

A Amazon Web Services (AWS) oferece serviços de infraestrutura de redes baseados em nuvem que auxiliam no projeto e no gerenciamento dos recursos de rede. Três componentes importantes da rede da AWS são: Virtual Private Cloud (VPC), Subnets e Security Groups.

### Virtual Private Network da AWS (VPC)

Uma VPC é uma rede virtual privada logicamente isolada dentro de uma região da AWS. Ela permite a definição de faixas de endereços IP, a configuração de tabelas de roteamento, gateways de internet e políticas de controle de acesso. Portanto, a VPC abrange toda a infraestrutura onde subnets, gateways e security groups coexistem.

A rede virtual privada da AWS fornece uma seção logicamente isolada da nuvem AWS, onde instâncias da AWS, como a EC2 (Amazon Elastic Compute Cloud), podem ser iniciadas. A EC2 é um serviço da AWS que fornece capacidade computacional na nuvem.

### Subnet

Uma Subnet é uma subdivisão da rede dentro da VPC, com uma faixa de endereços IP previamente definida, podendo ser pública (com acesso à internet via gateway), privada (sem rota direta à internet exigindo um NAT para acesso à internet pública), somente VPN (site-to-site VPN) ou isolada (acesso somente na própria VPC). O objetivo da Subnet é organizar os recursos dentro da VPC e controlar a conectividade entre os recursos com base nas tabelas de roteamento associadas. As Subnets dividem logicamente os recursos dentro da VPC em zonas de disponibilidade de modo a atingir alta disponibilidade e tolerância a falhas.

A VPC fornece a rede virtual onde as instâncias e outros recursos da AWS operam, enquanto as Subnets dividem essa rede em segmentos específicos, permitindo o controle de tráfego em nível granular.

### Security Groups

Um Security Group é um conjunto de regras que controla o tráfego de entrada e saída de instâncias ou recursos específicos em uma subnet. Ele atua como um firewall virtual, definindo regras para permitir ou negar o tráfego baseado em protocolos, portas e endereços IP, aplicando as regras a nível de instâncias EC2, por exemplo, independentemente da configuração da subnet.

O Security Group é stateful, ou seja, se o tráfego de entrada for permitido por uma regra, as respostas ao tráfego de saída são automaticamente permitidas e vice-versa.

Security Groups não se aplicam globalmente na VPC ou às subnets. Cada instância ou recurso pode ter vários Security Groups associados.

Portanto, uma VPC é o contêiner maior que engloba todas as Subnets e Security Groups. As Subnets dividem logicamente os recursos dentro da VPC em zonas de disponibilidade e controlam o tráfego externo através de tabelas de roteamento. Os Security Groups protegem instâncias e recursos específicos das Subnets, permitindo a granularidade das regras de acesso.