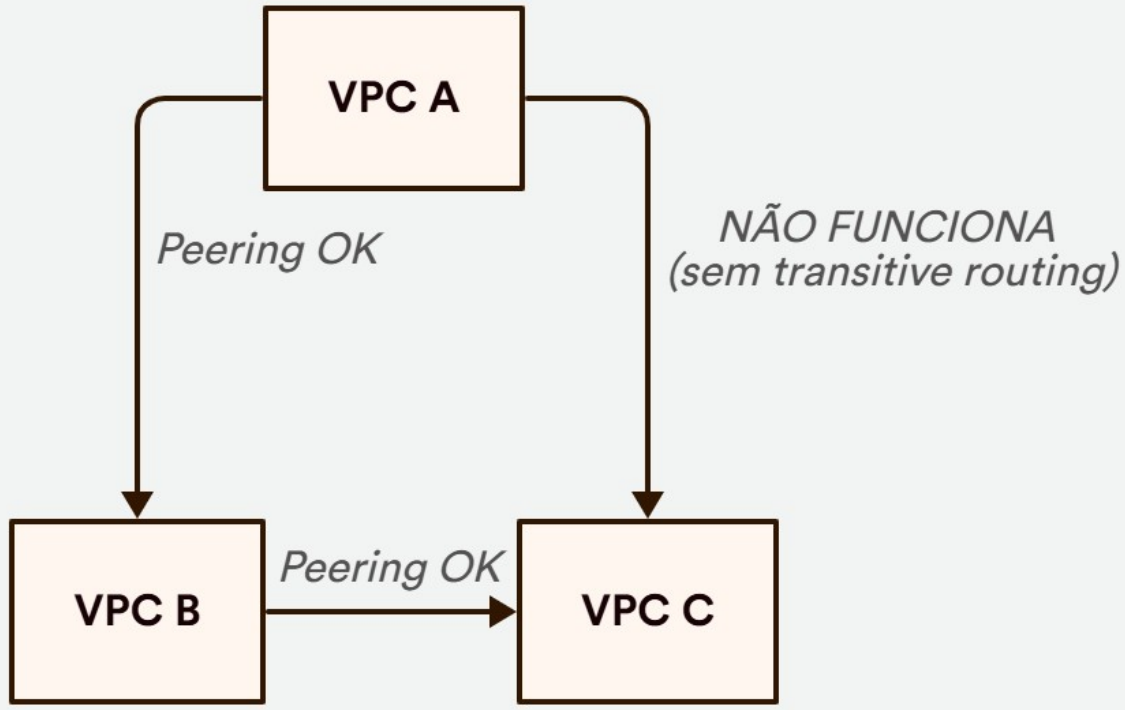
VPC Peering e Endpoints – Comunicação Privada entre VPCs e Serviços

Marlon Brehmer Anesi • Arquiteto de Soluções

VPC Peering: Conectando VPCs

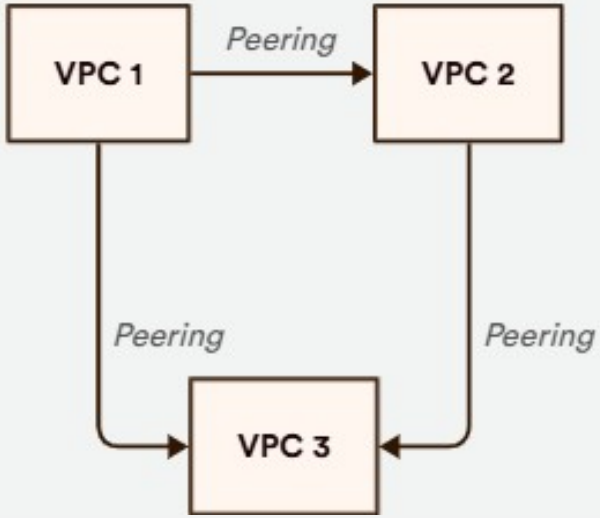
- Permite comunicação privada entre duas VPCs
- Sem necessidade de gateway, VPN ou internet
- Pode ser feito entre VPCs na mesma ou em diferentes regiões (inter-region)
- Não suporta transitive routing (A → B → C não funciona)



Considerações do VPC Peering

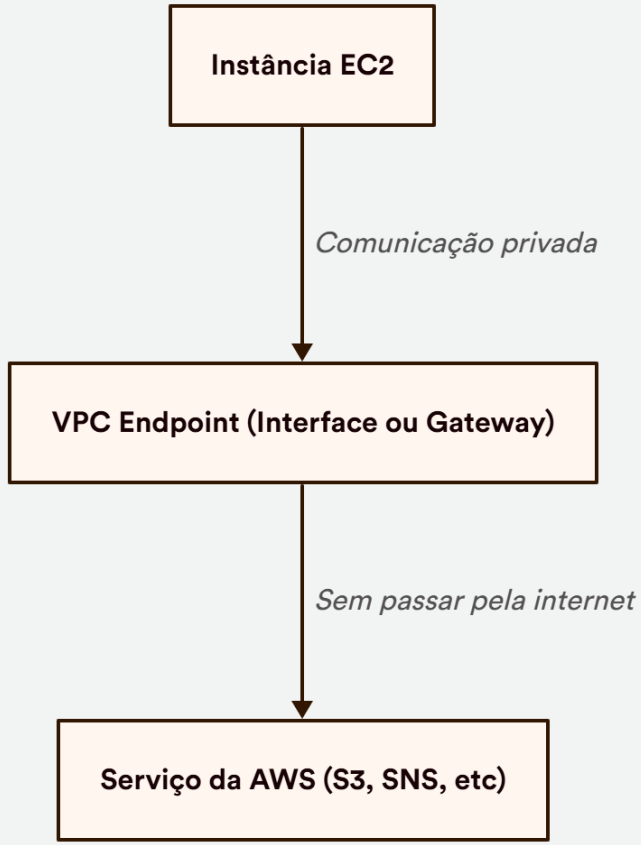
- As VPCs não podem ter blocos CIDR sobrepostos
- É necessário configurar rotas e permissões (SGs e NACLs)
- É ponto-a-ponto, exige uma conexão para cada par de VPCs
- Ideal para comunicação privada entre ambientes distintos

📌 *Para cada nova VPC que precisa se comunicar, é necessário configurar um novo peering. Isso escala de forma quadrática conforme o número de VPCs.*



VPC Endpoints

- Permitem acesso privado de uma VPC a serviços da AWS, sem usar internet
- Dois tipos: Interface Endpoints e Gateway Endpoints
- Interface: conecta a serviços via ENI, usado com SNS, SQS, etc.
- Gateway: usado com S3 e DynamoDB, integração direta com rotas



Comparativo Conceitual: Gateway vs Interface Endpoints

CATEGORIA	GATEWAY ENDPOINT	INTERFACE ENDPOINT
O que é?	Conexão privada para serviços específicos via tabela de rotas	ENI privada criada na VPC que se conecta ao serviço
Como funciona?	Adiciona rota no route table para redirecionar o tráfego	Cria uma ENI na sub-rede que representa o serviço
Casos de uso comuns	S3 e DynamoDB	SNS, SQS, API Gateway, Secrets Manager, etc.
Segurança	Permite políticas de endpoint	Permite políticas, SGs e NACLs
Custos	Gratuito (sem custo adicional por hora ou tráfego)	Custa por hora + tráfego transferido
Escalabilidade	Escala com simplicidade; sem dependência de subnets	Necessita ENIs em cada subnet usada
Dica para a prova 🧠	⚡ Se a pergunta envolver S3 ou DynamoDB → Gateway!	🔒 Se envolver ENI ou serviços com resposta bidirecional → Interface!

📌 *Tabela comparativa com colunas Gateway x Interface*

Boas Práticas e Dicas de Prova

- VPC Peering é útil para comunicação entre ambientes isolados
- Endpoints eliminam necessidade de NAT/IGW para serviços AWS
- Prefira Gateway Endpoint para S3/DynamoDB por simplicidade
- Não esqueça de atualizar as rotas e SGs após criar peering ou endpoints