

## Lab 3 - VPN

### 1. Inicie o CloudFormation para ambiente simulado de data center

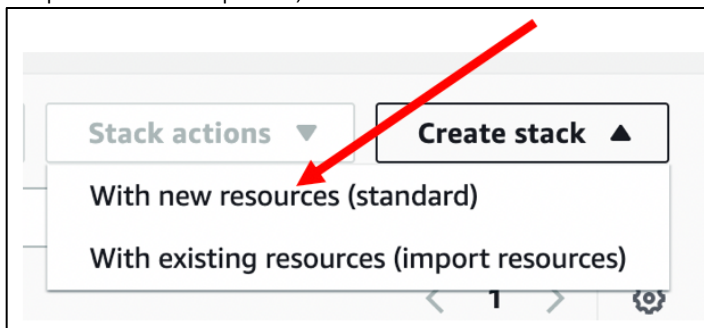
Se você estiver usando sua própria conta, você deve criar o ssh keypair:

- Navegar para o console EC2 - Pares de chaves
- Clique em **Criar par de chaves**
- De um nome (laboratorio3, por exemplo), clique em Criar par **de chaves**

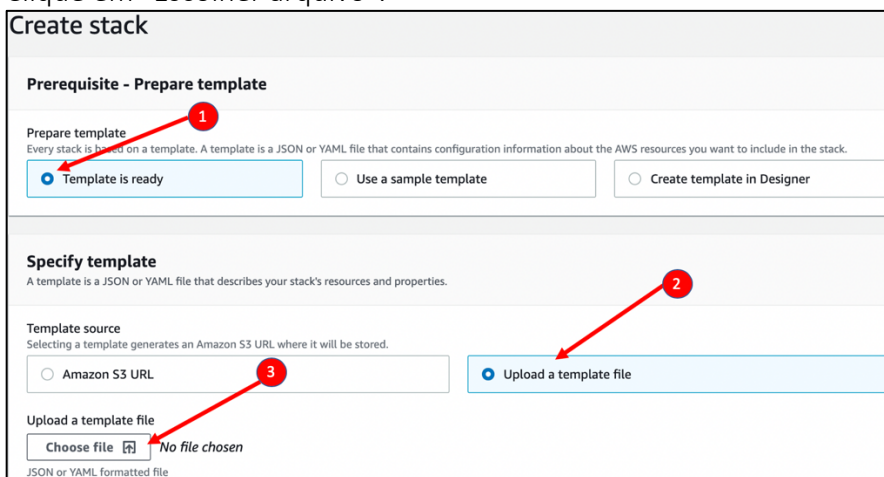
Agora estamos prontos para implantar um modelo de CloudFormation fornecido para o ambiente simulado no local.

<https://networking.workshop.aws/cfn/Basic-Lab2-On-prem-simulator.yaml>

- Navegue até o console CloudFormation
- Clique em "Criar pilha", selecione "Com novos recursos (padrão):"



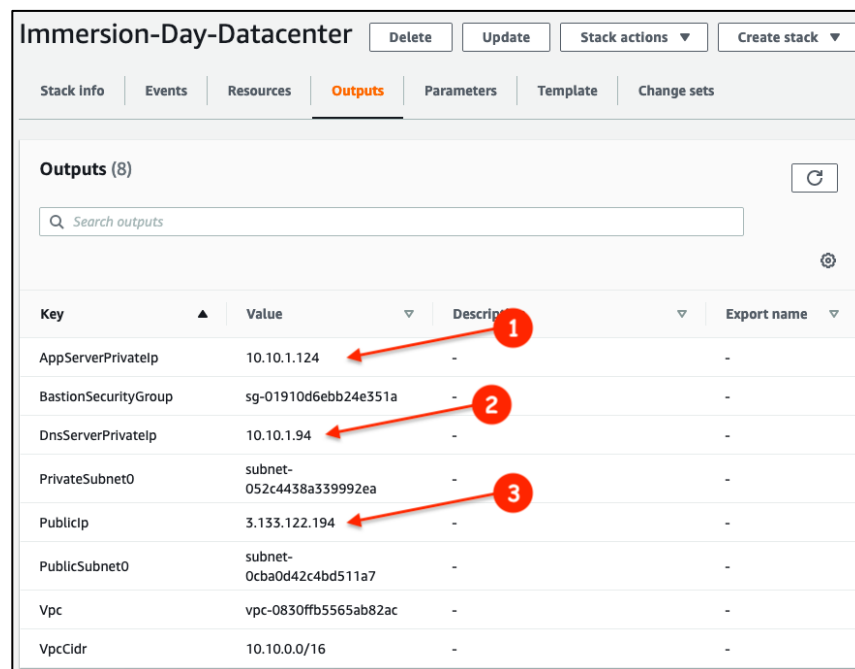
- Escolha "O modelo está pronto"
- "Carregar um arquivo de modelo"
- Clique em "Escolher arquivo".



- Use apenas o arquivo Basic-Lab2-On-prem-simulator.yaml e clique em "Next".

- Dê um nome a Stack, por exemplo, Network-Immday-DC. Essa stack criará 1 VPC com uma sub-rede pública e privada, bem como as três instâncias EC2 para o Bastion Host, DNS Server e Application Server.
- Revise os blocos de CIDR VPC e outros parâmetros. Para obter o parâmetro SshKeyName, selecione sua chave SSH. Clique em "Next".
- Aceite os valores padrão em "Configure opções de stack" e clique em "Próximo".
- Revise os parâmetros e clique em "Criar stack".

Aguarde que a stack seja criada. Navegue até a guia Saídas e tome nota do IP privado (1) do servidor de aplicativos, do IP privado (2) do servidor DNS e do IP público do bastion host (3).



Key	Value	Description	Export name
AppServerPrivateIp	10.10.1.124	-	-
BastionSecurityGroup	sg-01910d6ebb24e351a	-	-
DnsServerPrivateIp	10.10.1.94	-	-
PrivateSubnet0	subnet-052c4438a339992ea	-	-
PublicIp	3.133.122.194	-	-
PublicSubnet0	subnet-0cba0d42c4bd511a7	-	-
Vpc	vpc-0830ffb5565ab82ac	-	-
VpcCidr	10.10.0.0/16	-	-

## 2. Explore o ambiente simulado do datacenter

Lançamos agora um ambiente simulado de datacenter que consiste em um bastion host, um servidor de aplicativos web e um servidor DNS. Vamos garantir que os componentes estejam funcionando antes de passarmos a conectá-lo ao nosso ambiente AWS.

- Use a opção Connect a partir do console EC2, por exemplo, com OnPremBastion- no nome (ambas as opções funcionarão "EC2 Instance Connect" e "Session Manager").

Ou SSH no bastion host usando seu par de chaves.

```
ssh -i laboratorio3.pem ec2-user@<PUBLIC IP>
```

- Observe que a instância está usando o servidor DNS personalizado em vez do padrão VPC examinando o arquivo `/etc/resolv.conf`.

```
• cat /etc/resolv.conf
```

Note a linha "nameserver", que deve apontar para o endereço IP do Servidor DNS que você observou das saídas da stack CloudFormation acima.

- Teste o app server. Em nosso ambiente simulado de datacenter, usamos o nome de domínio interno "exemplo.corp" e o servidor de aplicativos tem uma entrada de hostname para "myapp.example.corp". Podemos testar que o servidor de aplicativos está funcionando usando o comando curl:

```
• curl http://myapp.example.corp
```

Se o servidor de aplicativos estiver funcionando corretamente, você verá uma resposta de "Olá, mundo".

Agora que verificamos a funcionalidade do nosso datacenter simulado on prem, vamos conectá-lo ao nosso Transit Gateway usando uma conexão VPN.

### 2.1 Estabelecer conectividade VPN entre a AWS e o datacenter

No Lab 1: Arquitetura de contas Multi-VPC, criamos um Transit Gateway para interconectar nossos 3 VPCs. Para integrar o ambiente simulado de datacenter, estabeleceremos uma conexão VPN entre o Transit Gateway e um dispositivo de gateway do cliente no datacenter. Como este é um ambiente simulado, usaremos o OpenSWAN como porta de entrada do cliente em execução no bastion host.

### 2.2 Crie um anexo transit gateway

- Navegue até o painel VPC - Anexos do Gateway de Trânsito e clique em "Criar anexo do Gateway de Trânsito".

- Crie um novo anexo VPN.
- Altere o tipo de anexo para **VPN** e selecione para criar um novo Gateway do **Cliente**.
  - Para endereço IP, digite o **IP público do bastion host** identificado na etapa anterior.
  - Altere as opções de roteamento para roteamento "estático".
  - Deixe todas as outras configurações em seus padrões
  - Clique em "Criar anexo"

- Selecione a guia Conexões VPN site a site no console VPC e aguarde a conexão VPN recém-criada para fazer a transição para o status disponível.
  - Uma vez que a conexão VPN esteja disponível, selecione "Configuração de download" e selecione "Openswan" para o fornecedor.
  - Salve o arquivo baixado para depois.

- Enquanto ainda estiver visualizando as conexões VPN local para local, selecione a guia Detalhes do túnel. Tome nota do "Endereço IP externo" para os dois túneis. Você se

referirá a eles mais tarde ao configurar os grupos de segurança do ambiente de datacenter simulado.

VPN Connection: vpn-0cb4d853125eacaaf

Details Tunnel Details Static Routes Tags

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed
Tunnel 1	3.21.79.28	169.254.102.8/30	DOWN	May 11, 2020 at 1:47:57 PM UTC-4
Tunnel 2	3.21.180.139	169.254.191.224/30	DOWN	May 11, 2020 at 1:47:55 PM UTC-4

- Como estamos usando roteamento estático para nossa conexão VPN, precisaremos criar manualmente uma rota para a rede de datacenter.
- No console VPC - Transit Gateway Route Tables certifique-se de que a tabela principal de rotas do Transit Gateway está selecionada e, em seguida, selecione a guia "Rotas" no painel inferior. Clique em "Criar rota" para adicionar uma nova rota estática.

Create Transit Gateway Route Table Actions

Filter by tags and attributes or search by keyword

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default prop
tgw-rtb-0f8172fb35fe57520	tgw-0729b820732f637fe	available	Yes	Yes	

Transit Gateway Route Table: tgw-rtb-0f8172fb35fe57520

Details Associations Propagations Routes Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

CIDR	Attachment	Resource type
<input type="checkbox"/> 10.0.0.0/16	tgw-attach-06a444f03825033ed   vpc-0bfe88cc0e4036b4	VPC
<input type="checkbox"/> 10.1.0.0/16	tgw-attach-040643acc0511b9cc   vpc-06a845565d0fa6adc	VPC
<input type="checkbox"/> 10.2.0.0/16	tgw-attach-0db64eb50f340142d   vpc-0540710528cec3d7c	VPC

- Digite o bloco CIDR para o ambiente simulado de data center 10.10.0.0/16 e selecione o anexo VPN que você acabou de criar. Clique em "Criar rota".

**Create route**

Add a static route to your Transit Gateway route table.

Transit Gateway ID: tgw-0729b820732f637fe

Transit Gateway route table ID: tgw-rtb-0f8172fb35fe57520

CIDR\*: 10.10.0.0/16

Blackhole: ☐

Choose attachment:

\* Required

Attachment ID	Resource ID	Name tag	Resource owner ID	Association route table
tgw-attach-040643acc0511b9cc	vpc-06a845565d0fa9adc	VPC B	506925741753	tgw-rtb-0f8172fb35fe57520
tgw-attach-06a444f03825033ed	vpc-0bfe188cc0e4036b4	VPC A	506925741753	tgw-rtb-0f8172fb35fe57520
tgw-attach-0db84eb509340142d	vpc-05407105280ec3d7c	VPC C	506925741753	tgw-rtb-0f8172fb35fe57520
tgw-attach-0c19cf843e8fec73c	vpc-0cb4c853125eacaf	VPN	506925741753	tgw-rtb-0f8172fb35fe57520

Create route

## 2.3 Configure o roteamento simulado do VPC do datacenter.

Como usaremos nosso bastion host como um gateway de cliente, precisaremos configurar nosso VPC simulado de datacenter para usar essa instância EC2 como roteador para alcançar os VPCs conectados ao Transit Gateway.

- Navegue até o console EC2 - Instâncias
- Localize bastion host e selecione-o. Seu nome começará com **OnPremBastion**.
- No menu "Ações", selecione "Networking", depois "Alterar fonte/verificação de destino".

**Launch Instance** **Connect** **Actions**

Filter by tags and attributes or search

Name	Instance ID	Instance Type	Availability Zone	Instance State
OnPremAppServer-Immersion-D...	i-0bc612156b952ca80	t2.micro	us-east-2a	Running
aws-cloud9-mb-10ef3821c6064a...	i-0cef70ecb6123266a	t2.micro	us-east-2b	Running
EC2 in VPC-B	i-0d812f76bba99ba0c	t2.micro	us-east-2a	Running
aws-cloud9-modernize-e09ee3d...				
EC2 in VPC-A				
OnPremBastion-Immersion-Day...	i-0bc612156b952ca80	t2.micro	us-east-2a	Running
EC2 in VPC-C				
OnPremDnsServer-Immersion-D...				

**Actions**

- Connect
  - Get Windows Password
- Create Template From Instance
- Launch More Like This
- Instance State
- Instance Settings
- Image
- Networking**
  - Change Security Groups
  - Attach Network Interface
  - Detach Network Interface
  - Disassociate Elastic IP Address
  - Change Source/Dest. Check**
  - Manage IP Addresses
- CloudWatch Monitoring

Selecione "Parar". Isso permitirá que você use a instância como roteador, passando o tráfego que não está destinado ao próprio endereço IP da instância EC2. Sem essa opção ativada, o EC2 não encaminhará pacotes IP para ou a partir da instância em que o endereço IP de

origem ou destino não corresponda ao da instância.

**Source / destination check** [Info](#)  
Each EC2 instance performs source and destination checks by default. The instance must be the source or destination of all the traffic it sends and receives.

Instance ID  
[i-000a3dd30495e2eed](#) (OnPremBastion-Network-Immday-DC)  
Network interface [Info](#)  
[eni-06922d0fb6aeaec6](#)  
Source / destination checking [Info](#)  
☒ Stop

**Info** If this is a NAT instance, you must stop source / destination checking. A NAT instance must be able to send and receive traffic when the source or destination is not itself.

▼ AWS CLI Command

```
aws ec2 modify-instance-attribute --instance-id=i-000a3dd30495e2eed --no-source-dest-check
```

Copy

Cancel

Save

- Com o bastion host ainda selecionado no console EC2, clique no Grupo de Segurança no painel inferior para visualizar e editar suas regras. Precisaremos permitir que os endpoints da AWS VPN se comuniquem com a instância sobre o IPSEC.

☒ OnPremBastion-Network-Immday-DC [i-000a3dd30495e2eed](#)

Instance: i-000a3dd30495e2eed (OnPremBastion-Network-Immday-DC)

Details

Security

Networking

Storage

Status checks

▼ Security details

IAM Role

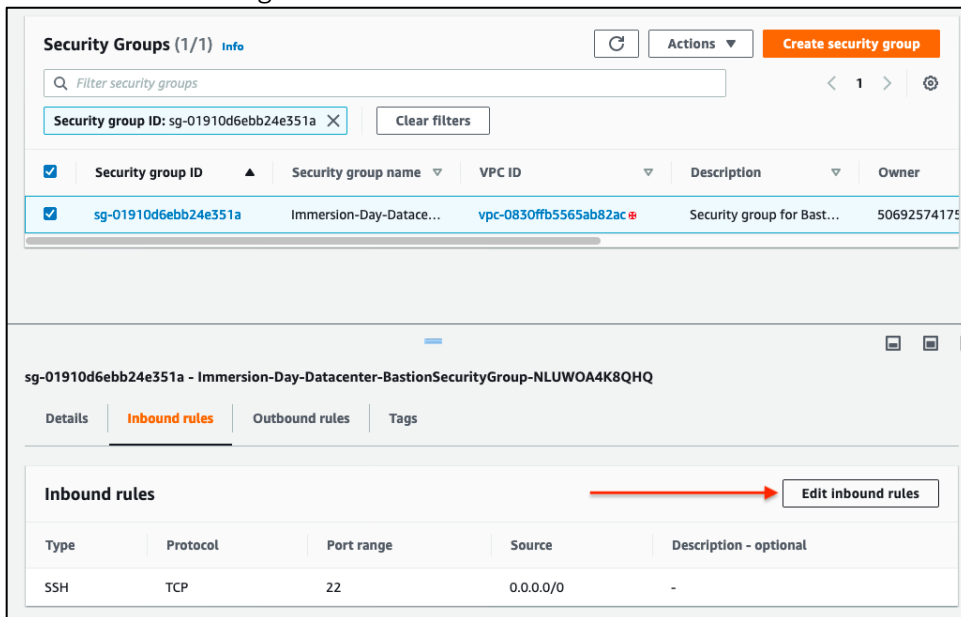
[AmazonSSMManagedInstanceCore](#)

Owner ID

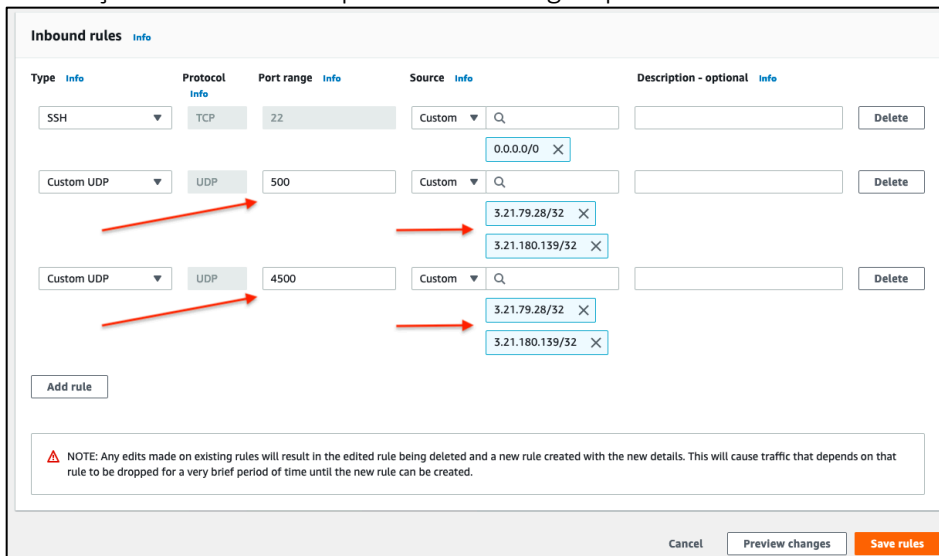
Security groups

[sg-0ad2c5d37e8719956](#) (Network-Immday-DC-BastionSecurityGroup-PVNTGQH887PT)

- Selecione "Editar regras de entrada".



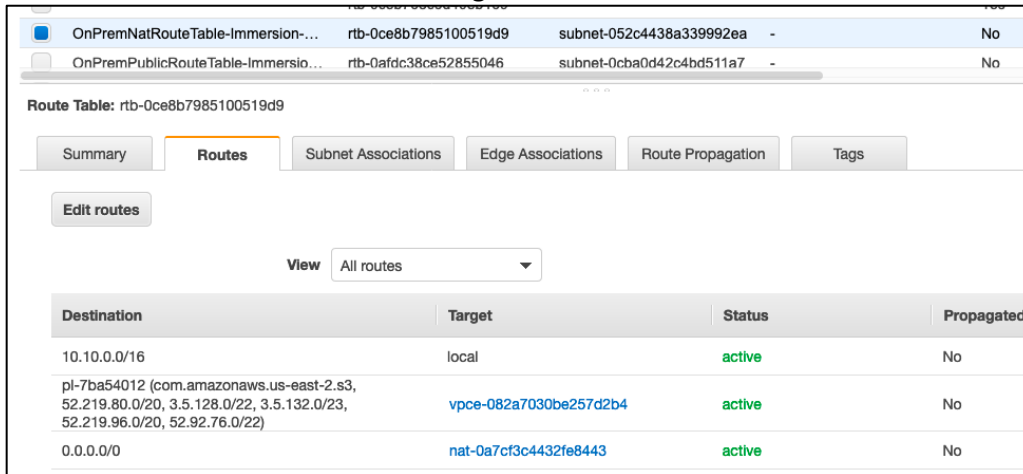
- Adicione regras para portas UDP 500 e 4500 para os dois endereços "externos" do túnel que você observou ao criar a conexão VPN na etapa 2.1 acima. A caixa de diálogo exige que você digite os endereços em notação CIDR, então basta anexar /32 ao fim dos dois endereços IP do túnel. Clique em Salvar regra quando terminar.



- Por fim, vamos atualizar as tabelas de rotas VPC para o ambiente simulado de datacenter para direcionar o tráfego para o ambiente AWS através do OpenSWAN no bastion host. Navegue até o console VPC e selecione "Tabelas de Rota"
- Localize a tabela de rotas OnPremNatRouteTable. Esta tabela de rotas é usada para a sub-rede privada que contém o servidor DNS e o App Server. O nome começará com

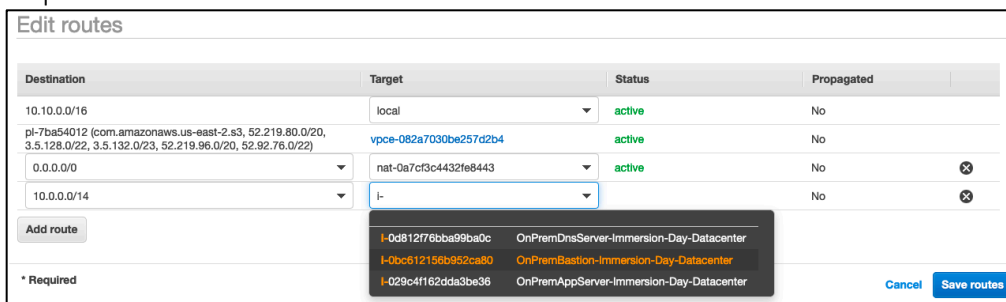


## OnPremNatRouteTable. Seleccione a guia Rotas.



Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
pl-7ba54012 (com.amazonaws.us-east-2.s3, 52.219.80.0/20, 3.5.128.0/22, 3.5.132.0/23, 52.219.96.0/20, 52.92.76.0/22)	vpce-082a7030be257d2b4	active	No
0.0.0.0/0	nat-0a7cf3c4432fe8443	active	No

- Clique em "Editar rotas". Adicione uma rota para o ambiente AWS VPC, consistindo dos três VPCs anexados ao Transit Gateway. A rota pode ser resumida como 10.0.0.0/14. Selecione "Instância" como o destino e selecione seu bastion host. Uma vez concluído, clique em "Salvar rotas".



Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
pl-7ba54012 (com.amazonaws.us-east-2.s3, 52.219.80.0/20, 3.5.128.0/22, 3.5.132.0/23, 52.219.96.0/20, 52.92.76.0/22)	vpce-082a7030be257d2b4	active	No
0.0.0.0/0	nat-0a7cf3c4432fe8443	active	No
10.0.0.0/14	i-		No

I-0d812f76bba99ba0c OnPremDnsServer-Immersion-Day-Datacenter

I-0bc612156b952ca80 OnPremBastion-Immersion-Day-Datacenter

I-029c4f162dda3be36 OnPremAppServer-Immersion-Day-Datacenter

\* Required

Cancel Save routes

Atualizar tabelas de rotas:

rt-vpc-a, rt-vpc-b, rt-vpc-c e inclua a rota para volta 10.10.0.0/16 – Transit Gateway

## 2.4 Configure OpenSWAN e suba o túnel

Agora que configuramos o VPC simulado do datacenter e criamos a conexão VPN com o Transit Gateway, estamos prontos para configurar o OpenSWAN no bastion host e subir o túnel. O OpenSWAN já foi instalado no bastion host. Usaremos o arquivo de configuração baixado na Etapa 2.1 para configurar a VPN.

- Use a opção Conectar para a instância Bastion no console EC2 para conectar à instância (opção gerenciador de sessão), ou apenas `ssh -i laboratorio3.key ec2-user@<PPP>` usando seu keypair.
- Editar o `/etc/sysctl.conf` para habilitar o encaminhamento de IP:
- `sudo nano /etc/sysctl.conf`

Adicione os seguintes parâmetros ao final do arquivo:

```
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.default.accept_source_route = 0
```

Para salvar as alterações pressione Ctrl+O, Enter, Ctrl+X

- Aplique as alterações de configuração usando sysctl:
- `sudo sysctl -p`
- Abra o arquivo de configuração que você baixou do console VPC na Etapa 2.2 para o gateway do cliente em um editor de texto. Seguiremos este arquivo para configurar o OpenSWAN para o Túnel 1. Como o OpenSWAN não fornece capacidade de failover de túnel embutido, estaremos apenas configurando um dos túneis.
- Crie um arquivo `aws.conf` em `/etc/ipsec.d` e edite da seguinte forma:
- `sudo nano /etc/ipsec.d/aws.conf`
- Copie e cole a seção "conn Tunnel1" das instruções do passo 4 do arquivo de configuração baixado (use o editor preferido para fazer as alterações).
- Faça as seguintes alterações:
  - Exclua a linha `auth=esp`.
  - Substitua `<LOCAL NETWORK>` na linha `"leftsubnet="` com o bloco CIDR para o ambiente simulado do data center: `10.10.0.0/16`
  - Substitua `<REMOTE NETWORK>` na linha `"rightsubnet="` com o bloco CIDR para o ambiente AWS: `10.0.0/14`
- A entrada final deve ser assim:

```
conn Tunnel1
  authby=secret
  auto=start
  left=%defaultroute
  leftid=<BASTION IP ADDRESS>
  right=<AWS VPN TUNNEL IP>
  type=tunnel
  ikelifetime=8h
  keylife=1h
  phase2alg=aes128-sha1;modp1024
  ike=aes128-sha1;modp1024
  keyingtries=%forever
  keyexchange=ike
  leftsubnet=10.10.0.0/16
  rightsubnet=10.0.0.0/14
  dpddelay=10
  dpdtimeout=30
  dpdaction=restart_by_peer
```

- Crie um arquivo `aws.secrets` em `/etc/ipsec.d` e edite da seguinte forma:
- `sudo nano /etc/ipsec.d/aws.secrets`

Copie e cole a linha `aws.secrets` a partir do passo 5 das instruções no arquivo de configuração.

- Habilitar e iniciar o OpenSWAN:
- `sudo systemctl enable ipsec.service`
- `sudo ipsec start`
- Levante o túnel enviando tráfego para o lado da AWS.

Encontre o endereço IP privado de uma das três instâncias EC2 em VPC A, VPC B ou VPC C e ping-o do bastion host:

```
ping <IP endereço de instância VPC>
```

Note que pode levar até 30 segundos antes que o túnel apareça e você comece a ver respostas de ping.