



SÃO
PAULO
TECH
SCHOOL

Infraestrutura em Nuvem

LAB03

Security Groups - AWS

Professor Marcio Santana

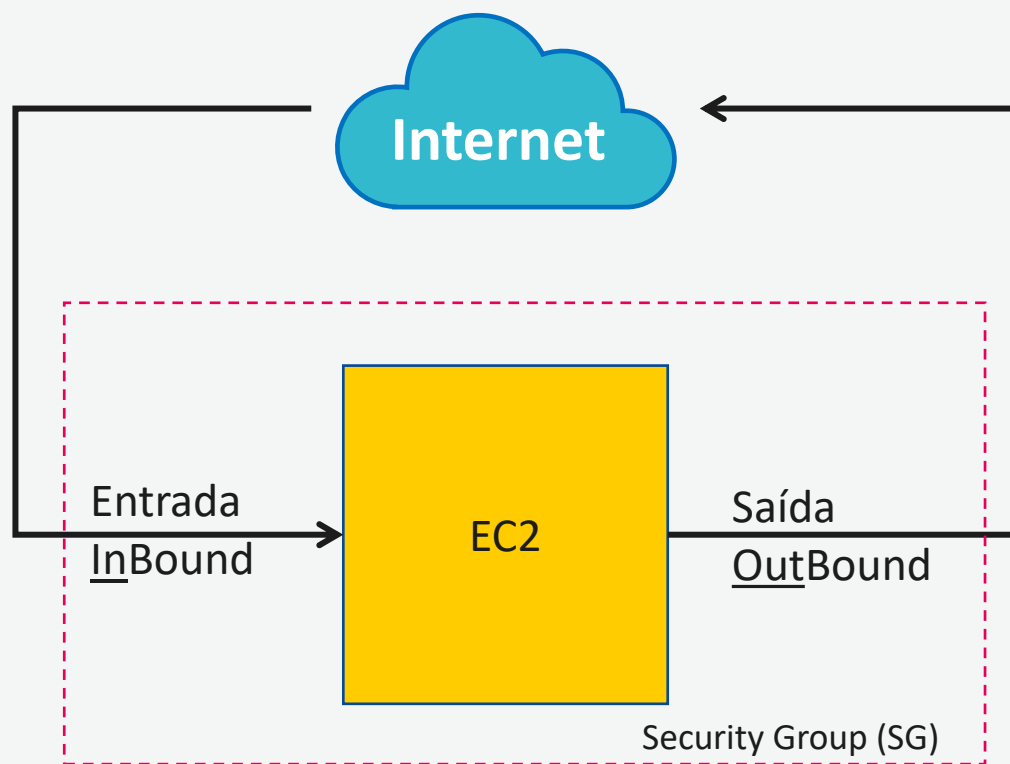
`marcio.santana@sptech.school`

Tópicos da Aula

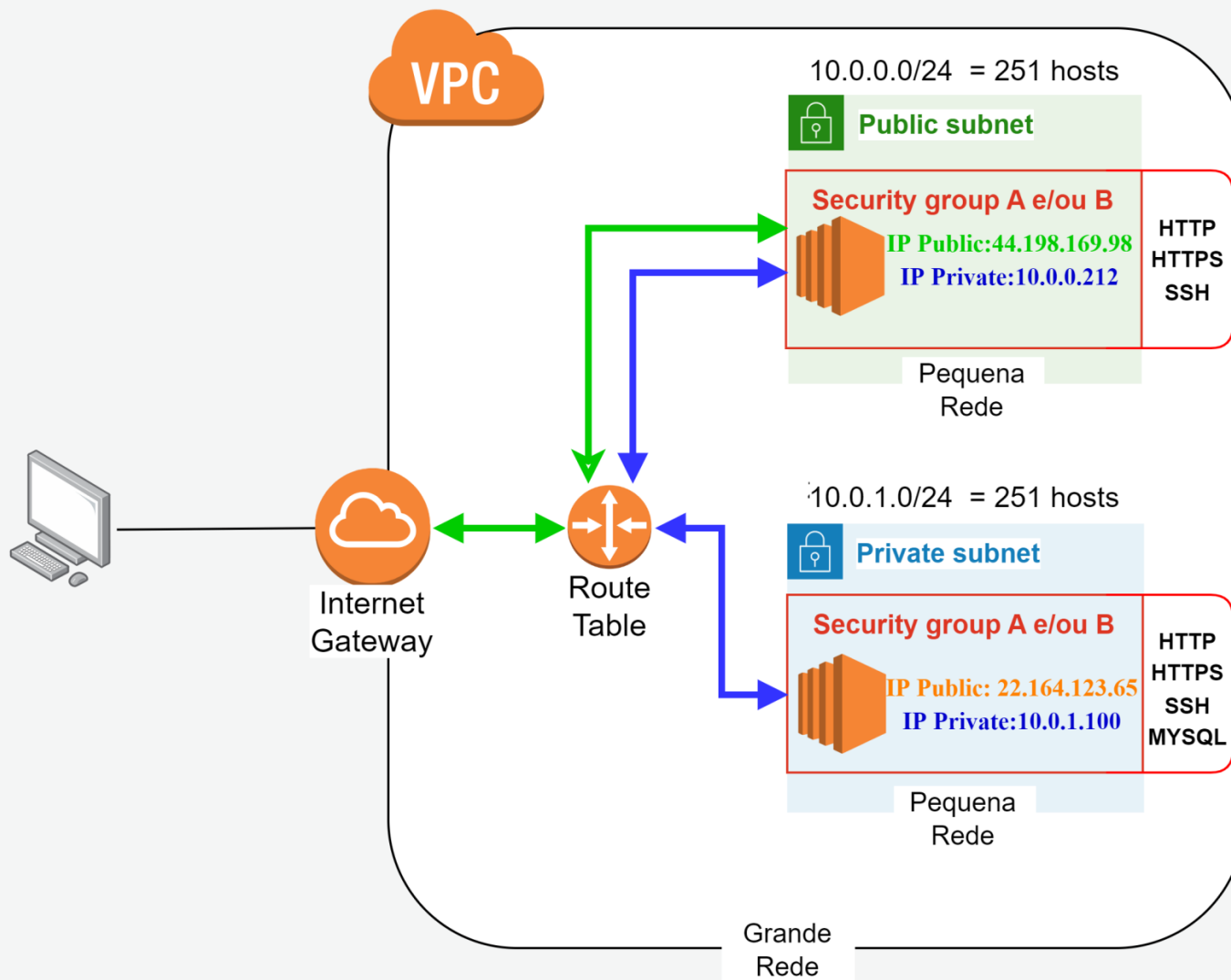
1. Criando o Security Groups
2. Associando os Security Groups
3. Alterando Security Group de uma EC2
4. Associando IP Elastic IP à EC2

Security Groups

Os Security Groups (SG) são **firewalls virtuais** que controlam o tráfego de entrada e saída das instâncias EC2 com base em regras de filtragem que você define.



Security Groups



1. Criando o Security Groups

Painel - Virtual Private Cloud - VPC

☐ New VPC Experience
[Learn more](#)

VPC Dashboard
Filter by VPC:

☒ VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

☒ SECURITY

Network ACLs

Security Groups

☒ REACHABILITY

Reachability Analyzer

Launch VPC Wizard

Launch EC2 Instances

Note: Your Instances will launch in the US East (N. Virginia) region.

Resources by Region

[Refresh Resources](#)

You are using the following Amazon VPC resources

VPCs
See all regions ▼

N. Virginia 1

NAT Gateways
See all regions ▼

N. Virginia 0

Subnets
See all regions ▼

N. Virginia 6

VPC Peering Connections
See all regions ▼

N. Virginia 0

Route Tables
[See all regions](#) ▼

N. Virginia 1

Network ACLs
See all regions ▼

N. Virginia 1

Internet Gateways
See all regions ▼

N. Virginia 1

Security Groups
See all regions ▼

N. Virginia 1

Egress-only Internet Gateways
See all regions ▼

N. Virginia 0

Customer Gateways
See all regions ▼

N. Virginia 0

DHCP options sets
See all regions ▼

N. Virginia 1

Virtual Private Gateways
See all regions ▼

N. Virginia 0

Elastic IPs
See all regions ▼

N. Virginia 0

Site-to-Site VPN Connections
See all regions ▼

N. Virginia 0

Service Health

Current Status	Details
Amazon EC2 - US East (N. Virginia)	Service is operating normally

[View complete service health details](#)

Settings

Zones

Console Experiments

Additional Information

[VPC Documentation](#)

[All VPC Resources](#)

[Forums](#)

[Report an Issue](#)

Transit Gateway Network Manager

Network Manager enables centrally manage your global network across AWS and on-premises. [Learn more](#)

[Get started with Network Manager](#)

VPC

- **Name/Tag**

Localização da RT.

- **Security group ID**

Identificação do SG.

- **Security group name**

Nasce junto com a VPC por isso fica default.

- **VPC ID**

Identificação da VPC associada.

- **Description**

Descrição do SG consome as portas liberadas.

- **Inbound Rules**

Regras de entrada.

- **Outbound Rules**

Regras de saída.

New VPC Experience [Learn more](#)

VPC Dashboard
EC2 Global View **New**

Filter by VPC:

VIRTUAL PRIVATE CLOUD

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- Carrier Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

SECURITY

- Network ACLs
- Security Groups**

Security Groups (1/2) [Info](#)

	Name	Security group ID	Security group name	VPC ID	Description	
<input checked="" type="checkbox"/>	vpc-lab01-bandtec	sg-0695da9ad08ca34b1	default	vpc-09ccb13e487278490	default VPC security gr...	8
<input type="checkbox"/>	-	sg-6893eb76	default	vpc-8c5d2ef1	default VPC security gr...	8

sg-0695da9ad08ca34b1 - default

Details | Inbound rules | Outbound rules | Tags

[You can now check network connectivity with Reachability Analyzer](#) [Run Reachability Analyzer](#) [×](#)

Details

Security group name default	Security group ID sg-0695da9ad08ca34b1	Description default VPC security group	VPC ID vpc-09ccb13e487278490
Owner 814569987389	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Security Groups

New VPC Experience

[Learn more](#)

VPC Dashboard

EC2 Global View New

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Security Groups (1/2) [Info](#)

Actions ▾

Create security group

Filter security groups

<div></div>	Name ▾	Security group ID ▾	Security group name ▾	VPC ID ▾	Description ▾	
<input checked="" type="checkbox"/>	vpc-lab01-bandtec	sg-0695da9ad08ca34b1	default	vpc-09ccb13e487278490	default VPC security gr...	8
<input type="checkbox"/>	-	sg-6893eb76	default	vpc-8c5d2ef1	default VPC security gr...	8

sg-0695da9ad08ca34b1 - default

Details

Inbound rules

Outbound rules

Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Create VPC

VPC > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

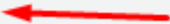
Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)



vpc-09ccb13e487278490 (vpc-lab01-bandtec)
10.0.0.0/23



vpc-8c5d2ef1
172.31.0.0/16

(default)

Security Groups – SSH e RDP

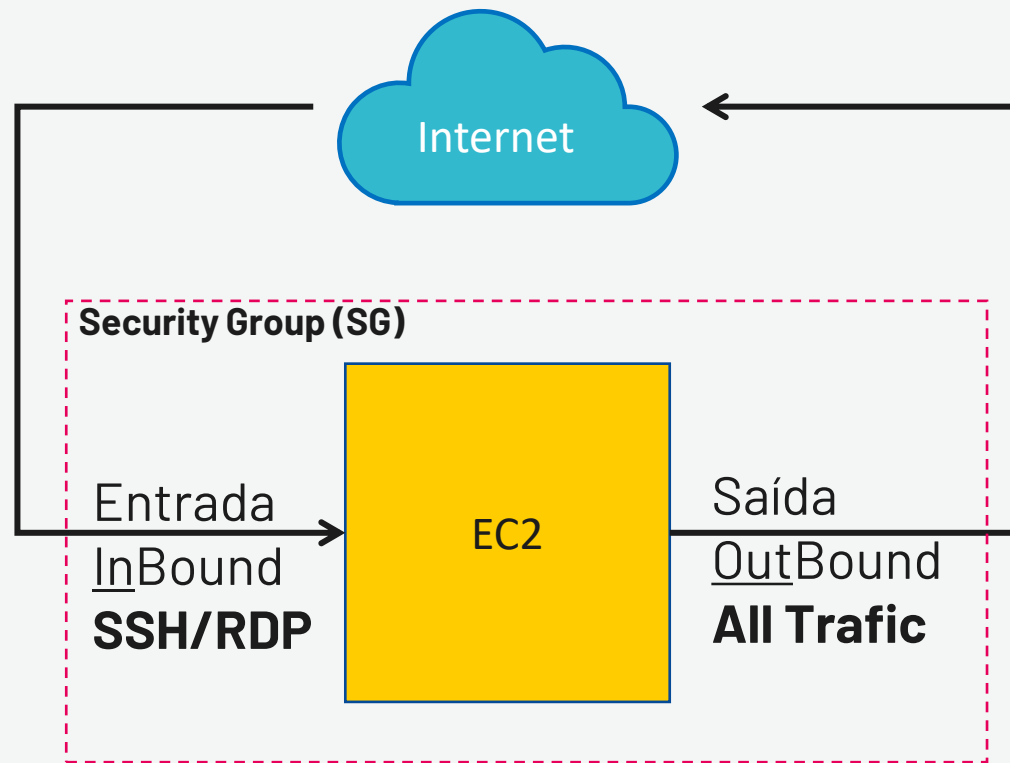
Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH ▼	TCP	22	Anywh... ▼ 0.0.0.0/0 ✕		Delete
RDP ▼	TCP	3389	Anywh... ▼ 0.0.0.0/0 ✕		Delete
Add rule					


Outbound rules [Info](#)


Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	
All traffic ▼	All	All	Custom ▼ 0.0.0.0/0 ✕		Delete
Add rule					


Security Groups



Security Groups – SSH e RDP

 Security group (sg-03251ed0008b40ab9 | AcessoRemoto) was created successfully








 Details

VPC > Security Groups > sg-03251ed0008b40ab9 - AcessoRemoto


sg-03251ed0008b40ab9 - AcessoRemoto




Actions ▼


Details

Security group name  AcessoRemoto	Security group ID  sg-03251ed0008b40ab9	Description  Regras de acesso remoto (SSH e RDP)	VPC ID  vpc-09ccb13e487278490
Owner  814569987389	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Security Groups (1/3) [Info](#)

 Actions ▼ [Create security group](#)

 1  

	Name ▼	Security group ID ▼	Security group name ▼	VPC ID ▼	Description ▼	O
<input checked="" type="checkbox"/>	SSH/RDP	sg-03251ed0008b40ab9	AcessoRemoto	vpc-09ccb13e487278490	Regras de acesso remo...	8'
<input type="checkbox"/>	vpc-lab01-bandtec	sg-0695da9ad08ca34b1	default	vpc-09ccb13e487278490	default VPC security gr...	8'
<input type="checkbox"/>	–	sg-6893eb76	default	vpc-8c5d2ef1	default VPC security gr...	8'

Security Groups – HTTP e HTTPS

VPC > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

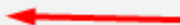
Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

vpc-09ccb13e487278490 (vpc-lab01-bandtec)
10.0.0.0/23



vpc-8c5d2ef1
172.31.0.0/16

(default)

Security Groups – HTTP e HTTPS

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
HTTP ▼	TCP	80	Anywh... ▼ 0.0.0.0/0 ✕		Delete
HTTPS ▼	TCP	443	Anywh... ▼ 0.0.0.0/0 ✕		Delete


Add rule


Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	
All traffic ▼	All	All	Custom ▼ 0.0.0.0/0 ✕		Delete

Add rule

Security Groups - HTTP e HTTPS

 Security group (sg-0de92ffbc94abb6ba | ServicoWeb) was created successfully








[▶ Details](#)

VPC > Security Groups > sg-0de92ffbc94abb6ba - ServicoWeb


sg-0de92ffbc94abb6ba - ServicoWeb

Actions ▼

Details

Security group name  ServicoWeb	Security group ID  sg-0de92ffbc94abb6ba	Description  Regras para servicos web (HTTP e HTTPS)	VPC ID  vpc-09ccb13e487278490
Owner  814569987389	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	


Security Groups (4) [Info](#)



Actions ▼

Create security group

< 1 >



<input type="checkbox"/>	Name ▼	Security group ID ▼	Security group name ▼	VPC ID ▼	Description ▼	O
<input type="checkbox"/>	SSH/RDP	sg-03251ed0008b40ab9	AcessoRemoto	vpc-09ccb13e487278490	Regras de acesso remo...	8'
<input type="checkbox"/>	vpc-lab01-bandtec	sg-0695da9ad08ca34b1	default	vpc-09ccb13e487278490	default VPC security gr...	8'
<input type="checkbox"/>	HTTP/HTTPS	sg-0de92ffbc94abb6ba	ServicoWeb	vpc-09ccb13e487278490	Regras para servicos w...	8'
<input type="checkbox"/>	-	sg-6893eb76	default	vpc-8c5d2ef1	default VPC security gr...	8'

2. Associando os Security Groups

EC2 + VPC

▼ Configurações de rede [Informações](#)

VPC - obrigatório [Informações](#)

vpc-05457dd99ea154589 (vpc-lab01-sptech)
10.0.0.0/23



Sub-rede [Informações](#)

subnet-0ba1b2e50bf5e571d sub-az1-pub-lab01-sptech
VPC: vpc-05457dd99ea154589 Proprietário: 463706972487
Zona de disponibilidade: us-east-1d Endereços IP disponíveis: 250 CIDR: 10.0.0.0/24



[Criar nova sub-rede](#)



Atribuir IP público automaticamente [Informações](#)

Habilitar

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

Grupos de segurança comuns [Informações](#)

Selecionar grupos de segurança



[Comparar regras do grupo de segurança](#)

Os grupos de segurança que você adicionar ou remover aqui serão adicionados ou removidos em todas as suas interfaces de rede.

► [Configuração avançada de rede](#)

3. Alterando Security Group de uma EC2

EC2 + SG

Instâncias (1/2) Informações

Conectar Estado da instância Ações Executar instâncias

Filtrar instâncias

	Name	ID de instância	Estado da instância	Tipo de inst
<input type="checkbox"/>	Back-end1	i-Of7ff8e312805b129	Interrompido	t2.micro
<input checked="" type="checkbox"/>	EC2 - API	i-0dbaa76d33c2dc06e	Executando	t2.micro

Alterar grupos de segurança

Obter senha do Windows

Modificar função do IAM

Conectar

Visualizar detalhes

Gerenciar estado da instância

Configurações de instância

Redes

Segurança

Imagem e modelos

Monitorar e solucionar problemas


EC2 + SG

Alterar grupos de segurança [Informações](#)


O Amazon EC2 avalia todas as regras dos grupos de segurança selecionados para controlar o tráfego de entrada e saída de e para sua instância. Você pode usar essa janela para adicionar e remover os grupos de segurança.

Detalhes da instância

ID de instância

 i-0dbaa76d33c2dc06e (EC2 - API)

ID de interface de rede

 eni-00d20d22cc36a4c60

Grupos de segurança associados

Adicione um ou mais grupos de segurança à interface de rede. Você também pode remover os grupos de segurança.

 *Selecionar grupos de segurança*

AcessoRemoto (sg-05ef31dff9b4fd4a2)

AcessoRemoto SSH/RDP

default (sg-0695da9ad08ca34b1)

default vpc-lab01-bandtec

EC2-Back (sg-0bb90db452c4c65b8)

EC2-Back

ServicoWeb (sg-0e4ad551968f88693)

ServicoWeb HTTP/HTTPS

ServicoWeb

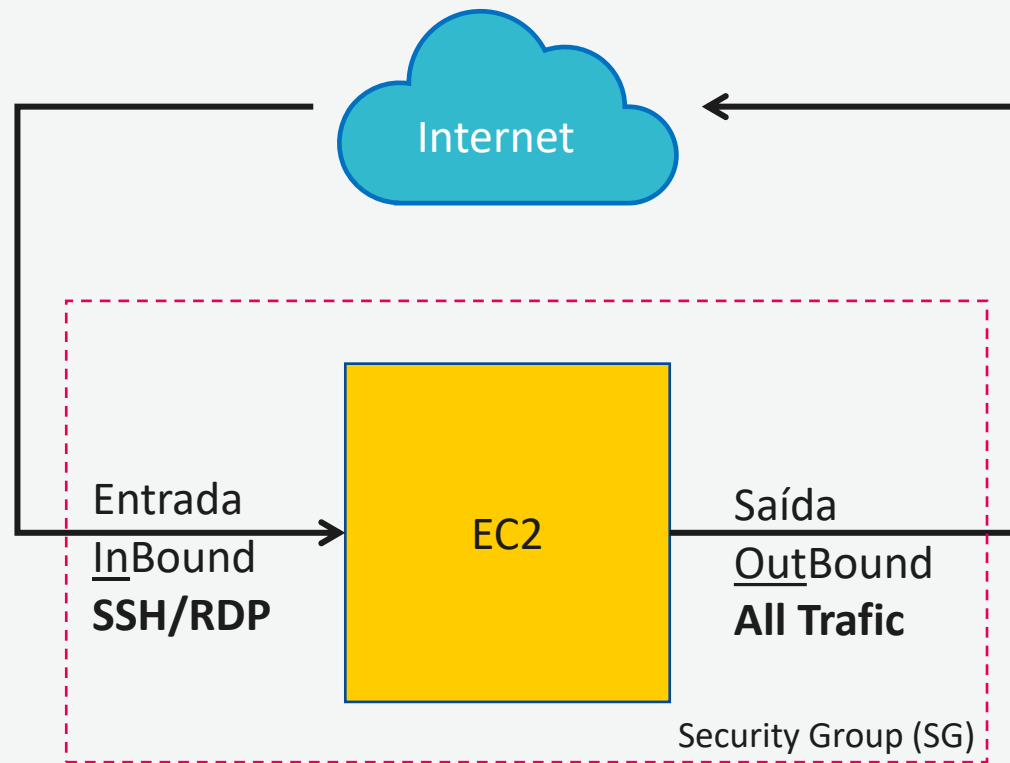
sg-0e4ad551968f88693

Remover

Cancelar

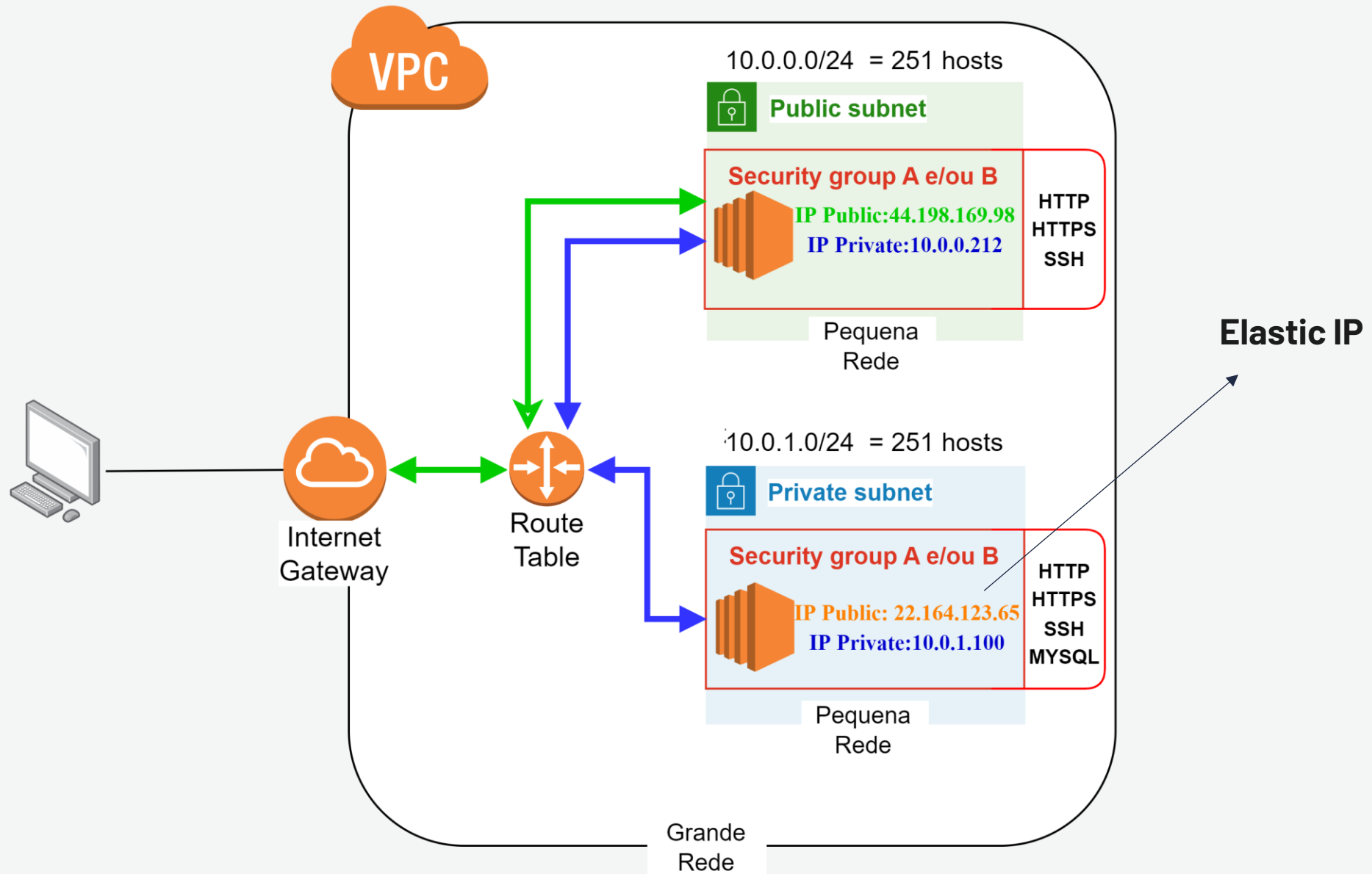
Salvar

Security Groups



4. Associando IP Elastic IP à EC2

Elastic IP



Security group:

Aplicado no recurso: permite definir regras granulares, que sejam efetivas em um único recurso;

Precisa ser aplicado em todos recursos: para funcionar corretamente, o security group precisa estar associado com todos os recursos necessários, sendo fácil esquecer de configurar em algum recurso;

Pode apenas permitir tráfego: não é possível criar uma regra para negar o tráfego (DENY) em um security group;

Interpretado de forma compilada: como ele funciona anexado a um recurso, todas as regras dos security groups associadas nesse recurso são combinadas e as regras com maior abrangência são consideradas;

Agradeço
a sua atenção!

Marcio Santana

marcio.santana@sptech.school

SÃO
PAULO
TECH
SCHOOL