SÃO
PAULO
TECH
SCHOOL

Infraestrutura em Nuvem

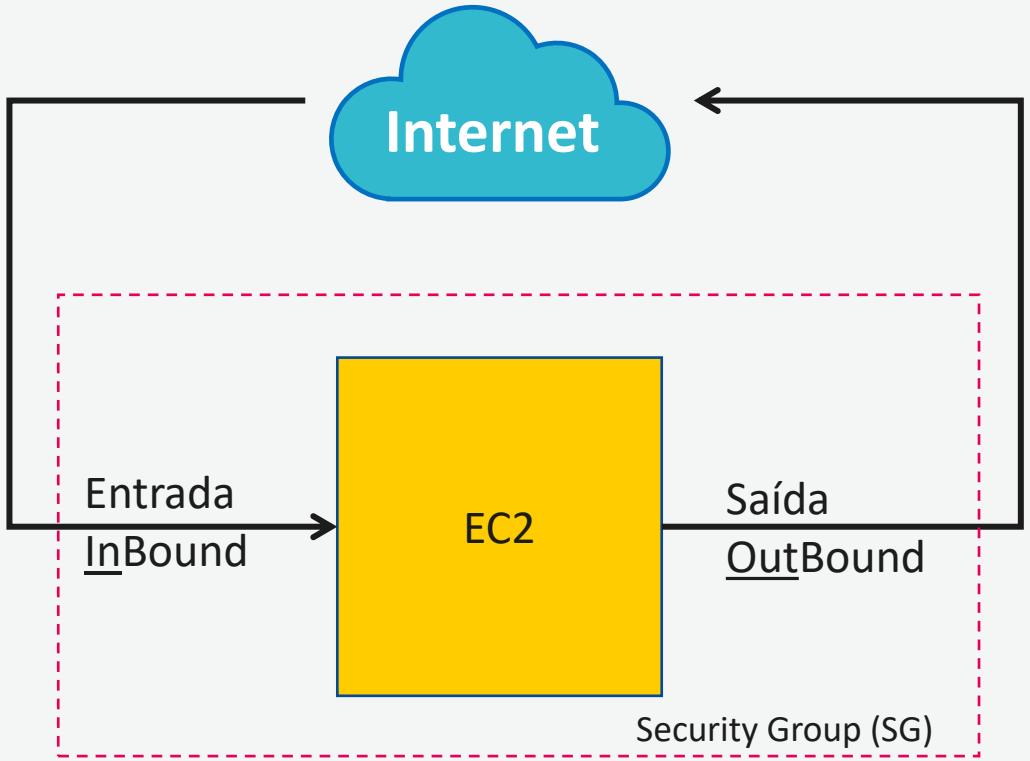
LAB04
ACL

Professor Marcio Santana

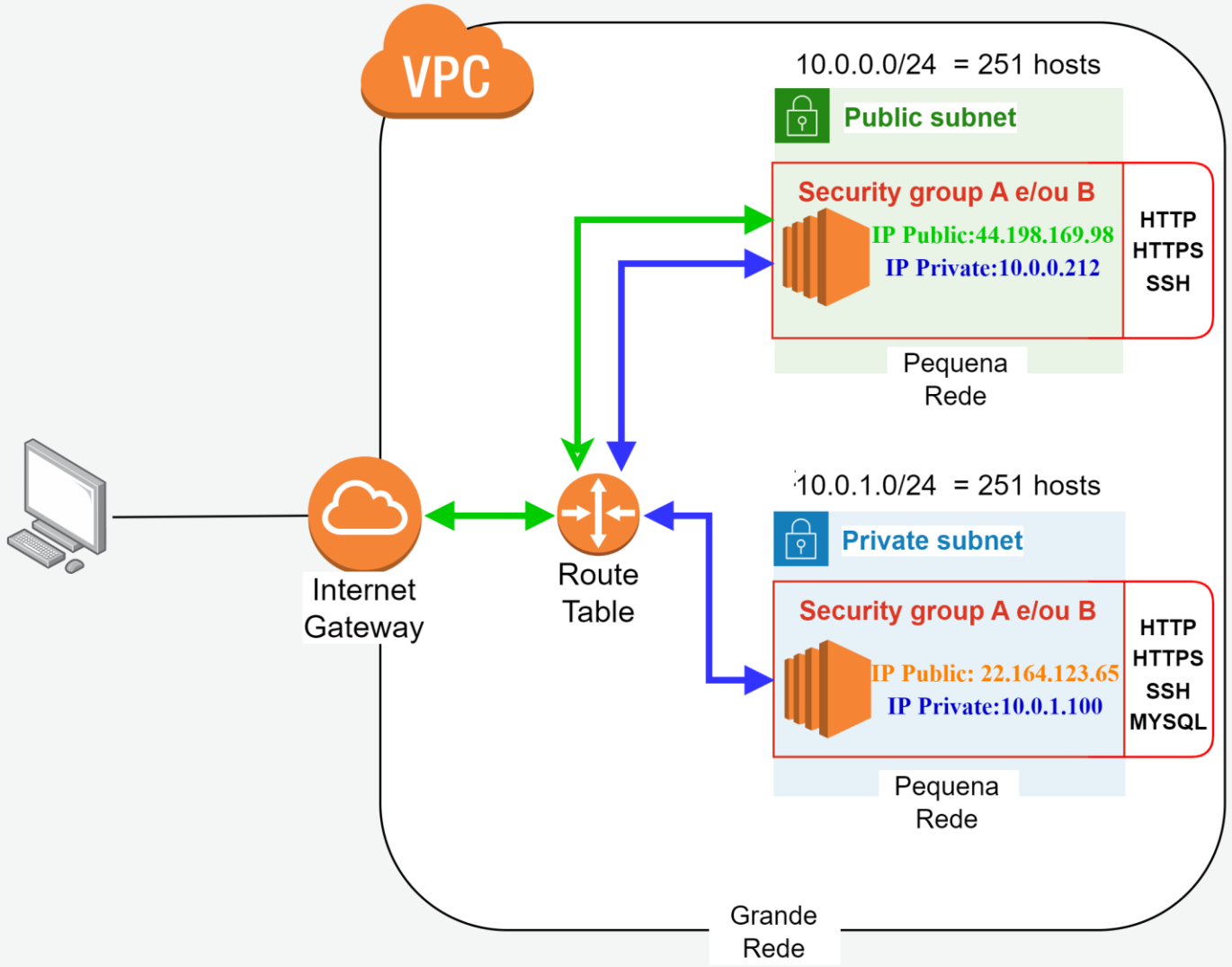
marcio.santana @sptech.school

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



ACL

As **ACLs** (Access Control Lists) na VPC (Virtual Private Cloud) são um recurso de controle de tráfego que funciona no nível da sub-rede, oferecendo uma **camada adicional de segurança** além dos grupos de segurança (security groups).

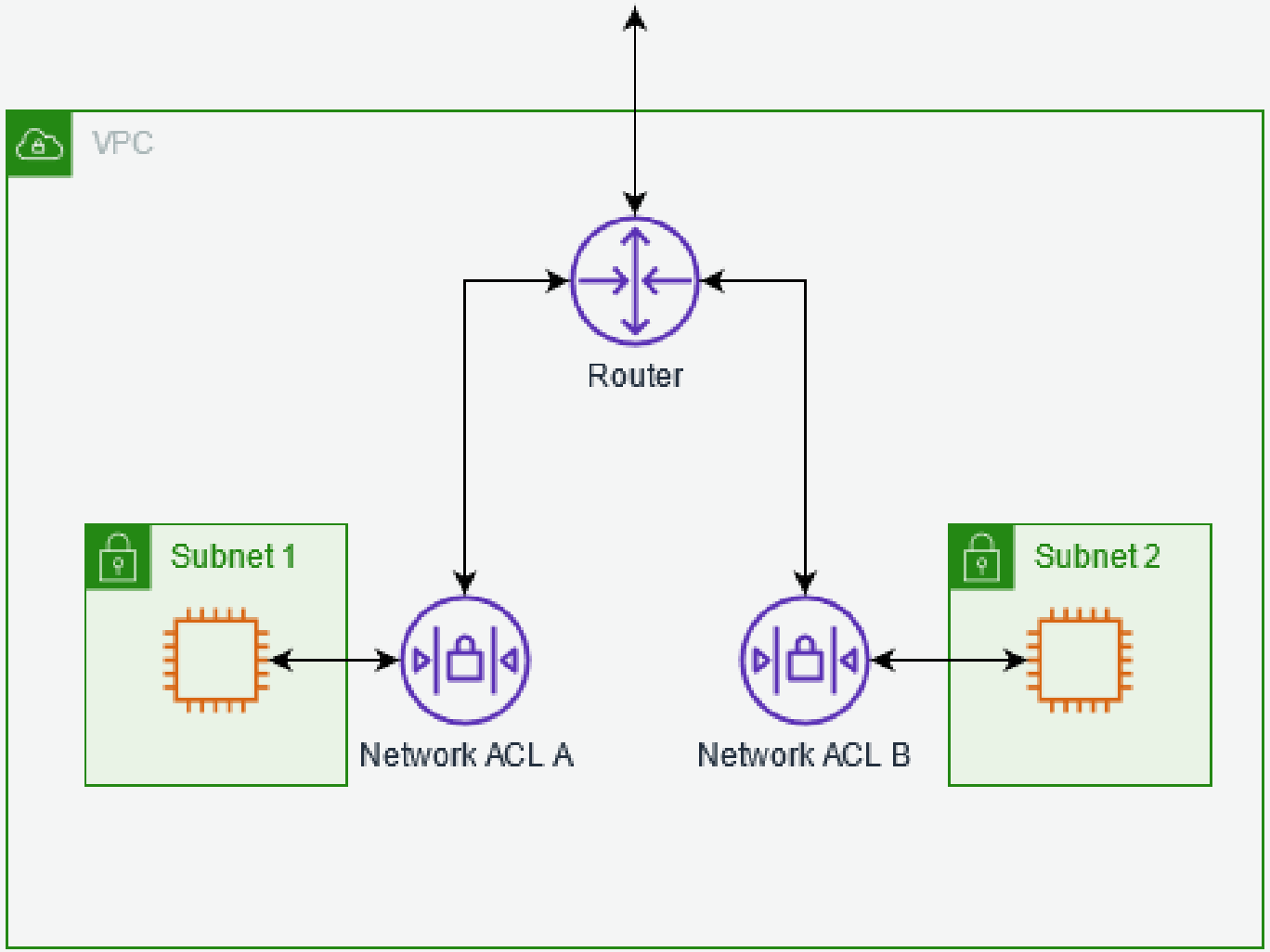
Controle de Tráfego de Entrada e Saída: As ACLs podem **permitir** ou **negar** tráfego tanto de entrada quanto de saída em nível de sub-rede, sendo aplicadas antes que o tráfego atinja qualquer instância na VPC.

Ordem das Regras: As regras nas ACLs são **processadas numericamente**, de acordo com o número de regra, de menor para maior. Quando uma regra correspondente é encontrada, a execução para, e a ação de "permitir" ou "negar" é tomada.

Aplicação em Sub-redes: Uma ACL é associada a uma **sub-rede inteira**, e todas as instâncias dentro dessa sub-rede estão sujeitas às regras dessa ACL.

ACLs são úteis para ter um controle de tráfego em camadas e fornecer proteção adicional para seus recursos na nuvem, especialmente quando se lida com **múltiplas sub-redes** em uma mesma VPC.

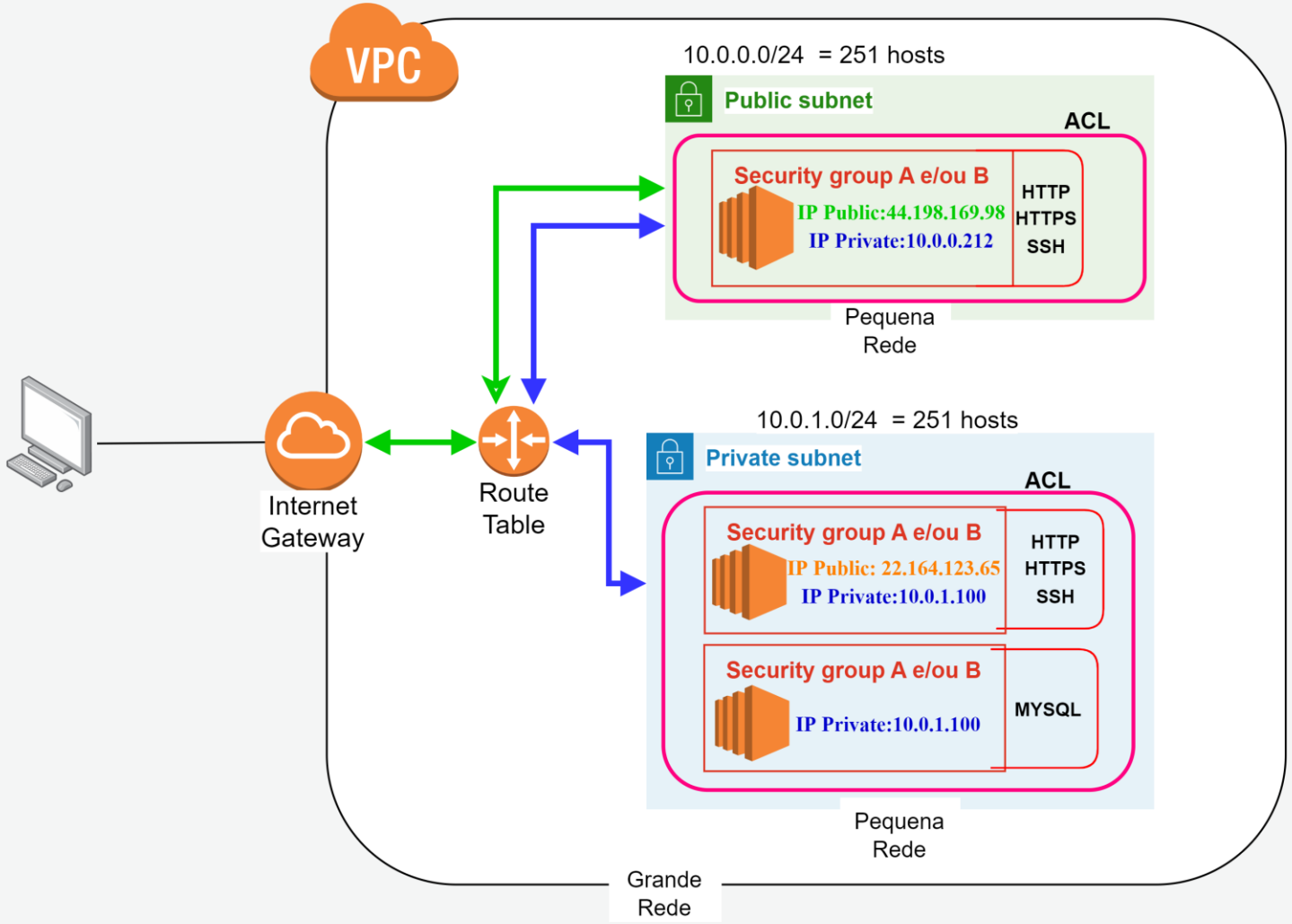
ACL



Control subnet traffic with network access control lists - Amazon Virtual Private Cloud

ACL

Uma lista de controle de acesso (ACL) de rede é uma camada de segurança para sua VPC que atua como firewall para **controlar o tráfego** de entrada e saída de uma ou mais **sub-redes**.



Network ACLs (2) Informações

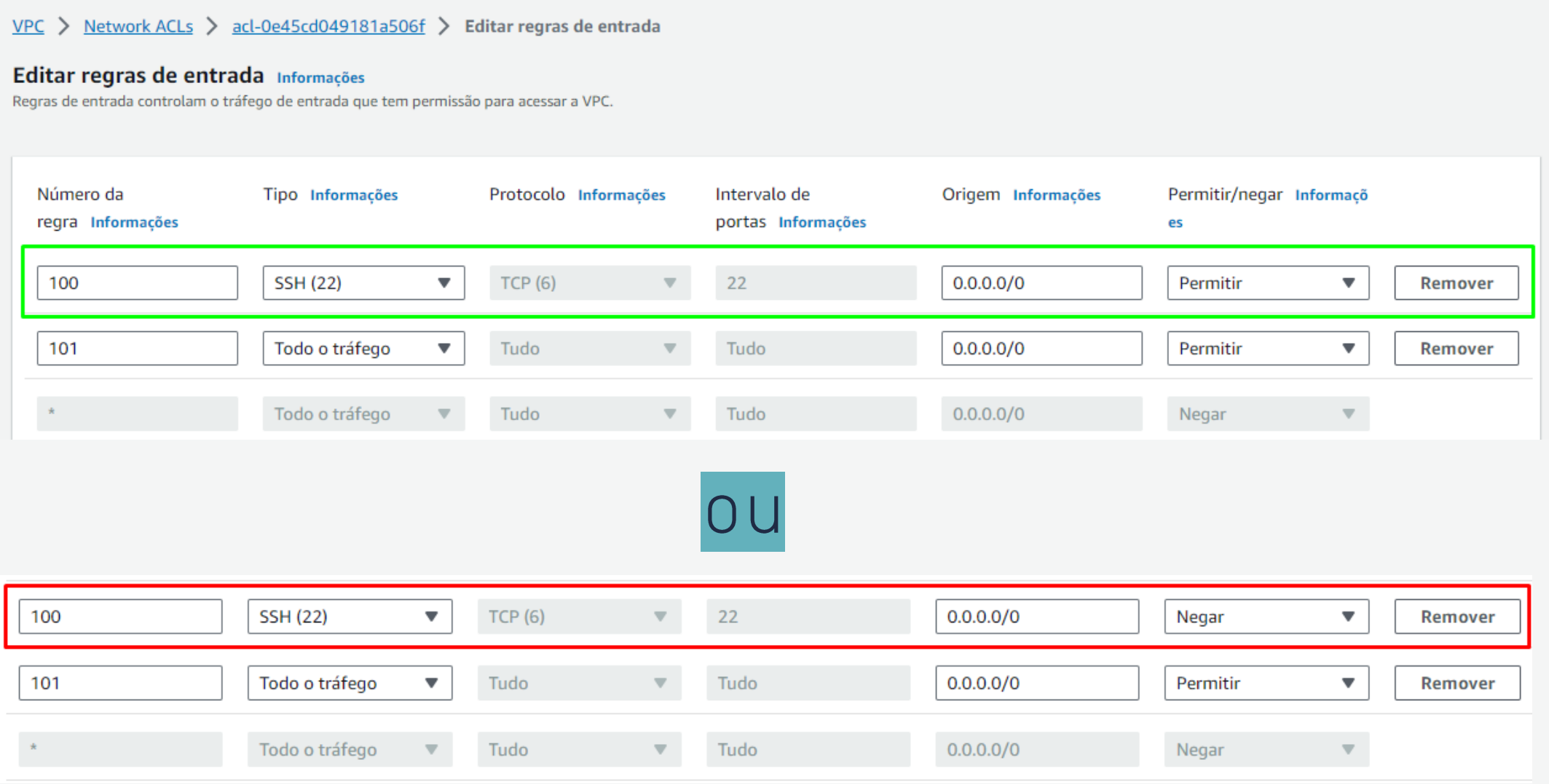
Ações | Criar Network ACL

Find resources by attribute or tag

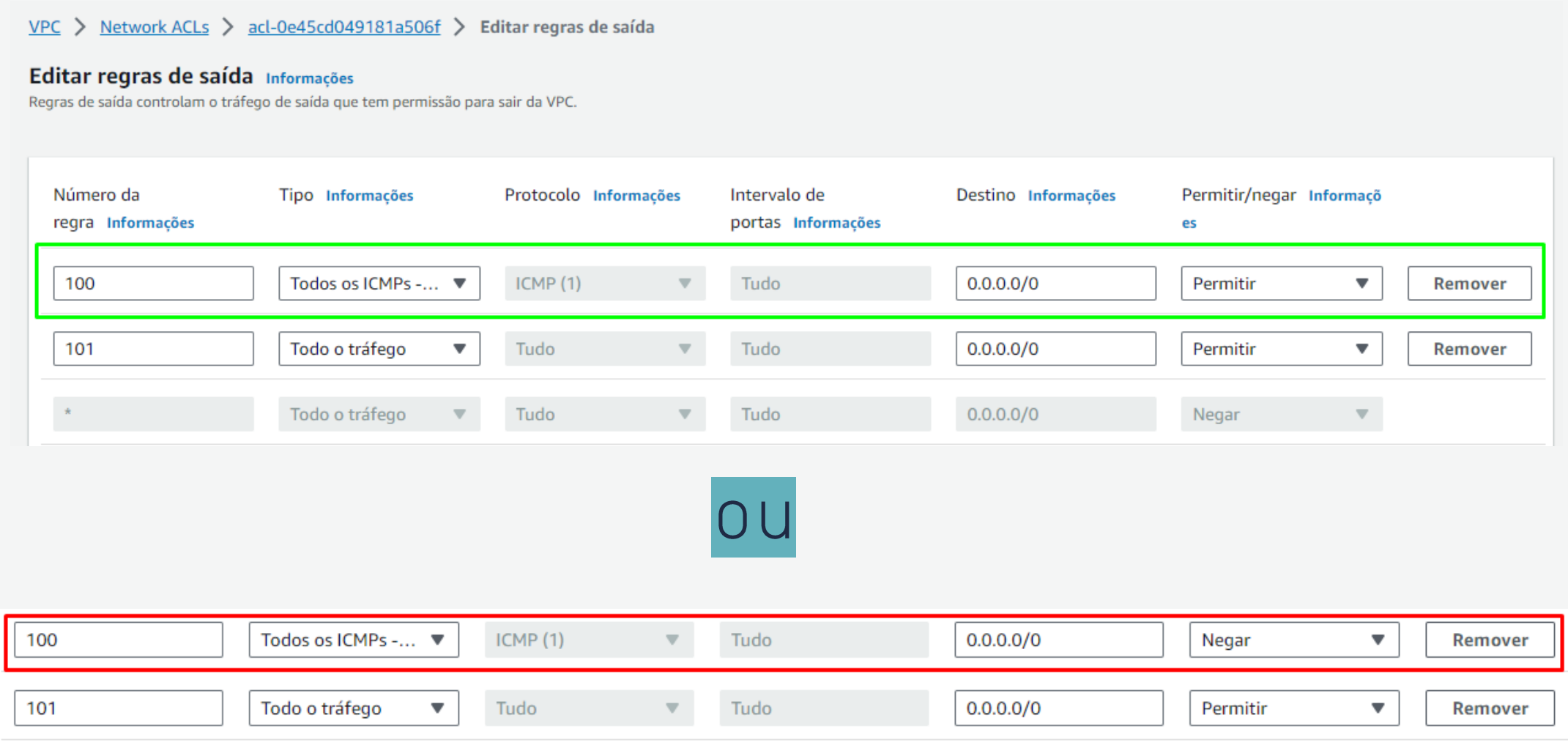
1

Name	ID da Network ACL	Associado a	Padrão	ID da VPC	Contagem de regras de entrada	Contagem de regras de
lab04	acl-00bb9e3ba3aed5d14	2 Sub-redes	Sim	vpc-028e44a8a54233c4d / vpc-lab01-sptech	2 Regras de entrada	2 Regras de saída
–	acl-0d946fd8333e5bae3	6 Sub-redes	Sim	vpc-0b9817adec1b0eace	2 Regras de entrada	2 Regras de saída

Requisições de **Entradas** [SubRede]



Requisições de **Saídas** [SubRede]



ou

Resumo ACL

Aplicado na subnet: permite definir regras mais globais, que sejam efetivas em uma subnet completa;

Transparente para os recursos: todos os recursos dessa subnet tem seu tráfego filtrado, o que pode resultar em uma grande quantidade de regras;

Pode permitir ou negar tráfego: funciona de forma mais similar a um firewall convencional, podendo permitir (ALLOW) ou negar o tráfego (DENY);

Interpretado sequencialmente: cada regra é interpretada individualmente, onde a sequência que as regras são configuradas importa;

Exemplo: Você quer bloquear todo o tráfego de entrada em uma sub-rede proveniente de uma **faixa de IPs maliciosa** específica ou de um país inteiro. Uma ACL seria usada para isso.

Resumo SG

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;

Exemplo: Exemplo prático: Você tem uma instância de aplicação e deseja permitir somente o tráfego HTTP e SSH de endereços IP específicos. O Security Group será usado para definir essas permissões.

Desafio

1. Sub-rede Pública (Servidores Web):

Objetivo: Permitir tráfego HTTP/HTTPS (porta 80/443) e SSH (porta 22) vindo da internet.

- **ACL Associada 1**:
  - **Regra 100**: Permitir tráfego de entrada na porta 80 (HTTP) de qualquer origem.
  - **Regra 110**: Permitir tráfego de entrada na porta 443 (HTTPS) de qualquer origem.
  - **Regra 120**: Permitir tráfego de entrada na porta 22 (SSH) apenas do seu endereço IP público (exemplo: IP SPTech).
  - **Regra 200**: Permitir tráfego de saída para qualquer destino (todas as portas).

2. Sub-rede Privada (Servidores de Banco de Dados):

- **Objetivo**: Permitir somente o tráfego da sub-rede pública e bloquear acesso direto da internet.

- **ACL Associada 2**:
  - **Regra 100**: Permitir tráfego de entrada na porta 3306 (MySQL) proveniente apenas da sub-rede pública (endereços IP dentro da faixa CIDR da sub-rede pública).
  - **Regra 200**: Permitir tráfego de saída para a sub-rede pública (para comunicação de volta).
  - **Regra 300**: Bloquear qualquer outro tráfego de entrada (regra implícita que nega tudo que não for permitido explicitamente).

Agradeço
a sua atenção!

Marcio Santana

marcio.santana@sptech.school

SÃO PAULO TECH SCHOOL