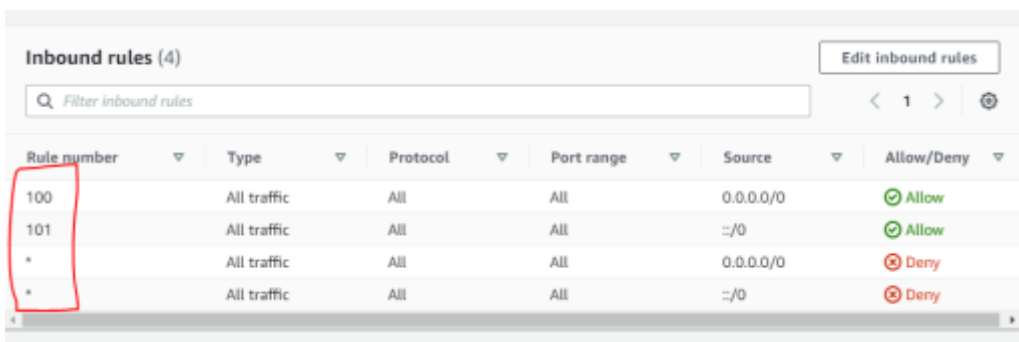


10 - CONFIGURANDO ACL

ACL = Access list

- Cria permissões ou bloqueios referentes a um determinado serviço ou acesso.
- Temos um tipo de acl mas que pode ter 2 formatos:
 - Inbound (entrando)
 - Outbound (saindo)
- Elas trabalham com linhas:
 - 100 -> permitir ping
 - 150 -> permitir SSH
 - 200 -> Deny HTTP
- Todo trafego que entra tem que sair, logo, possuímos regras de entradas e saidas.
- As ACLs são sempre executadas de cima para baixo, e ao encontrar o que procura, para no caminho.
- Se permitirmos em uma linha e depois bloquear, na proxima linha, o que será levado em conta eh a primeira linha.
- As Acls estão dentro de VPC
- Ja Existem duas ACLS criadas, uma do VPC padrão (default) e outra criada quando criamos o VPC do clube cloud;
- Essa ACL possui rotas de inbound e rotas de Outbound.
- Nas rotas de inbound



Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

- Temos uma regra de numero 100 onde, ela permite qualquer trafego, com qualquer tipo de protocolo, para qualquer numero de porta, de qualquer destino.

- A regra 101 é a mesma coisa, so que para o IPV6

- nas Outbound rules

acl-02e8b5ba41abe9969 / ACL ClubeCloud

Details | Inbound rules | **Outbound rules** | Subnet associations | Tags

Outbound rules (4) Edit outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
101	All traffic	All	All	::/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	✗ Deny
*	All traffic	All	All	::/0	✗ Deny

- falam a mesma coisa que as inbounds rules.

- è por isso que mesmo não tralbahando ,com acls, conseguimos fazer o ping funcionar e o SSH tbm.

```
C:\WINDOWS\system32\cmd.exe - ping 52.37.55.131 -t

Resposta de 52.37.55.131: bytes=32 tempo=234ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=246ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=234ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=237ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=239ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=238ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=241ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=234ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=243ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=240ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=239ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=239ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=229ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=241ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=241ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=237ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=247ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=238ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=237ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=236ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=236ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=250ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=233ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=220
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=220

ec2-user@ip-10-1-1-247:~
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Thu Jun  3 13:28:50 2021 from 179.105.155.6

  _ | _ | _ )
  _ | ( _ /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
6 package(s) needed for security, out of 17 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-1-1-247 ~]$
```

- A partir do momento que criamos uma subnet, cria um vpc, e essa subnet é associada a internet, as duas subnets associadas vem para a ACL Default.

- Logo toda subnet que criamos virá para a ACL padrão.
- O que a amazon quer é que a ACL ja esteja criada, então voce não irá criar uma subnet e depois criar uma acl e depois voce permite o trafego e bloqueia. Ao criar a subnet, automaticamente são adicionadas a ACL padrão.
- Vamos criar uma ACL nossa e dar um nome a ela.

Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

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

VPC
VPC to use for this network ACL.

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

Remove

Add new tag

You can add 49 more tags.

Cancel

Create network ACL

- Perceba que nada aconteceu ao criarmos a ACL.
- Nossa ACL criada não possui nenhuma regra, somente o bloqueio q veio por default, tanto na inbound quanto na outbound.

acl-0ece8e4e1322f9de9 / ClubeCloud-ACL

Details **Inbound rules** Outbound rules Subnet associations Tags

Inbound rules (2)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	:::0	Deny

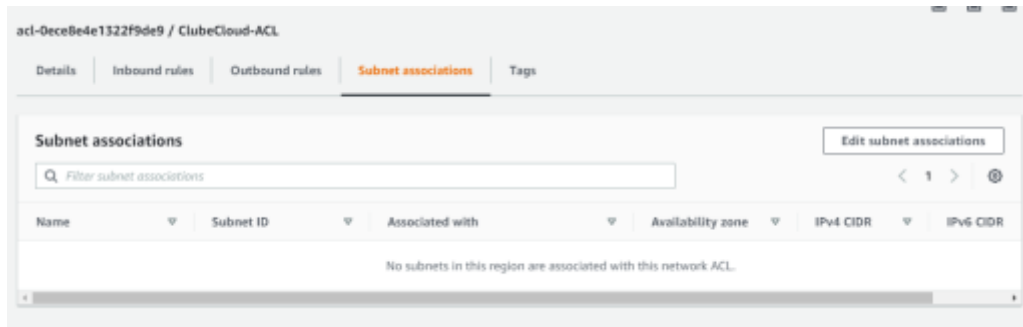
- Essas são regras padrões de bloqueio, agem como se fossem um firewall, e o firewall age da seguinte maneira:

- Bloqueia tudo e permite depois.

- Logo ao criarmos a ACL ela vem por padrão bloqueada.

- O nosso tráfego ainda está rodando porque não temos nenhuma rede associada a essa ACL ainda.

- Nossas subnets estão associadas a ACL padrão.



- Vamos fazer algo que não devemos fazer em um ambiente de produção, vamos jogar nossas subnets dentro da ACL que criamos. Vamos com certeza perder acesso, pois não tem nenhuma regra associada.

- O processo de migração de ACL seria:

- 1- ver a acl que está funcionando.

- 2- copiar todas as regras.

- 3 - Aplicar para a ACL nova

- 4 - E depois fazer a associação.

- Vamos fazer o contrário para verificar o servidor deixando de funcionar.

- Adicionando as subnets na ACL

Edit subnet associations [Info](#)

Change which subnets are associated with this network ACL.

Available subnets (1/2)

Filter subnet associations

< 1 > ⌵

<input type="checkbox"/>	Name	Subnet ID	Associated with	Availability zone	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	clubcloud-Sales	subnet-004a70ec099737e3d	acl-02e8b5ba41abe9969 / ACL ClubeCloud	us-west-2a	10.1.1.0/24	-
<input type="checkbox"/>	clubcloud-Finance	subnet-0646ac4cb579bcdb8	acl-02e8b5ba41abe9969 / ACL ClubeCloud	us-west-2b	10.1.2.0/24	-

Selected subnets

subnet-004a70ec099737e3d / clubcloud-Sales X

Cancel

Save changes

acl-0ece8e4e1322f9de9 / ClubeCloud-ACL

Details Inbound rules Outbound rules **Subnet associations** Tags

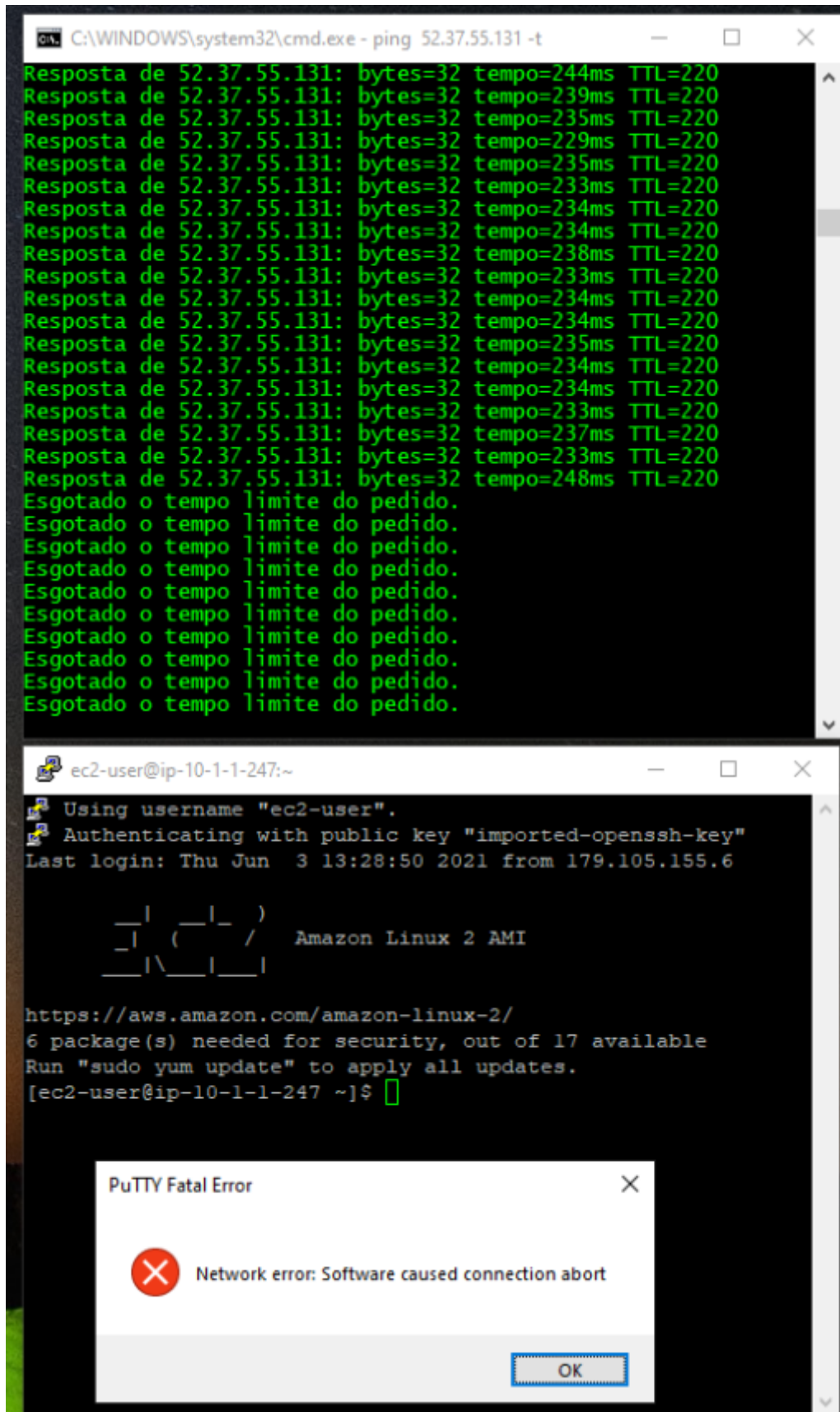
Subnet associations (1)

Filter subnet associations

Edit subnet associations

< 1 > ⌵

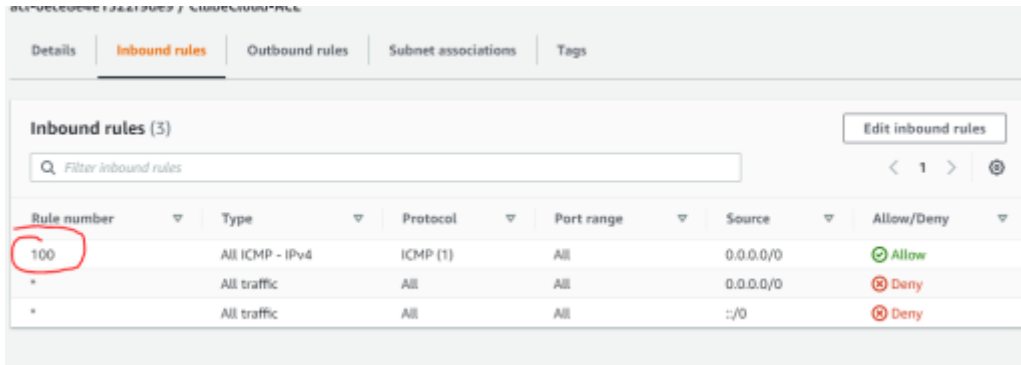
Name	Subnet ID	Associated with	Availability zone	IPv4 CIDR	IPv6 CIDR
clubcloud-Sales	subnet-004a70ec099737e3d	acl-0ece8e4e1322f9de9 / ClubeCloud-ACL	us-west-2a	10.1.1.0/24	-



- Perdemos tanto o acesso ao servidor publico quanto o acesso ao SSH

- Vamos configurar isso

1- editar rotas inbound



Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

- O trafego agora ja pode entrar para o servidor

- A amazon fala que é uma boa pratica começar com a regra de numero 100

- O ping ainda não retornou pois so alteramos a inbound, ou seja, so temos o trafego com permissão de entrada e não de saída.

- Logo todo trafego que voce coloca in voce tbm tem que colocar no out.

```
Esgotado o tempo limite do pedido.  
Esgotado o tempo limite do pedido.  
Esgotado o tempo limite do pedido.  
Esgotado o tempo limite do pedido.  
Esgotado o tempo limite do pedido.  
Esgotado o tempo limite do pedido.  
Resposta de 52.37.55.131: bytes=32 tempo=247ms TTL=221  
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221  
Resposta de 52.37.55.131: bytes=32 tempo=239ms TTL=221  
Resposta de 52.37.55.131: bytes=32 tempo=238ms TTL=221
```

- Automaticamente apos ser colocada a regra de outbound o ping retorna a funcionar.

-2 - Vamos agora corrigir nosso problema de SSH

- Todo problema de SSH é a mesma coisa que ICMP

2.1 - editando inbound rules

- Vamos adicionar uma nova regra de numero 200, colocar de 100 para 200, nos da um range de trabalho posterior para novas regras.

- Criamos uma regra TCP na porta 22 (SSH)

Edit inbound rules [info](#)

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number info	Type info	Protocol info	Port range info	Source info	Allow/Deny info	
100	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Allow	Remove
200	Custom TCP	TCP (6)	22	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	
*	All traffic	All	All	::/0	Deny	

[Add new rule](#) [Sort by rule number](#)

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

- Lembrando que ainda não irá funcionar pois precisamos criar a mesma regra para o outbound rules

acl-0ece8e4e1322f9de9 / ClubeCloud-ACL

[Details](#) [Inbound rules](#) [Outbound rules](#) [Subnet associations](#) [Tags](#)

Inbound rules (4) [Edit inbound rules](#)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Allow
200	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

- Mesmo colocando regras de SSH no inbound e outbound rules, o SSH ainda não esta conectando, existe outro pequeno problema...

- O nosso servidor sai para a internet atraves de um internet gateway, a comunicação entre o servidor e o internet gateway para fazer o acesso a internet, a comunicação entre eles não é atraves de SSH e muito menos atraves de ping, eles utilizam portas especificas para se comunicarem.

- O servidor não sabe que o internet gateway tem comunicação ate agora. Conseguimos passar o ping, mas precisamos de mais informações para utilizar o internet gateway

- na parte de documentação das ACLS vamos encontrar uma parte chamada PORTAS EFEMERAS.

- Entre o servidor e o internet gateway temos que liberar as portas 1024 a 65535, se não os dois não conseguem conversar.

- Voce precisa ter essa regra liberada na sua ACL entre os dois dispositivos.

- Vamos para a ACL > inbound rules

Edit inbound rules [info](#)

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number info	Type info	Protocol info	Port range info	Source info	Allow/Deny info	
<input type="text" value="100"/>	All ICMP - IPv4 ▾	ICMP (1) ▾	All	<input type="text" value="0.0.0.0"/>	Allow ▾	<button>Remove</button>
<input type="text" value="200"/>	SSH (22) ▾	TCP (6) ▾	22	<input type="text" value="0.0.0.0"/>	Allow ▾	<button>Remove</button>
<input type="text" value="300"/>	Custom TCP ▾	TCP (6) ▾	1024-65535	<input type="text" value="0.0.0.0"/>	Allow ▾	<button>Remove</button>
<input type="text" value="*"/>	All traffic ▾	All ▾	All	<input type="text" value="0.0.0.0"/>	Deny ▾	
<input type="text" value="*"/>	All traffic ▾	All ▾	All	<input type="text" value="::/0"/>	Deny ▾	

Add new ruleSort by rule number

CancelPreview changesSave changes

- Precisamos fazer a mesma coisa para rotas de outbound rules

```
C:\WINDOWS\system32\cmd.exe - ping 52.37.55.131 -t

Resposta de 52.37.55.131: bytes=32 tempo=233ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=244ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=240ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=234ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=233ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=234ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=231ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=231ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=231ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=233ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=241ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=230ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=233ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=238ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=239ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=234ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=231ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=232ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=233ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=239ms TTL=221
Resposta de 52.37.55.131: bytes=32 tempo=235ms TTL=221
```

```
ec2-user@ip-10-1-1-247:~

Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Thu Jun  3 14:01:47 2021 from 179.105.155.6

  ____|_____|_____)
  ____|_____|_____/   Amazon Linux 2 AMI
  ____|_____|_____|

https://aws.amazon.com/amazon-linux-2/
6 package(s) needed for security, out of 17 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-1-1-247 ~]$
```

- Agora vemos o SSH e o ping funcionando novamente.
- O mesmo Acontece para HTTP e HTTPS.

as regras para os servidores web são as seguintes:

80 - http

443 - https

- Precisamos filtrar o maximo possivel de trafego com as ACLS

