



SÃO
PAULO
TECH
SCHOOL

Computação e sistemas distribuídos em nuvem

ACL + Security Group

Eduardo Verri

eduardo.verri@sptech.school

Grupo de segurança [Security Group]

Grupo de segurança é como um firewall virtual. Possui regras de segurança de entrada e saída nas quais todo o tráfego de entrada é bloqueado por padrão em privado no AWS EC2.

Não permite protocolo específico ninguém conseguirá acessar nossas instâncias usando este protocolo você pode parar o tráfego usando essa regra por padrão tudo que for negado.

Existem vários grupos de segurança múltiplos em instâncias EC2. Não podemos bloquear um endereço IP específico usando esse grupo de segurança, mas sim usando a lista de acesso à rede. No qual editamos qualquer regra um grupo de segurança com efeito mais rápido.

Lista de controle de acesso à rede

[Network Access Control List]

Network ACL é uma rede padrão modificável. Ele permite todo o tráfego IPv4 de entrada ou saída e aqui criamos um tipo de rede personalizada para toda ou cada rede personalizada ACL nega todo o tráfego de entrada e saída.

Esta rede é a regra de entrada e saída separada e sem estado, com um limite padrão de 20 para ambas as regras e começando com a regra de numeração mais baixa.

Em que todas as sub redes na VPC devem ser combinadas com a ACL da rede, uma sub rede - uma ACL da rede por vez. Ele oferece suporte a regras e regras de negação e opera no nível da sub rede.

Básico sobre Network ACL

- Cada sub rede na sua VPC deve estar associada a uma Network ACL. Se você não associar explicitamente uma sub rede a uma ACL de rede, a sub rede será automaticamente associada à ACL de rede padrão.
- Você pode associar uma Network ACL a diversas sub redes. Entretanto, uma sub rede pode ser associada apenas a uma ACL de rede por vez. Ao associar uma Network ACL a uma sub rede, a associação anterior é removida.
- Uma ACL de rede possui regras de entrada e regras de saída. Cada regra pode permitir ou negar tráfego. Cada regra tem um número de 1 a 32766. As regras são avaliadas em ordem, começando pela regra de número mais baixo, ao decidir se permite ou nega o tráfego. Recomendado criar regras em incrementos (por exemplo, incrementos de 10 ou 100) para poder inserir novas regras posteriormente, se necessário.
- As regras da ACL da rede são avaliadas quando o tráfego entra e sai da sub rede, e não quando é roteado dentro de uma sub rede

Regras Network ACL

Você pode adicionar ou remover regras da ACL de rede padrão ou criar ACLs de rede adicionais para sua VPC. Quando você adiciona ou remove regras de uma rede ACL, as alterações são aplicadas automaticamente às sub redes às quais ela está associada.

- Número da regra. As regras são avaliadas começando pela regra de número mais baixo. Assim que uma regra corresponde ao tráfego, ela é aplicada independentemente de qualquer regra de número mais alto que possa contradizê-la.
- Tipo. O tipo de tráfego; por exemplo, SSH. Você também pode especificar todo o tráfego ou um intervalo personalizado.
- Protocolo. Você pode especificar qualquer protocolo que tenha um número de protocolo padrão. Para obter mais informações, consulte Números de protocolo. Se você especificar ICMP como protocolo, poderá especificar qualquer um ou todos os tipos e códigos ICMP.

Regras Network ACL

- Faixa de porta. A porta de escuta ou intervalo de portas para o tráfego. Por exemplo, 80 para tráfego HTTP.
- Fonte. [Somente regras de entrada] A origem do tráfego (intervalo CIDR).
- Destino. [Somente regras de saída] O destino do tráfego (intervalo CIDR).
- Permite/ negar. Se deve permitir ou negar o tráfego especificado.

Se você adicionar uma regra usando uma ferramenta de linha de comando ou a API do Amazon EC2, o intervalo CIDR será automaticamente modificado para seu formato canônico. Por exemplo, se você especificar 100.68.0.18/18 para o intervalo CIDR, criaremos uma regra com um intervalo CIDR 100.68.0.0/18.

Default Network ACL

A ACL de rede padrão é configurada para permitir que todo o tráfego entre e saia das sub-redes às quais está associada. Cada rede ACL também inclui uma regra cujo número de regra é um asterisco (*). Esta regra garante que se um pacote não corresponder a nenhuma das outras regras numeradas, ele será negado. Você não pode modificar ou remover esta regra.

Inbound					
Rule #	Type	Protocol	Port range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule #	Type	Protocol	Port range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/vpc-network-acls.html

Security Group vs Network ACL

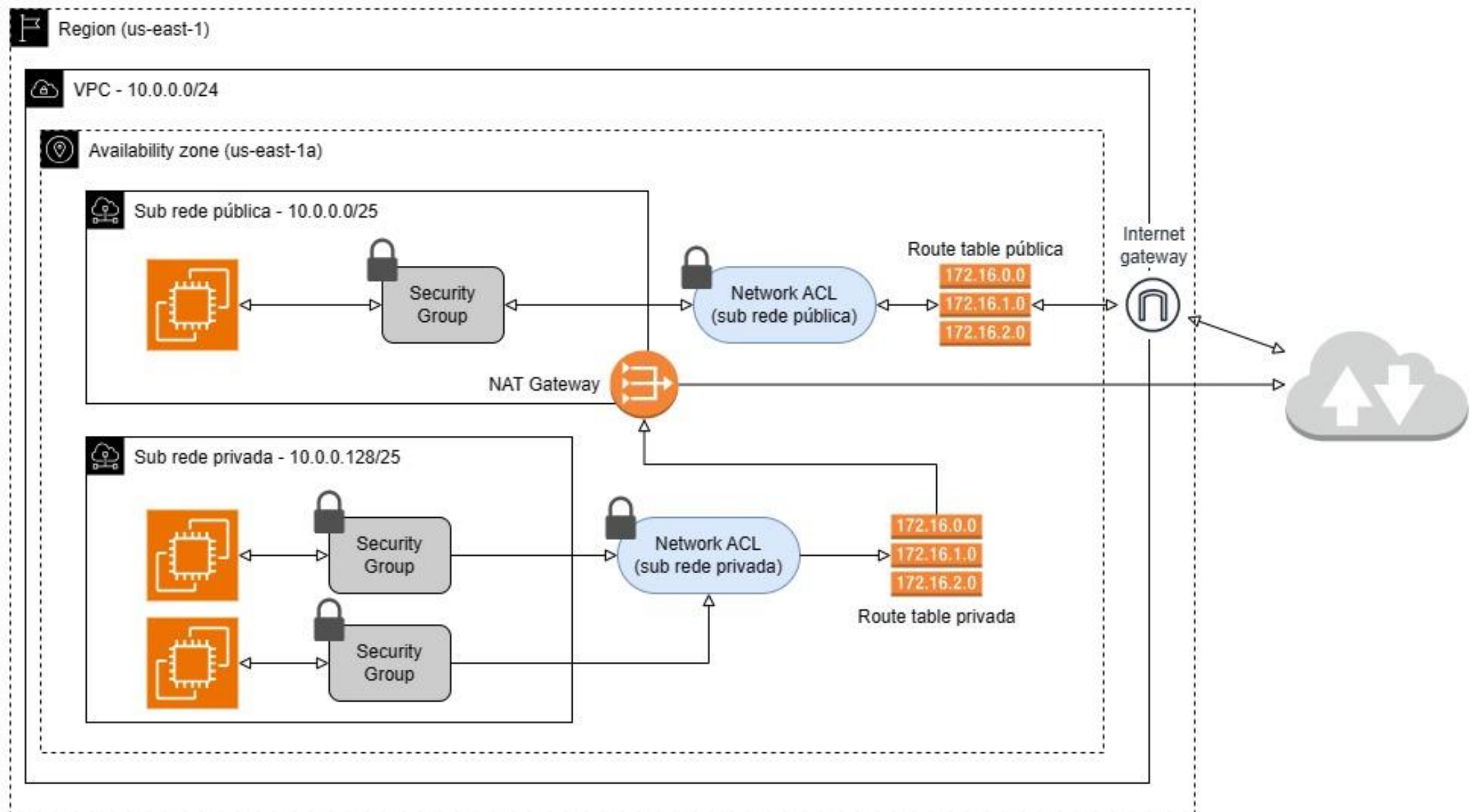
Security Group	Network Access Control List
No grupo de segurança, operamos em nível de instância	Na rede ACL, operamos no nível de sub rede
Suporta apenas regras de permissão	Suporta regras de permissão e regras de negação
É stateful quando criamos uma regra de entrada ou saída	É stateless, o tráfego de retorno deve ser permitido explicitamente
Não podemos bloquear endereços IP específicos	Podemos bloquear endereços IP específicos
Todas as regras são avaliadas antes de decidir permitir o tráfego	As regras são processadas em ordem numérica ao decidir se permitem tráfego
Tudo começa com a configuração de inicialização da instância	Inicia quando atribuímos a sub rede para todas as instâncias
Aplica-se quando alguém especifica o grupo de segurança ao iniciar a instância e associa-se ao grupo de segurança	Eles não dependem do usuário, aplicam automaticamente todas as instâncias com sub rede

Firewall STATELESS vs STATEFUL

Os firewalls **STATELESS** verificam os pacotes individualmente antes de decidir se devem ou não permiti-los, enquanto os firewalls **STATEFUL** são capazes de rastrear o movimento dos pacotes pela rede, criando perfis para melhor reconhecer conexões seguras e inseguras na origem.

Implementação da Network ACL

Arquitetura de referência



Search results for 'vpc'

Services (12)

Features (57)

Resources **New**

Documentation (12,825)

Knowledge Articles (244)

Marketplace (585)

Blogs (849)

Events (15)

Tutorials (10)

Services

See all 12 results ▶



VPC ★

Isolated Cloud Resources



AWS Firewall Manager ☆

Central management of firewall rules



Detective ☆

Investigate and Analyze potential security issues



Managed Services ☆

IT operations management for AWS

Features

See all 57 results ▶

Dashboard



Serviços

Search

[Alt+S]



Norte da Virgínia

voclabs/user3047831=Testar_aluno @ 6374-2359-2261



EC2



S3



VPC

DHCP

IPs elásticos

Listas de prefixos

gerenciados

Endpoints

Serviços de endpoint

Gateways NAT

Conexões de
emparelhamento

▼ Segurança

ACLs da rede

Grupos de segurança

▼ Firewall de DNS

Grupos de regras

Listas de domínios

▼ Network Firewall

Firewalls

Criar VPC

Executar instâncias do EC2

Observação: suas instâncias serão executadas na região Leste dos EUA.

Recursos por região

Atualizar recursos

Você está usando os seguintes recursos do Amazon VPC

VPCs

Leste dos EUA 2

[Ver todas as regiões](#)

Gateways NAT

Leste dos EUA 1

[Ver todas as regiões](#)

Sub-redes

Leste dos EUA 8

[Ver todas as regiões](#)

Conexões de
emparelhamento de VPC

Leste dos
EUA 0

[Ver todas as regiões](#)

Tabelas de rotas

Leste dos EUA 4

[Ver todas as regiões](#)

Network ACLs

Leste dos EUA 2

[Ver todas as regiões](#)

Gateways da Internet

Leste dos EUA 2

[Ver todas as regiões](#)

Grupos de segurança

Leste dos EUA 6

[Ver todas as regiões](#)

Integridade de serviço

[Visualizar todos os detalhes da integridade do serviço](#)

Configurações

[Zonas](#)

[Experimentos do console](#)

Informações adicionais

[Documentação da VPC](#)

[Todos os recursos da VPC](#)

[Fóruns](#)

[Relatar um problema](#)

AWS Network Manager

O AWS Network Manager fornece ferramentas e recursos para ajudar você a gerenciar e monitorar sua rede na AWS. O Network Manager facilita a execução de gerenciamento de conectividade,



CloudShell

Comentários

© 2024, Amazon Web Services, Inc. ou suas afiliadas.

[Privacidade](#)

[Termos](#)

[Preferências de cookies](#)

[VPC](#) > [Network ACLs](#) > Criar Network ACL

Criar Network ACL

[Informações](#)

Uma Network ACL é uma camada de segurança adicional que age como um firewall para o controle de tráfego de entrada e saída de uma sub-rede.

Configurações da Network ACL

Nome - *opcional*

Cria uma tag com uma chave de "Nome" e um valor que você especifica.

VPC

VPC a ser usada para essa ACL de rede



Tags

Uma tag é um rótulo que você atribui a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional. Você pode usar tags para pesquisar e filtrar seus recursos ou rastrear os custos da AWS.

Chave

Valor - *opcional*

Q Name



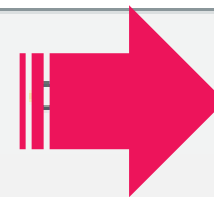
Q acl-publica



Remover tag

Adicionar tag

Você pode adicionar mais 49 tags



Criar Network ACL

Painel da VPC

Visualização global do EC2

Filtrar por VPC:

Selecionar uma VPC

Nuvem privada virtual

Suas VPCs

Sub-redes

Tabelas de rotas

Gateways da Internet

Gateways da Internet somente de saída

Gateways da operadora

Conjuntos de opções de DHCP

IPs elásticos

Listas de prefixos gerenciados

Network ACLs (1/3) Informações

Find resources by attribute or tag

	Name	ID da Network ACL	Associado a	Padrão	ID da VPC
<input type="checkbox"/>	-	acl-0cebf0e99aa96eb8f	6 Sub-redes	Sim	vpc-0c9618cf78e3253
<input checked="" type="checkbox"/>	acl-publica	acl-0aa7e2a9491b2ff62	-	Não	vpc-000e299487bb7b

acl-0aa7e2a9491b2ff62 / acl-publica

Detalhes

Regras de entrada

Regras de saída

Assoc

Detalhes

ID da Network ACL	Associado a	Padrão	ID da VPC
acl-0aa7e2a9491b2ff62	-	Não	vpc-000e299487bb7bd45 / minha-vpc-01
Proprietário			

Está criada a ACL, contudo não temos nenhuma sub rede associada. Iremos associar a sub rede pública

Painel da VPC

Visualização global do EC2

Filtrar por VPC:

Selecionar uma VPC ▾

▼ Nuvem privada virtual

Suas VPCs

Sub-redes

Tabelas de rotas

Gateways da Internet

Gateways da Internet somente de saída

Gateways da operadora


Conjuntos de opções de DHCP

IPs elásticos

Listas de prefixos gerenciados

Network ACLs (1/3) Informações

< 1 >



<input type="checkbox"/>	Name ▾	ID da Network ACL ▾	Associado a ▾	Padrão ▾	ID da VPC ▾
<input type="checkbox"/>	-	acl-0cebf0e99aa96eb8f	6 Sub-redes	Sim	vpc-0c9618cf78e3253
<input checked="" type="checkbox"/>	acl-publica	acl-0aa7e2a9491b2ff62	-	Não	vpc-000e299487bb7b

acl-0aa7e2a9491b2ff62 / acl-publica

Detalhes

Regras de entrada


Regras de saída

Associações de sub-rede

Tags

Associações de sub-rede

< 1 >



Nome ▾	ID da sub-rede ▾	Associado a ▾	Zona de disponi... ▾	CIDR IPv4 ▾
--------	------------------	---------------	----------------------	-------------

Editar associações de sub-rede Informações

Alterar quais sub-redes estão associadas a essa ACL de rede.

Sub-redes disponíveis (1/2)

Filter subnet associations

< 1 > ⚙

	Nome	ID da sub-rede	Associado a	Zona de disponibilid...	CIDR IPv4	CIDR IPv6
<input type="checkbox"/>	sub-rede-privada	subnet-079c930b4ceead...	acl-0efa832749cab61d7	us-east-1a	10.0.0.128/25	–
<input checked="" type="checkbox"/>	sub-rede-publica	subnet-0abfa13c29a353...	acl-0efa832749cab61d7	us-east-1a	10.0.0.0/25	–

Sub-redes selecionadas

subnet-0abfa13c29a353ef3 / sub-rede-publica ✕

Cancelar

Salvar alterações

aws

Serviços

Search

[Alt+S]

Norte da Virgínia

voclabs/user3047831=Testar_aluno @ 6374-2359-2261

EC2

S3

VPC

Painel da VPC

Visualização global do EC2

Filtrar por VPC:

Selecionar uma VPC

Nuvem privada virtual

Suas VPCs

Sub-redes

Tabelas de rotas

Gateways da Internet

Gateways da Internet somente de saída

Gateways da operadora

Conjuntos de opções de DHCP

IPs elásticos

Listas de prefixos gerenciados

Network ACLs (1/3) Informações

Find resources by attribute or tag

Name	ID da Network ACL	Associado a	Padrão	ID da VPC
-	acl-0efa832749cab61d7	subnet-079c930b4ceead050 / sub-rede-privada	Sim	vpc-000e299487bb7b...
-	acl-0cebf0e99aa96eb8f	6 Sub-redes	Sim	vpc-0c9618cf78e3253...
<input checked="" type="checkbox"/> acl-publica	acl-0aa7e2a9491b2ff62	subnet-0abfa13c29a353ef3 / sub-rede-publica	Não	vpc-000e299487bb7b...

Detalhes

Regras de entrada

Regras de saída

Associações de sub-rede

Tags

Regras de entrada (1)

Editar regras de entrada

Filter inbound rules

Número da regra	Tipo	Protocolo	Intervalo de por...	Origem	Permitir/negar
*	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	Deny

[VPC](#) > [Network ACLs](#) > [acl-0aa7e2a9491b2ff62 / acl-publica](#) > Editar regras de entrada

Editar regras de entrada [Informações](#)

Regras de entrada controlam o tráfego de entrada que tem permissão para acessar a VPC.

Id	Tipo Informações	Protocolo Informações	Intervalo de portas Informações	Origem Informações	Permitir/negar Informações	
100	Todo o tráfego ▼	Tudo ▼	Tudo	0.0.0.0/0	Permitir ▼	Remover
*	Todo o tráfego ▼	Tudo ▼	Tudo	0.0.0.0/0	Negar ▼	

[Adicionar nova regra](#) [Classificar por número de regra](#)

Cancelar

Visualizar alterações

Salvar alterações

Serviços

[Alt+S]

Norte da Virgínia ▾

voclabs/user3047831=Testar_aluno @ 6374-2359-2261 ▾

Painel da VPC

Visualização global do EC2

Filtrar por VPC:

Selecionar uma VPC ▾

Nuvem privada virtual

Suas VPCs

Sub-redes

Tabelas de rotas

Gateways da Internet

Gateways da Internet somente de saída

Gateways da operadora

Conjuntos de opções de DHCP

IPs elásticos

Listas de prefixos gerenciados

Você atualizou com êxito as regras de entrada de acl-0aa7e2a9491b2ff62 / acl-publica

Network ACLs (1/3) Informações

Ações ▾

Criar Network ACL

< 1 >

Name ▾	ID da Network ACL ▾	Associado a ▾	Padrão ▾	ID da VPC
	acl-0efa832749cab61d7	subnet-079c930b4ceead050 / sub-rede-privada	Sim	vpc-000e299487bb7b...
-	acl-0cebf0e99aa96eb8f	6 Sub-redes	Sim	vpc-0c9618cf78e3253...
<input checked="" type="checkbox"/> acl-publica	acl-0aa7e2a9491b2ff62	subnet-0abfa13c29a353ef3 / sub-rede-publica	Não	vpc-000e299487bb7b...

acl-0aa7e2a9491b2ff62 / acl-publica

Detalhes

Regras de entrada

Regras de saída

Associações de sub-rede

Tags

Regras de saída (1)

< 1 >

Editar regras de saída

[VPC](#) > [Network ACLs](#) > [acl-0aa7e2a9491b2ff62 / acl-publica](#) > Editar regras de saída

Editar regras de saída [Informações](#)

Regras de saída controlam o tráfego de saída que tem permissão para sair da VPC.

Número da regra	Tipo Informações	Protocolo Informações	Intervalo de portas Informações	Destino Informações	Permitir/negar Informações	
100	Todo o tráfego ▼	Tudo ▼	Tudo	0.0.0.0/0	Permitir ▼	<button>Remover</button>
*	Todo o tráfego ▼	Tudo ▼	Tudo	0.0.0.0/0	Negar ▼	

Adicionar nova regraClassificar por número de regra

Cancelar

Visualizar alterações

Salvar alterações


```
PS C:\Users\Eduardo Verri\Desktop\chaves\4ads> ssh -i "myssh.pem" ubuntu@18.209.13.196
The authenticity of host '18.209.13.196 (18.209.13.196)' can't be established.
ED25519 key fingerprint is SHA256:5+bUQhgL9sqaBT45ptq9GiIuz26op0ynGaLIb63PGf0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.209.13.196' (ED25519) to the list of known hosts.
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 Tue Mar  5 22:46:49 UTC 2024
```

```
System load:  0.23876953125      Processes:            134
Usage of /:   38.9% of 11.45GB    Users logged in:     0
Memory usage: 6%                 IPv4 address for eth0: 10.0.0.80
Swap usage:   0%
```

```
Expanded Security Maintenance for Applications is not enabled.
```

```
79 updates can be applied immediately.
46 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

```
32 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
```

```
Last login: Wed Feb 28 20:12:14 2024 from 131.72.61.70
```

```
ubuntu@ip-10-0-0-80:~$ |
```



Atividade Redes

- Crie uma nova VPC e configure duas sub redes (pública e privada)
- Crie e configure Internet Gateway (sub rede pública) e NAT Gateway (sub rede privada)
- Crie e configure as tabelas de rotas
- Provisione uma instância em cada sub rede e teste os acessos
- Utilize a ACL criada para configurar regras de acesso de **entrada** específicas para HTTP (porta 80), HTTPS (porta 443) e SSH (porta 22) para a sub rede pública de **qualquer origem**.
- Crie uma nova ACL para a sub rede privada e configure regra de acesso de entrada para HTTP (porta 80), HTTPS (porta 443) e SSH (porta 22) para a sub rede privada apenas do **intervalo de endereço IP da rede pública**.
- Ambas, as saídas podem ficar permitidas para qualquer origem.
- **Tire print ao longo de todo o desenvolvimento como evidência.**

Agradeço
a sua atenção!



SÃO
PAULO
TECH
SCHOOL