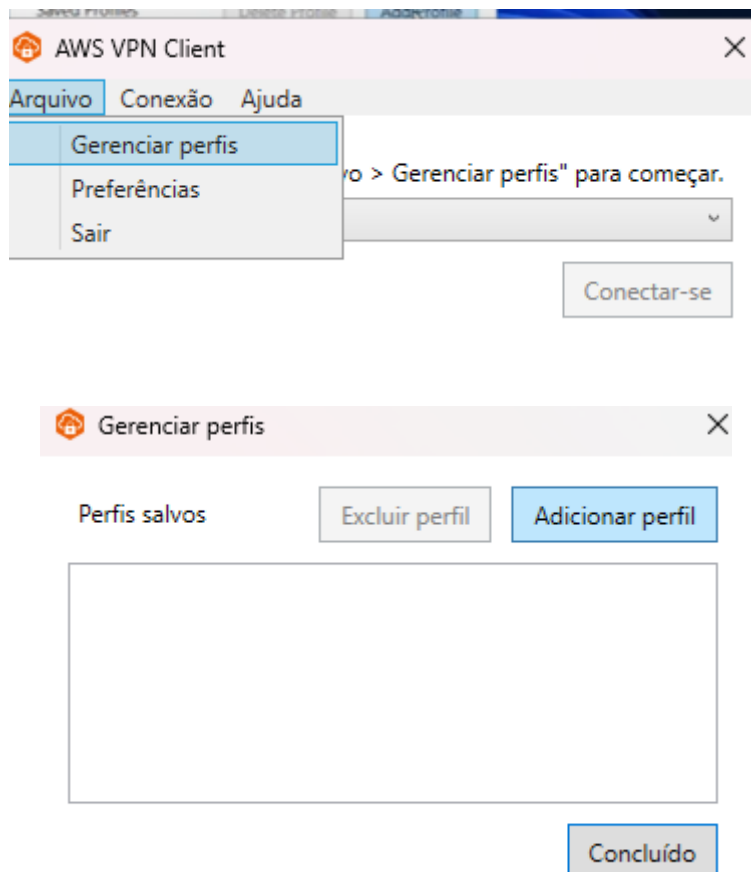
Esses dois arquivos respectivamente.

### ACESSANDO:

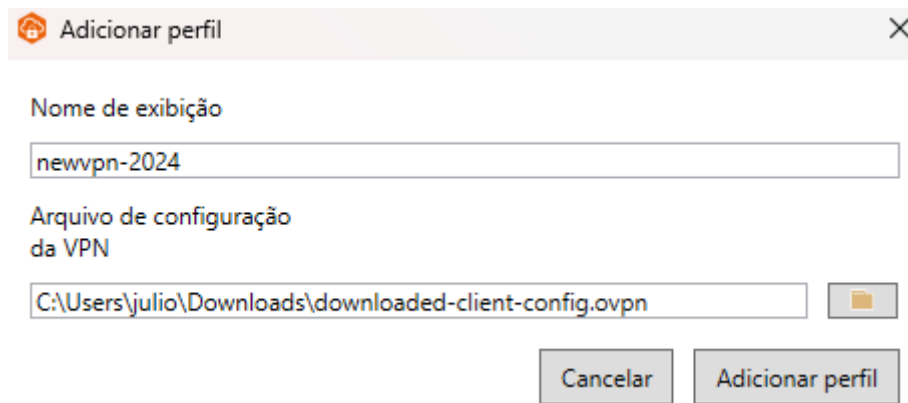
Precisamos de software para se conectar a essa vpn o aws client vpn pode baixar ele acessando o link em baixo.

<https://aws.amazon.com/pt/vpn/client-vpn-download/>

com ele aberto vamos ir em arquivo e em gerenciar perfis.

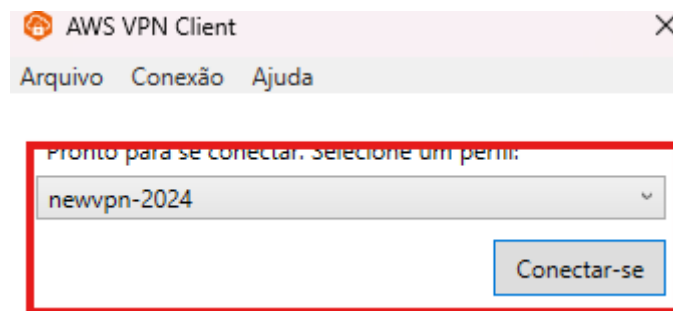


Nele vamos clicar em Adicionar perfil.



adicionando vamos colocar o nome de exibição e em arquivo vamos colocar o arquivo recém configurado.

Depois só Conectar-se.



Com isso podemos pegar nosso private ipv4 address da nossa máquina e testar o ping nele.

```
C:\Users\julio>ping 10.1.2.254

Disparando 10.1.2.254 com 32 bytes de dados:
Resposta de 10.1.2.254: bytes=32 tempo=137ms TTL=126
Resposta de 10.1.2.254: bytes=32 tempo=138ms TTL=126

Estatísticas do Ping para 10.1.2.254:
    Pacotes: Enviados = 2, Recebidos = 2, Perdidos = 0 (0% de
    perda),
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 137ms, Máximo = 138ms, Média = 137ms
Control-C
^C
C:\Users\julio>
```