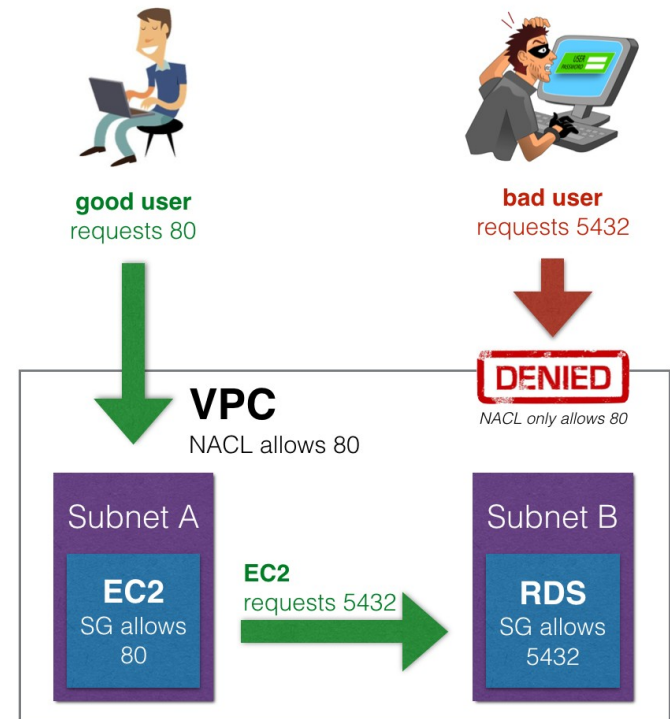


Security Groups

“AWS Firewall”

Security Groups

- Um *Security Group* atua como um firewall virtual que controla o tráfego para uma ou mais instâncias.
- As regras de um *Security Group* **controlam o tráfego de entrada e saída** que tem permissão para atingir as instâncias associadas ao grupo de segurança.
- Todas as regras criadas são sempre do tipo **PERMISSIVAS**.
- Por padrão, os *Security Groups* **PERMITEM** todo o tráfego de saída (Outbound).
- Os *Security Groups* são **stateful**





Security Groups

- Quando você associa vários security groups a uma instância, as regras de cada security group são efetivamente agregadas para criar um conjunto de regras. Usamos esse conjunto de regras para determinar se devemos permitir acesso.
- Componentes de cada regra:
 - **Protocolo:** TCP, UDP, ICMP entre outros.
 - **Intervalo de portas:** 22 (SSH) ou por exemplo 2000-3000
 - **Tipo de código do ICMP:** echo-reply ou echo-request por exemplo
 - **Origem ou destino:** 172.29.0.3/32 ou 172.29.0.0/24
 - **(Opcional) Descrição:** um comentário sobre a regra

ATENÇÃO: Ao criar uma regra no *Security Group*, **SEMPRE** passe o máximo de informações possíveis, pois isso evita “buracos” na construção no seu Firewall. Evite regras do tipo **any to any**.



Links para consulta



https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/ec2-security-groups.html