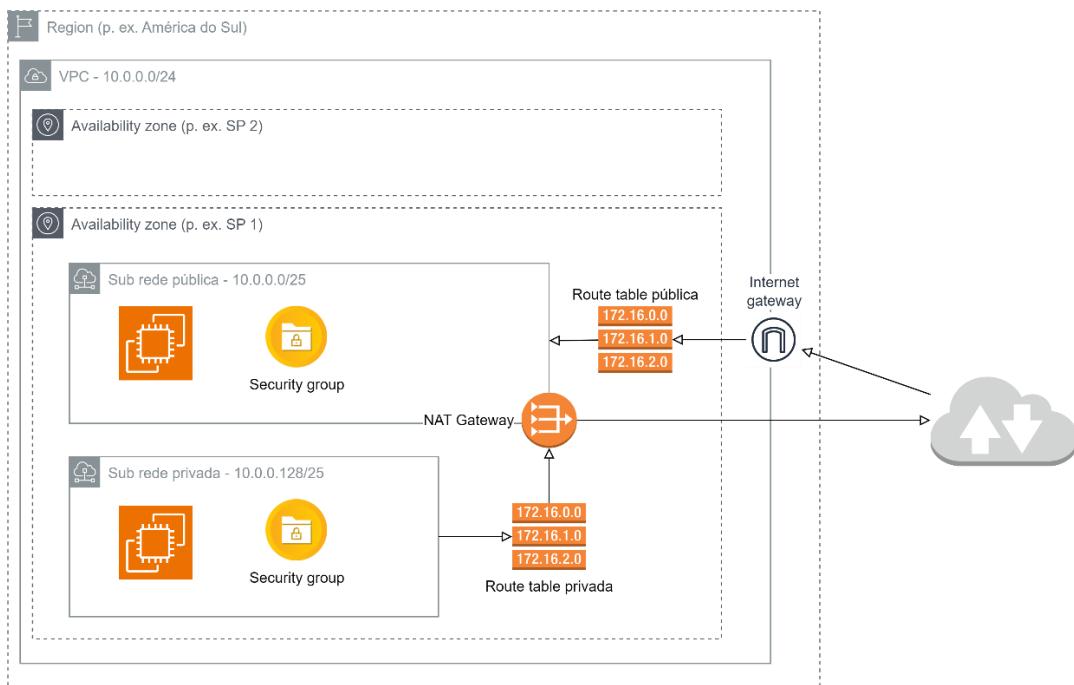


## Sumário

Arquitetura de referência .....	2
Configurando a VPC.....	2
Provisionamento instância em sub redes .....	7
Configurando Internet Gateway e Route Table .....	15
Configurando NAT Gateway e Route Table.....	21

## Arquitetura de referência



## Configurando a VPC

Acesse o console AWS e busque por VPC

A captura de tela mostra a interface do AWS CloudFront com a barra de busca "vpc" selecionada. A lista de resultados inclui:

- Services (12)**: VPC, AWS Firewall Manager, Detective, Managed Services.
- Features (57)**: Documentation, Knowledge Articles, Marketplace, Blogs, Events, Tutorials.

A captura de tela mostra o "VPC dashboard" no AWS CloudFront. A interface inclui:

- VPC dashboard**: Botões para "Create VPC" e "Launch EC2 Instances". Nota: "Your Instances will launch in the US East region."
- Resources by Region**: Seção com links para "VPCs", "NAT Gateways", "Subnets", "VPC Peering Connections", "Route Tables", "Network ACLs", "Internet Gateways" e "Security Groups", todos no "US East 1" (0 ou 1 recursos).
- Service Health**: Link para "View complete service health details".
- Settings**: Links para "Zones" e "Console Experiments".
- Additional Information**: Links para "VPC Documentation", "All VPC Resources", "Forums" e "Report an Issue".
- AWS Network Manager**: Descrição: "AWS Network Manager provides tools and features to help you".

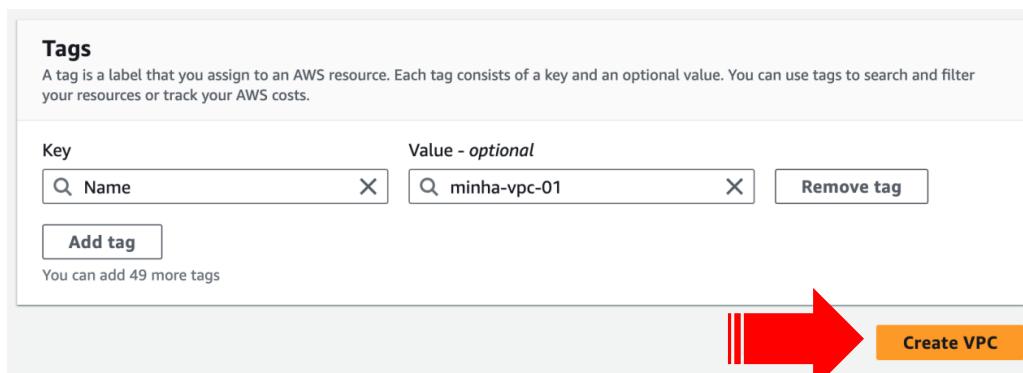
Por padrão, a AWS disponibiliza uma VPC por região, mas iremos criar uma VPC.

The screenshot shows the AWS VPC dashboard with the URL [voclabs/user3047831=Testar\\_aluno @ 6374-2359-2261](#). On the left, there's a sidebar with options like VPC dashboard, EC2 Global View, Filter by VPC, and a Virtual private cloud section with Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, and Managed prefix lists. The main area is titled 'Your VPCs (1) Info' and shows one VPC entry: Name - vpc-0c9618cf78e32536a, VPC ID - vpc-0c9618cf78e32536a, State - Available, IPv4 CIDR - 172.31.0.0/16, and IPv6 - -. A large red arrow points to the 'Create VPC' button in the top right of the main panel.

The screenshot shows the 'Create VPC' wizard. Step 1: VPC settings. It has a title 'Create VPC Info'. Below it, a sub-section 'Resources to create Info' with a note 'Create only the VPC resource or the VPC and other networking resources.' Two radio buttons are shown: 'VPC only' (selected) and 'VPC and more'. A 'Name tag - optional' field contains 'minha-vpc-01'. Another sub-section 'IPv4 CIDR block Info' shows '10.0.0.0/24' in a text input field with a note 'CIDR block size must be between /16 and /28.' Below this are radio buttons for 'IPv4 CIDR manual input' (selected) and 'IPAM-allocated IPv4 CIDR block'. The final section 'Tenancy Info' shows a dropdown menu set to 'Default'.

Utilizaremos um endereçamento padrão de classe A, com uma máscara de sub rede /24 o que nos permite criar 128 IPs. Note que a AWS limita entre uma faixa de /16 e /28

This is a continuation of the 'Create VPC' wizard from the previous screenshot, showing the completed configuration. The 'IPv4 CIDR' field now contains '10.0.0.0/24'. The 'IPv6 CIDR block' section is still set to 'No IPv6 CIDR block'. The 'Tenancy' section remains at 'Default'.



**Tags**

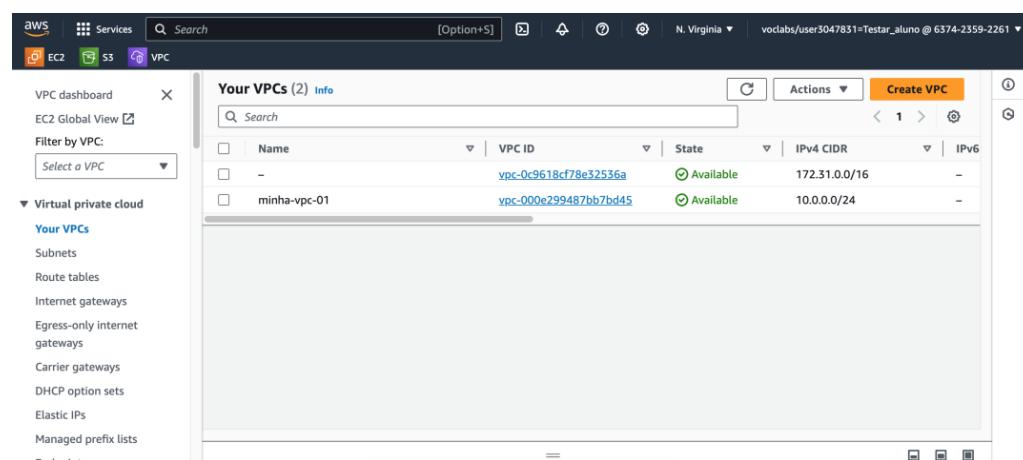
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Name	minha-vpc-01

**Add tag**

You can add 49 more tags

**Create VPC**

Your VPCs (2) Info

Name	VPC ID	State	IPv4 CIDR	IPv6
-	vpc-0c9618cf78e32536a	Available	172.31.0.0/16	-
minha-vpc-01	vpc-000e299487bb7bd45	Available	10.0.0.0/24	-

Agora, criaremos algumas sub redes para associar à essa VPC. Lembrando que para a divisão dos IPs podemos usar uma calculadora de sub redes

## Visual Subnet Calculator

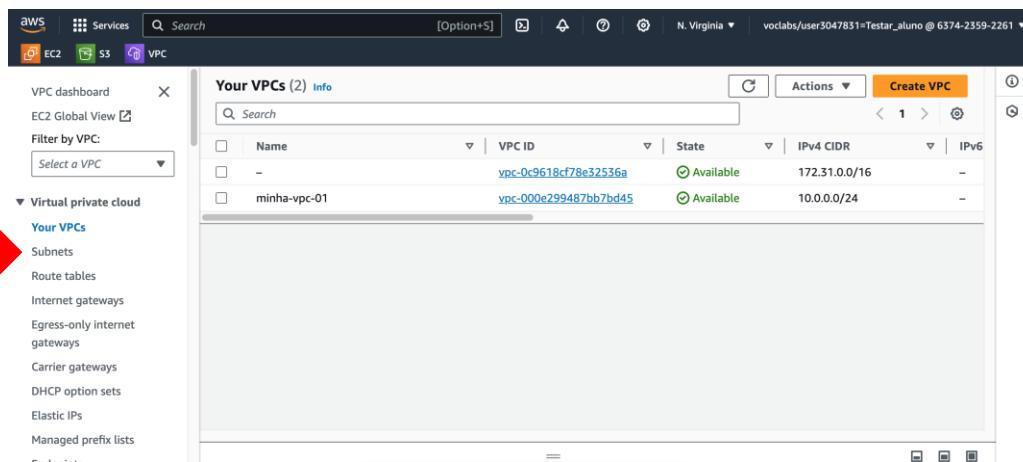
Enter the network you wish to subnet:

Network Address	Mask bits
10.0.0.0	/24
<input type="button" value="Update"/> <input type="button" value="Reset"/>	

Show columns:  Subnet address  Netmask  Range of addresses  Useable IPs  Hosts  Divide  Join

Click below to split and join subnets.  
If you wish to save this subnetting for later, bookmark [this hyperlink](#).

Subnet address	Range of addresses	Useable IPs	Hosts	Divide	Join
10.0.0.0/25	10.0.0.0 - 10.0.0.127	10.0.0.1 - 10.0.0.126	126	<input type="button" value="Divide"/>	<input type="button" value="Join"/>
10.0.0.128/25	10.0.0.128 - 10.0.0.255	10.0.0.129 - 10.0.0.254	126	<input type="button" value="Divide"/>	<input type="button" value="Join"/>



Your VPCs (2) Info

Name	VPC ID	State	IPv4 CIDR	IPv6
-	vpc-0c9618cf78e32536a	Available	172.31.0.0/16	-
minha-vpc-01	vpc-000e299487bb7bd45	Available	10.0.0.0/24	-

The screenshot shows the AWS VPC Subnets page. On the left, there's a sidebar with options like EC2, S3, and VPC. The main area is titled 'Subnets (6) Info' and lists six subnets with columns for Name, Subnet ID, State, and VPC. A red arrow points to the orange 'Create subnet' button at the top right of the table.

Name	Subnet ID	State	VPC
-	subnet-0af8100dbdd84e1d3	Available	vpc-0c9618cf78e32536a
-	subnet-0fdadfbff292654f	Available	vpc-0c9618cf78e32536a
-	subnet-004327ab697136c16	Available	vpc-0c9618cf78e32536a
-	subnet-028040b439f8086d3	Available	vpc-0c9618cf78e32536a
-	subnet-071364c1a286178ae	Available	vpc-0c9618cf78e32536a
-	subnet-0b2510e592bb0992a	Available	vpc-0c9618cf78e32536a

This screenshot shows the 'Create subnet' wizard. The first step is 'VPC'. It has a dropdown for 'VPC ID' containing 'vpc-000e299487bb7bd45 (minha-vpc-01)'. Below it is a section for 'Associated VPC CIDRs' with an input field containing '10.0.0.0/24'.

This screenshot shows the 'Subnet settings' step. It has a heading 'Subnet 1 of 1'. Under 'Subnet name', there's a text input with 'sub-rede-publica'. Under 'Availability Zone', there's a dropdown with 'US East (N. Virginia) / us-east-1a'.

### Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

#### Subnet 1 of 1

**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.

10.0.0.0/24

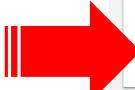
**IPv4 subnet CIDR block**  
10.0.0.0/25 128 IPs

< > ^ ^

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/> <input type="button" value="X"/>	<input type="text" value="sub-rede-publica"/> <input type="button" value="X"/>
<input type="button" value="Remove"/>	

Add new tag  
You can add 49 more tags.


**Subnet 2 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](#)**

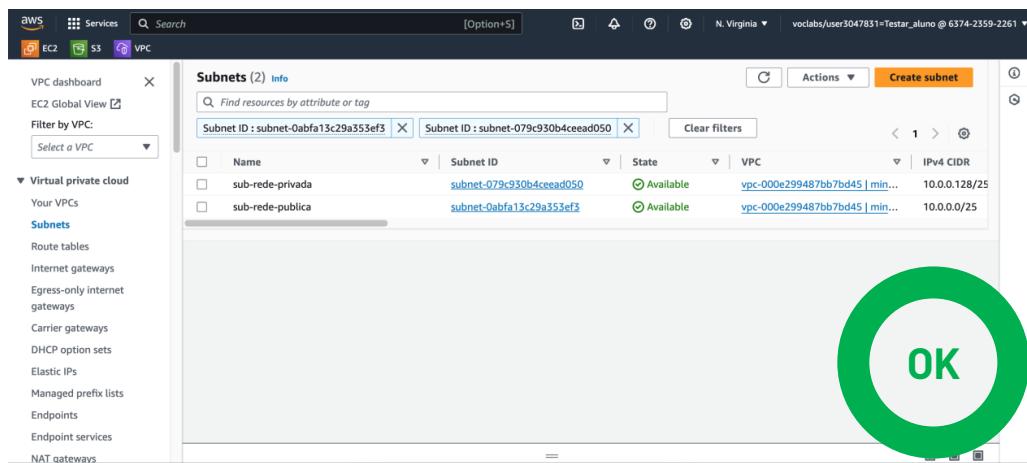
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

**IPv4 subnet CIDR block**

128 IPs

&lt; &gt; ^ ^

**Tags - optional**



## Provisionamento instância em sub redes

Agora temos duas sub redes, uma privada e uma pública. Podemos então provisionar duas instâncias, uma em cada sub rede para que possamos realizar os testes de acesso

The image contains two screenshots of the AWS EC2 interface. The top screenshot shows the 'Services' search results with a red arrow pointing to the 'EC2' service. The bottom screenshot shows the 'Instances' page with a red arrow pointing to the 'Launch instances' button. Both screenshots show the AWS navigation bar and search bar at the top.

[EC2](#) > [Instances](#) > Launch an instance

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

Name

ec2-pública

[Add additional tags](#)

### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

*Search our full catalog including 1000s of application and OS images*

#### Quick Start



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

#### Amazon Machine Image (AMI)

[Ubuntu Server 22.04 LTS \(HVM\), SSD Volume Type](#)

ami-0c7217cdde317cfec (64-bit (x86)) / ami-05d47d29a4c2d19e1 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

#### Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-12-07

#### Architecture

64-bit (x86)

#### AMI ID

ami-0c7217cdde317cfec

[Verified provider](#)

### ▼ Instance type [Info](#) | [Get advice](#)

#### Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true  
On-Demand Windows base pricing: 0.0162 USD per Hour  
On-Demand SUSE base pricing: 0.0116 USD per Hour  
On-Demand RHEL base pricing: 0.0716 USD per Hour  
On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

All generations

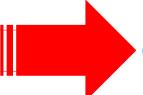
[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

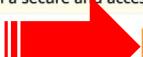
**▼ Key pair (login) [Info](#)**

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select  Create new key pair

**Create key pair** 

Key pair name  
Key pairs allow you to connect to your instance securely.  
myssh 

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

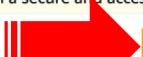
RSA RSA encrypted private and public key pair

ED25519 ED25519 encrypted private and public key pair

Private key file format

.pem For use with OpenSSH

.ppk For use with PuTTY

 When prompted, store the private key in a secure and accessible location on 

**Create key pair**

**▼ Network settings [Info](#)**  Edit

Network [Info](#)  
vpc-0c9618cf78e32536a

Subnet [Info](#)  
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)  
Enable

### ▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-000e299487bb7bd45 (minha-vpc-01)  
10.0.0.0/24

Subnet [Info](#)

subnet-0abfa13c29a353ef3 sub-rede-publica  
VPC: vpc-000e299487bb7bd45 Owner: 637423592261 Availability Zone: us-east-1a IP addresses available: 123 CIDR: 10.0.0.0/25

Create new subnet

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group  Select existing security group

### Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	Add CIDR, prefix list or security <input type="text"/> 0.0.0.0	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 0, 0.0.0.0/0) [Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
Custom TCP	TCP	0
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	Add CIDR, prefix list or security <input type="text"/> 0.0.0.0	e.g. SSH for admin desktop

### ▼ Configure storage [Info](#) [Advanced](#)

1x  8 GiB  Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

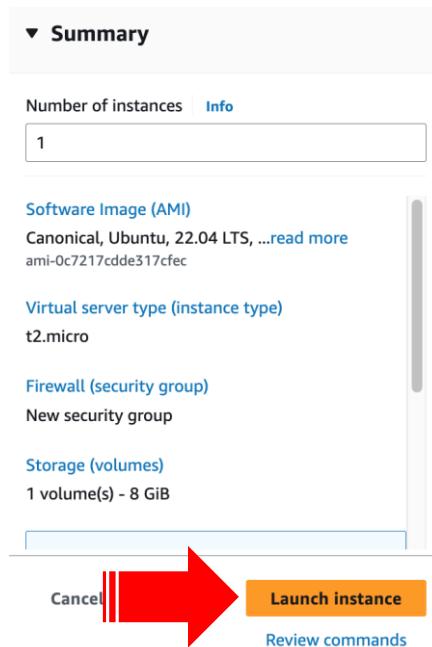
[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)



Provisionamos a instância que estará na sub rede pública, agora provisionaremos a máquina que ficará em uma sub rede privada

EC2 > Instances > Launch an instance

## Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags Info**

Name: ec2-privada [Add additional tags](#)

**Application and OS Images (Amazon Machine Image) Info**

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

**Recent** [Quick Start](#)

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE Linux

[Browse more AMIs](#) Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type ami-0c7217cdde317cfec (64-bit (x86)) / ami-05d47d29a4c2d19e1 (64-bit (Arm)) Virtualization: hvm ENA enabled: true Root device type: ebs	Free tier eligible
--	--------------------

Description  
Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-12-07

Architecture	AMI ID
64-bit (x86)	ami-0c7217cdde317cfec
	<span style="border: 1px solid green; padding: 2px;">Verified provider</span>

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro	Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true	<input type="radio"/> All generations
On-Demand Windows base pricing: 0.0162 USD per Hour	
On-Demand SUSE base pricing: 0.0116 USD per Hour	
On-Demand RHEL base pricing: 0.0716 USD per Hour	
On-Demand Linux base pricing: 0.0116 USD per Hour	

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

myssh	<input type="button" value="Create new key pair"/>
-------	--

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-000e299487bb7bd45 (minha-vpc-01) 10.0.0.0/24	<input type="button" value="Create new VPC"/>
---	---

Subnet [Info](#)

subnet-079c930b4ceead050	sub-rede-privada
VPC: vpc-000e299487bb7bd45 Owner: 637423592261	
Availability Zone: us-east-1a IP addresses available: 123 CIDR: 10.0.0.128/25	

Auto-assign public IP [Info](#)

Disable
---------

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

<input type="radio"/> Create security group	<input checked="" type="radio"/> Select existing security group
---	---

Common security groups [Info](#)

Select security groups	<input type="button" value="Compare security group rules"/>
launch-wizard-4 sg-096bec2517d868b00 X	

VPC: vpc-000e299487bb7bd45

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

**Configure storage** [Info](#) [Advanced](#)

1x  GiB  Root volume (Not encrypted)

[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

[⟳ Click refresh to view backup information](#) [G](#)

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

**Summary**

Number of instances [Info](#)  
1

Software Image (AMI)  
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)  
ami-0c7217cdde317cfec

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
launch-wizard-4

Storage (volumes)  
1 volume(s) - 8 GiB

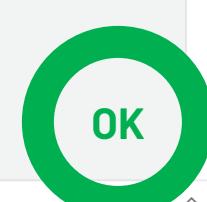
[Cancel](#) [Launch instance](#)



**Instances (2) [Info](#)**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
ec2-pública	i-045b76021c54d238c	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1a
ec2-privada	i-0022e7afbda84fc98	Running	t2.micro	0/2 checks passed	<a href="#">View alarms +</a>	us-east-1a

**Select an instance**



Vamos observar os IPv4 de cada uma das máquinas

Para a EC2 pública

**Instances (1/2) Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/> ec2-pública	i-045b76021c54d238c	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<a href="#">View alarms</a> +	us-east-1a
<input type="checkbox"/> ec2-privada	i-0022e7afbda84fc98	<span>Running</span>	t2.micro	<span>Initializing</span>	<a href="#">View alarms</a> +	us-east-1a

**Instance: i-045b76021c54d238c (ec2-pública)**

**Details** | Status and alarms New | Monitoring | Security | Networking | Storage | Tags

**Instance summary** [Info](#)

Instance ID: [i-045b76021c54d238c \(ec2-pública\)](#)

Public IPv4 address: [54.226.249.155 \[open address\]](#)

Private IPv4 addresses: [10.0.0.74](#)

Para a EC2 privada

**Instances (1/2) Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/> ec2-pública	i-045b76021c54d238c	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<a href="#">View alarms</a> +	us-east-1a
<input checked="" type="checkbox"/> ec2-privada	i-0022e7afbda84fc98	<span>Running</span>	t2.micro	<span>Initializing</span>	<a href="#">View alarms</a> +	us-east-1a

**Instance: i-0022e7afbda84fc98 (ec2-privada)**

**Details** | Status and alarms New | Monitoring | Security | Networking | Storage | Tags

**Instance summary** [Info](#)

Instance ID: [i-0022e7afbda84fc98 \(ec2-privada\)](#)

Public IPv4 address: -

Private IPv4 addresses: [10.0.0.225](#)

Como habilitamos um IP de saída, a EC2 pública poderá ter um acesso à internet, vamos testá-lo com a conexão SSH

```
[ 10:44 ] [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
$ ssh -i myssh.pem ubuntu@54.226.249.155
ssh: connect to host 54.226.249.155 port 22: Operation timed out
[ 10:46 ] [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
$
```

**Ele não cria acesso à EC2! Por que isso?**

Porque, apesar desta máquina ter um IP público, a minha sub rede não tem acesso à internet, ela não está exposta à internet. Para isso precisaremos configurar um elemento de rede que expõem a rede, que é o internet gateway!

## Configurando Internet Gateway e Route Table

The screenshot shows the AWS VPC dashboard with a search bar at the top containing 'internet gateway'. A red arrow points from the left towards the search results. The results are categorized under 'Features' and 'Services'. Under 'Features', 'Internet gateway' is listed as a 'VPC feature'. Under 'Services', 'AWS IoT FleetWise' is listed.

The screenshot shows the 'Internet gateways' list page. A red arrow points from the right towards the 'Create internet gateway' button. The table lists one item: 'igw-05250eaa58b936059' with state 'Attached' and VPC ID 'vpc-0c9618cf78e32556a'.

### Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

**Internet gateway settings**

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

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="meu-ig-01"/> <input type="button" value="Remove"/>

You can add 49 more tags.

VPC > Internet gateways > igw-0a05c9c7ba9fbbe44 / meu-ig-01

**Details** **Info**

Internet gateway ID	igw-0a05c9c7ba9fbbe44	State	Detached	VPC ID	-
Tags			Owner		
			63742351		

**Actions**

- Attach to VPC
- Detach from VPC
- Manage tags
- Delete

VPC > Internet gateways > Attach to VPC (igw-0a05c9c7ba9fbbe44) [Info](#)

### VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

**Available VPCs**  
Attach the internet gateway to this VPC.

**AWS Command Line Interface command**

**Attach internet gateway**

VPC > Internet gateways > igw-0a05c9c7ba9fbbe44 / meu-ig-01

**Details** **Info**

Internet gateway ID	igw-0a05c9c7ba9fbbe44	State	Attached	VPC ID	vpc-000e299487bb7bd45   minha-vpc-01	Owner	637423592261
Tags			Manage tags				
			< 1 > @				

**Vamos testar novamente. Continua não indo!**

Falta eu "ensinar" a rota da minha sub rede para o internet gateway, fazemos isso com uma tabela de rota (route table).

The screenshot shows the AWS VPC Features page. A red arrow points to the 'Route table' item under the 'Features' section. The 'Route table' item is highlighted with a purple icon and the text 'VPC feature'. Other items listed include 'Transit Gateway route tables', 'Local gateway route tables', and 'Route 53 dashboard'.

The screenshot shows the AWS Route tables list page. A red arrow points to the 'Create route table' button in the top right corner of the main content area. The table lists two existing route tables: 'rtb-089193038c58ad98a' and 'rtb-05e04adb38a3682e8', both associated with 'vpc-0c9e'.

The screenshot shows the 'Create route table' wizard. The first step, 'Route table settings', includes fields for 'Name - optional' (set to 'rt-publica') and 'VPC' (set to 'vpc-000e299487bb7bd45 (minha-vpc-01)'). The second step, 'Tags', shows a single tag 'Name: rt-publica' and a 'Create route table' button at the bottom right.

Como essa tabela de rota vai apontar para a internet eu vou associá-la à minha rede pública

The screenshot shows the AWS VPC Route Tables interface. A red arrow points from the left sidebar to the 'Route tables' section. Another red arrow points from the 'Subnet associations' tab to the 'Edit subnet associations' dialog. A third red arrow points from the 'Edit routes' dialog back to the main route table page.

**Route tables**

**rtb-0fad5af79ed4f1c21 / rt-publica**

**Details**

Route table ID	rtb-0fad5af79ed4f1c21	Main	No	Explicit subnet associations	Edge associations
VPC	vpc-000e299487bb7bd45   minha-vpc-01	Owner ID	657423592261		

**Subnet associations**

**Explicit subnet associations (0)**

**Edit subnet associations**

**Available subnets (1/2)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
sub-rede-publica	subnet-0abfa13c29a353ef3	10.0.0.0/25	-	Main (rtb-05e0-)

**Selected subnets**

subnet-0abfa13c29a353ef3 / sub-rede-publica

**Save associations**

**Routes**

**Routes (1)**

Destination	Target	Status	Propagated
10.0.0.0/24	local	Active	No

**Edit routes**

**Destination**: 10.0.0.0/24    **Target**: local    **Status**: Active    **Propagated**: No

**Add route**

**Save changes**

Pronto, agora minha tabela de rotas determinou que qualquer IP fora do range de 10.0.0.0/24 será resolvido na Internet! Vamos testar, e vemos que agora temos acesso SSH à máquina!!

```
[ 11:06 ] [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
$ ssh -i myssh.pem ubuntu@54.226.249.155
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Sun Feb 25 14:06:16 UTC 2024

System load: 0.0          Processes:         96
Usage of /: 20.5% of 7.57GB Users logged in: 0
Memory usage: 20%          IPv4 address for eth0: 10.0.0.74
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-74:~$
```



Mas este acesso é a máquina pública, como podemos acessar a máquina privada? Iremos fazer uma cópia de segurança com o comando **scp**

**scp -i chave\_pem <arquivo\_origem> <local\_destino>**

```
● ○ ● sshkey — eduardoverri@Eduardos-MacBook-Pro — zsh — 67x27
...untu@54.226.249.155 ..esktop/sshkey ..esktop/sshkey +
[ 11:51 ] [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
[ $ scp -i ./myssh.pem /Users/eduardoverri/Desktop/sshkey/myssh.pem ]
ubuntu@54.226.249.155:/home/ubuntu/.ssh/myssh.pem
myssh.pem          100% 1674   11.7KB/s  00:00
[ 11:51 ] [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
$
```

Acessando a EC2 na rede pública (tag: ec2-pública)

```
● ○ ● sshkey — ubuntu@ip-10-0-0-74: ~/.ssh — ssh -i myssh.pem ubuntu@54...
...untu@54.226.249.155 ..esktop/sshkey ..esktop/sshkey -
ubuntu@ip-10-0-0-74:~/.ssh$ ll
total 16
drwx----- 2 ubuntu ubuntu 4096 Feb 25 14:51 .
drwxr-x--- 5 ubuntu ubuntu 4096 Feb 25 14:40 ..
-rw----- 1 ubuntu ubuntu 387 Feb 25 13:31 authorized_keys
-r----- 1 ubuntu ubuntu 1674 Feb 25 14:51 myssh.pem
ubuntu@ip-10-0-0-74:~/.ssh$
```

Se quisermos conectar na instância privada, podemos através da pública com ssh! Conceito de jump server ou bastião (bastion host)

```
...@ip-10-0-0-225:~ ssh -i myssh.pem ubuntu@54.226.249.155
[ubuntu@ip-10-0-0-74:~/ssh$ ssh -i myssh.pem ubuntu@10.0.0.225
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 System information as of Sun Feb 25 14:58:17 UTC 2024

 System load: 0.0          Processes:                 94
 Usage of /:   20.5% of 7.57GB  Users logged in:      0
 Memory usage: 20%          IPv4 address for eth0: 10.0.0.225
 Swap usage:   0%

 Expanded Security Maintenance for Applications is not enabled.

 0 updates can be applied immediately.

 Enable ESM Apps to receive additional future security updates.
 See https://ubuntu.com/esm or run: sudo pro status

 The list of available updates is more than a week old.
 To check for new updates run: sudo apt update

 Last login: Sun Feb 25 14:58:18 2024 from 10.0.0.74
 To run a command as administrator (user "root"), use "sudo <command>".
 See "man sudo_root" for details.

ubuntu@ip-10-0-0-225:~$
```

Mas temos um problema, bloqueamos o acesso à essa VM de fora da rede, mas e para atualizar os pacotes de nossa instância? E criarmos um CI/CD? Precisaremos acessar a internet, de dentro, mas não permitir que de fora seja acessada. Nesses casos precisaremos de um NAT Gateway, que permite a saída para a Internet, mas bloqueia a entrada da Internet.

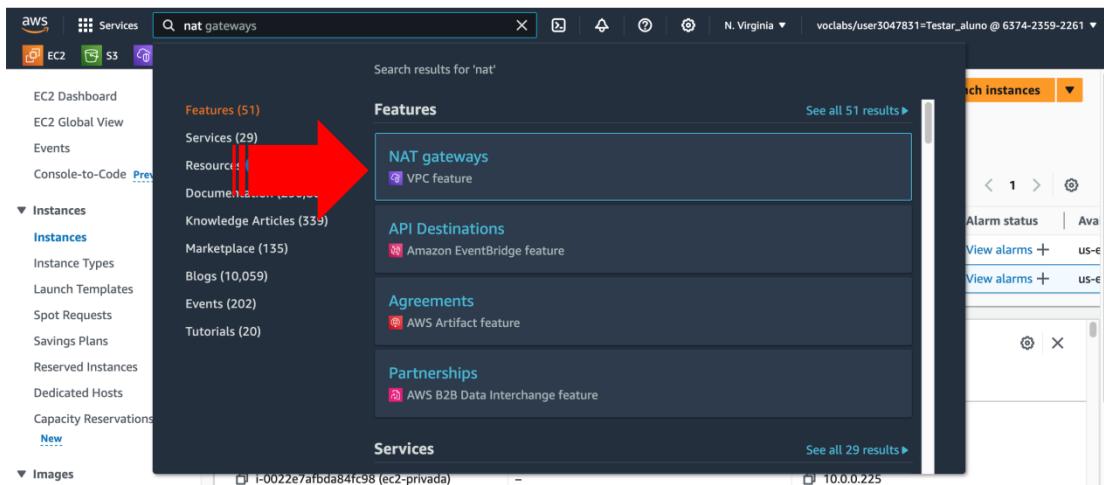
Ao tentar acessar de fora não temos acesso

```
sshkey — eduardoverri@Eduardos-MacBook-Pro — zsh — 104x25
...h -i myssh.pem ubuntu@54.226.249.155 ..esktop/sshkey ..esktop/sshkey
[ 12:00 ] [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
$ ssh -i myssh.pem ubuntu@10.0.0.225
ssh: connect to host 10.0.0.225 port 22: Operation timed out
[ 12:02 ] [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
$
```

Ao tentar realizar um `sudo apt update`, não funciona!

```
sshkey --ubuntu@ip-10-0-0-225: ~ - ssh -i myssh.pem ubuntu@54.226.249.155 - 104x25
...h -i myssh.pem ubuntu@54.226.249.155 ..esktop/sshkey ..esktop/sshkey
iate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c04:b8fe:122c:bb55:6b84). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c05:178c:ad29:43bf:eb48). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c05:178c:ad29:43bf:eb48). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c00:7447:9a97:fa56:c9d2). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c00:7447:9a97:fa56:c9d2). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c00:7447:9a97:fa56:c9d2). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c01:32a9:41b2:cf3a:904a). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c01:ed0c:fdfa:1470:afc0). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c02:b55:260f:8030:b812). - connect (101: Network is unreachable)
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/jammy-security/InRelease Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::102). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::103). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::103). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::103). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::103). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::103). - connect (101: Network is unreachable) Could not connect to security.ubuntu.com:80 (185.125.190.39), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.81), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.82), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.83), connection timed out Could not connect to security.ubuntu.com:80 (185.125.190.36), connection timed out
W: Some index files failed to download. They have been ignored, or old ones used instead.
ubuntu@ip-10-0-0-225:$
```

## Configurando NAT Gateway e Route Table



### NAT gateway settings

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

The name can be up to 256 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

**Connectivity type**  
Select a connectivity type for the NAT gateway.  
 Public  
 Private

**Elastic IP allocation ID** Info  
Assign an Elastic IP address to the NAT gateway.

**Additional settings** Info

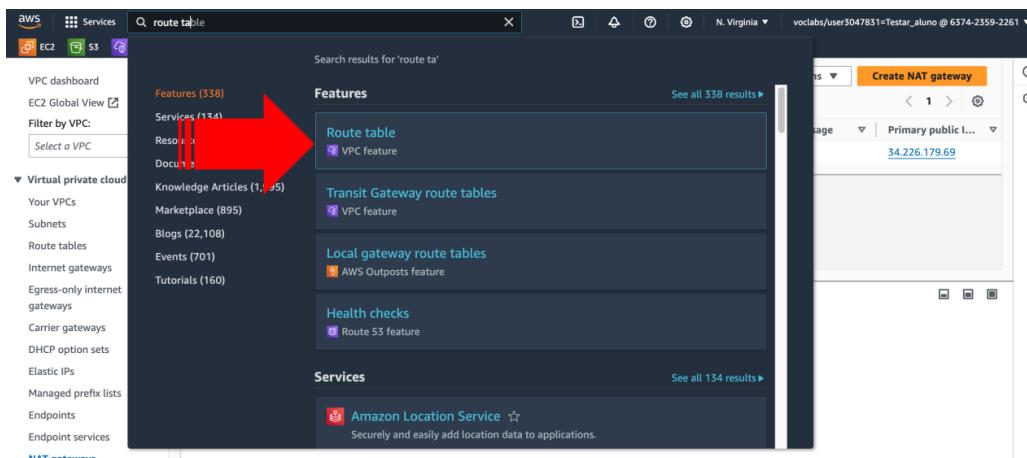
Vamos alocar o NAT gateway na sub rede pública, pois ele terá acesso à Internet. Iremos também alocar um IP elástico para ele, caso tivéssemos criado um IP elástico poderíamos alocar o criado. Ao final clicamos em **Create NAT gateway**.

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="nat-01"/> <input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>	
You can add 49 more tags.	

Só que da mesma forma que criamos um tabela de rota entre a sub rede pública e o Internet Gateway, precisaremos criar uma tabela de rota entre a sub rede privada e o NAT gateway!



### Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

**Route table settings**

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

**VPC**  
The VPC to use for this route table.

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="rt-privada"/> <input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>	

You can add 49 more tags.

Da mesma forma com o Internet Gateway, preciso associar as sub redes e definir as rotas!

### Edit subnet associations

Change which subnets are associated with this route table.

**Available subnets (1/2)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> sub-rede-privada	<a href="#">subnet-079c930b4ceead050</a>	10.0.0.128/25	-	Main (rtb-05e04adb38a3682e8)
<input type="checkbox"/> sub-rede-publica	<a href="#">subnet-0abfa13c29a353ef3</a>	10.0.0.0/25	-	rtb-0fad5af79ed4f1c21 / rt-publica

**Selected subnets**

The screenshot shows the 'Edit routes' section of the AWS VPC Route Tables. A red arrow points to the 'Add route' button at the bottom left. Another red arrow points to the 'Save changes' button at the bottom right. The table lists a route for '10.0.0.0/24' with a target of 'NAT Gateway'.

Destination	Target	Status	Propagated
10.0.0.0/24	local Q local	Active	No
0.0.0.0/0	NAT Gateway nat-00f70ff30e0a93b13	-	No

E agora ao rodar `sudo apt update` minha máquina que está numa sub rede privada tem acesso à Internet! O NAT Gateway permite o tráfego outbound, bloqueando o tráfego inbound de Internet à nossa VM. Mas colocamos ele na sub rede pública pois ele tem acesso à Internet.

```
sshkey — ubuntu@ip-10-0-0-225: ~ -- ssh -i myssh.pem ubuntu@54.226.249.155 — 104x25
...h -i myssh.pem ubuntu@54.226.249.155 ..esktop/sshkey ..esktop/sshkey +
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [16 B]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [24.3 kB]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [16.5 kB]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [644 B]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [16 B]
Get:29 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1192 kB]
Get:30 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [217 kB]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [1452 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [239 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [842 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [161 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [16.8 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [37.1 kB]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [7476 B]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [260 B]
Fetched 29.7 MB in 6s (5400 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
76 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-10-0-0-225:~$
```

OK