Segurança em VPCs: NACLs, SGs, Bastion e Flow Logs

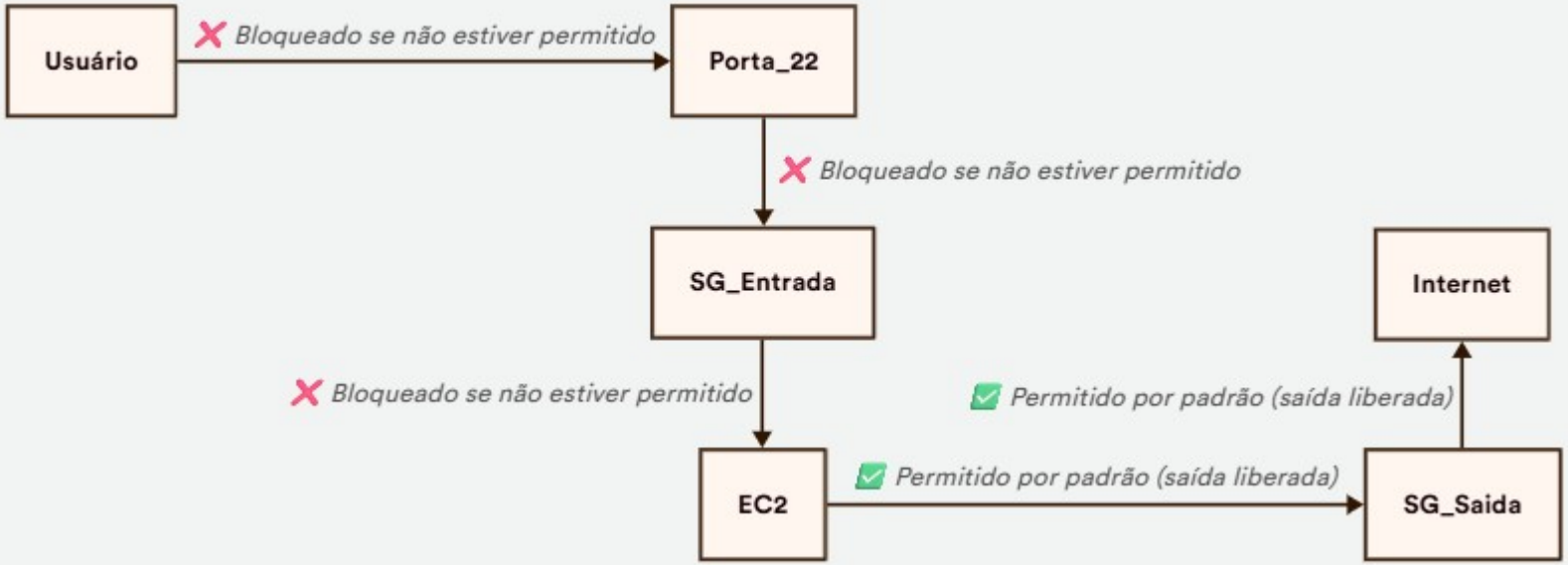
Marlon Brehmer Anesi • Arquiteto de Soluções

Diferença entre Stateless e Stateful

Característica	Stateless (ex: NACL)	Stateful (ex: SG)
Tipo de Recurso	Network ACL	Security Group
Nível de Atuação	Nível da Subnet	Nível da Instância
Controle de Tráfego	Entrada e saída devem ser configuradas separadamente	Respostas a tráfego permitido são automaticamente liberadas
Tipo de Regras	Permite ou nega tráfego	Apenas permite tráfego (não nega)
Ordem de Avaliação	Avaliação por número de regra (menor → maior)	Avaliação implícita por prioridade (não configurável)
Indicado para	Camada de rede / controle amplo	Controle específico de instâncias

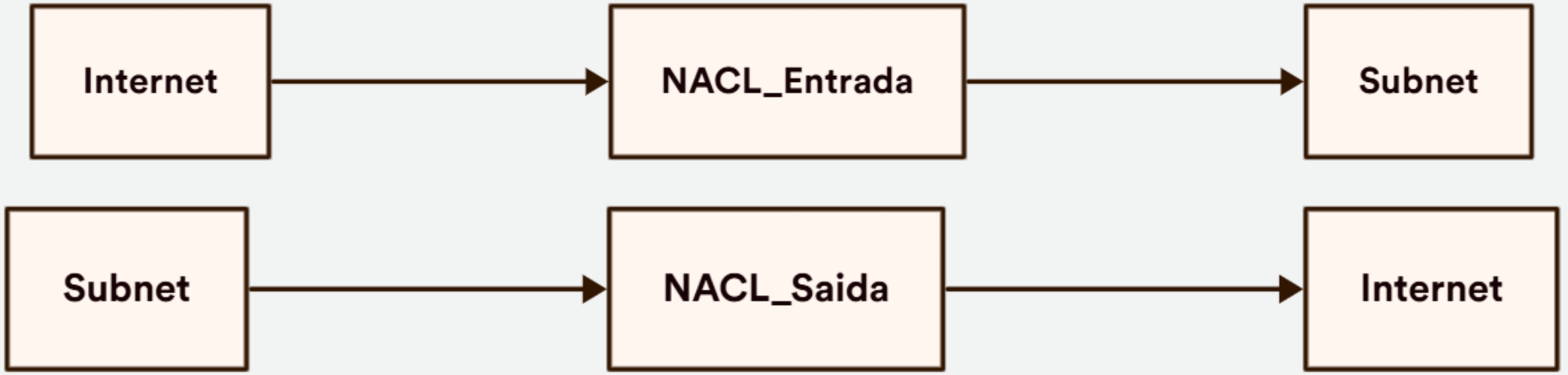
Security Groups (SGs)

- Firewall virtual no nível da instância (EC2, RDS, etc)
- Define regras de entrada e saída por porta/IP/protocolo
- É stateful: resposta é automaticamente permitida
  - Por padrão, permite toda saída e bloqueia toda entrada – só entra o que for permitido.
- Associado diretamente ao recurso (instância)



Network ACLs (NACLs)

- Firewall no nível da subnet
- Define regras de entrada e saída por IP, porta, protocolo
- É stateless: a resposta precisa de uma regra explícita
  - Cada direção (entrada/saída) precisa de uma regra independente, ida ≠ volta
- Avaliação em ordem numérica (regra menor tem prioridade)

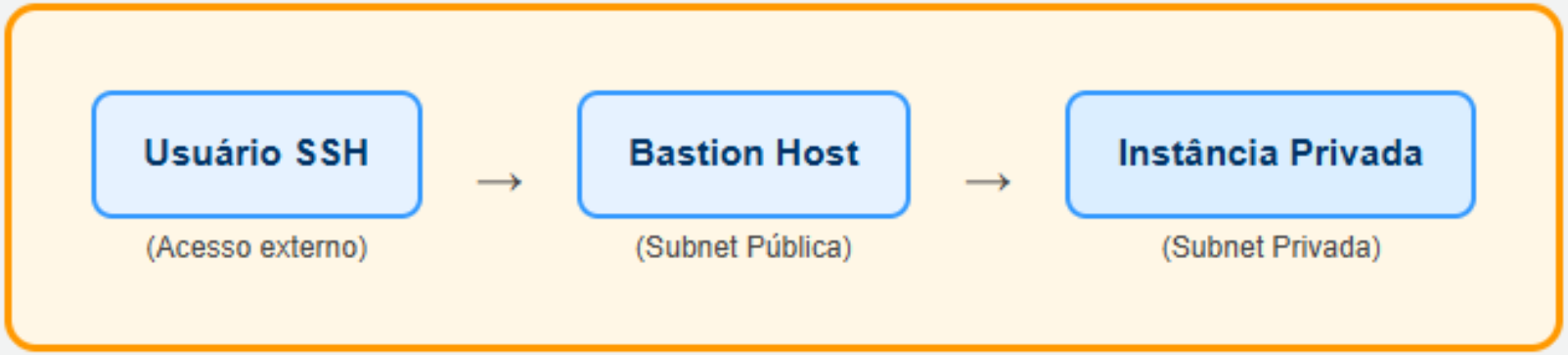


Diferença entre SG (Security Group) e NACL (Network ACL)

Característica	Security Group (SG)	Network ACL (NACL)	Dica para prova
Associação	Instância (nível de recurso)	Subnet (nível de rede)	Lembre que SG é aplicado direto na EC2
Tipo	Stateful	Stateless	Questões adoram testar essa diferença
Respostas	Permite resposta automaticamente	Precisa de regra explícita de saída e entrada	NACL: ida ≠ volta sem regra específica
Regras	Apenas permite (não nega)	Permite ou nega tráfego	Cuidado: SG não bloqueia, só permite
Ordem de Avaliação	Implícita, não configurável	Numérica: menor número tem prioridade	Números pequenos são avaliados primeiro
Uso comum	Padrão para controle de acesso	Camada adicional de segurança em rede	Ambos podem ser usados juntos

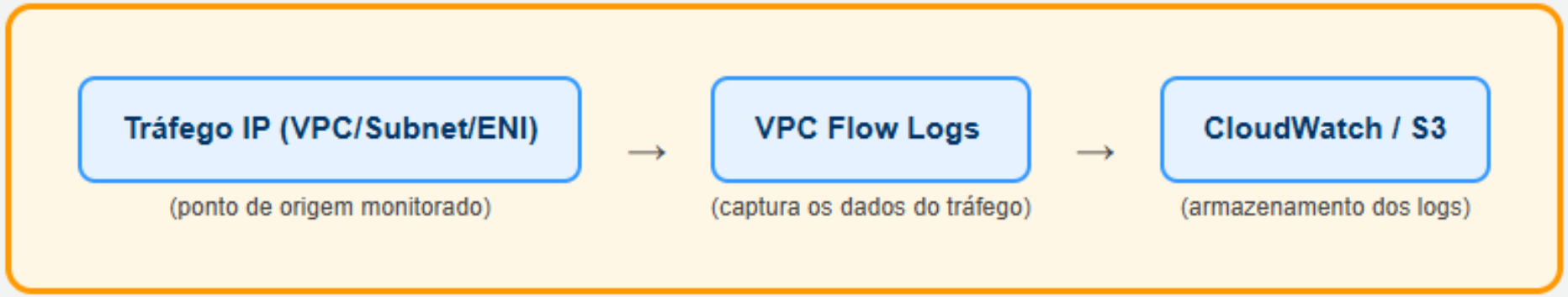
Bastion Host

- Instância EC2 pública usada para acesso SSH a instâncias privadas
- Colocado em subnet pública, com SG restrito
- Permite acesso controlado e auditável à rede privada
- Recomenda-se o uso de chaves SSH e MFA



VPC Flow Logs

- Captura informações sobre tráfego IP na VPC
- Pode ser ativado por VPC, subnet ou interface
- Logs são enviados para CloudWatch ou S3
- Útil para troubleshooting e auditoria de segurança



Boas Práticas e Dicas de Prova

- Use SGs para controle granular por instância
- Use NACLs para regras mais amplas por subnet
- Bastion Host é a ponte segura para ambientes privados
- Flow Logs ajudam a identificar anomalias e auditorias