

Resumo de VPC

- **VPC:** nuvem privada virtual
- **Sub-redes:** vinculadas a uma AZ, partição de rede da VPC ((dentro tem NACL))
- **Gateway de Internet:** no nível da VPC, fornece acesso à Internet
- **Gateway / Instâncias NAT:** fornece acesso à Internet para sub-redes privadas
- **ACL:** LISTA de controle de acesso à rede ((ACL)) **Network ACLs. ((ACL das Redes))**
- **NACL:** regras de sub-rede sem estado para entrada e saída ... O uso de NACL não é obrigatório

O NACL não lista usuários, ele gerencia uma lista de IPs que permite ou nega o tráfego de entrada ou saída das subnets.

- **Grupos de segurança:** stateful, operam no nível da instância EC2 ou ENI
 - **Peering de VPC:** ((conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs)) conecta duas VPC com intervalos de **Uma conexão de emparelhamento de VPC** é uma conexão de rede entre duas VPCs que permite rotear o tráfego entre elas de forma privada. A conexão de emparelhamento de VPC não é transitiva, uma conexão de emparelhamento de VPC separada deve ser feita entre duas VPCs que precisam se comunicar entre si. IP não sobrepostos, não transitivos
-
- **VPC Endpoints:** forneça acesso privado aos serviços da AWS dentro do VPC
 - **Logs de fluxo de VPC:** logs de tráfego de rede
 - **Site to Site VPN:** VPN pela Internet pública entre DC local e AWS
 - **Direct Connect:** conexão privada direta com AWS
 - **Transit Gateway:** conecta milhares de redes VPC e locais

alerta de exame:

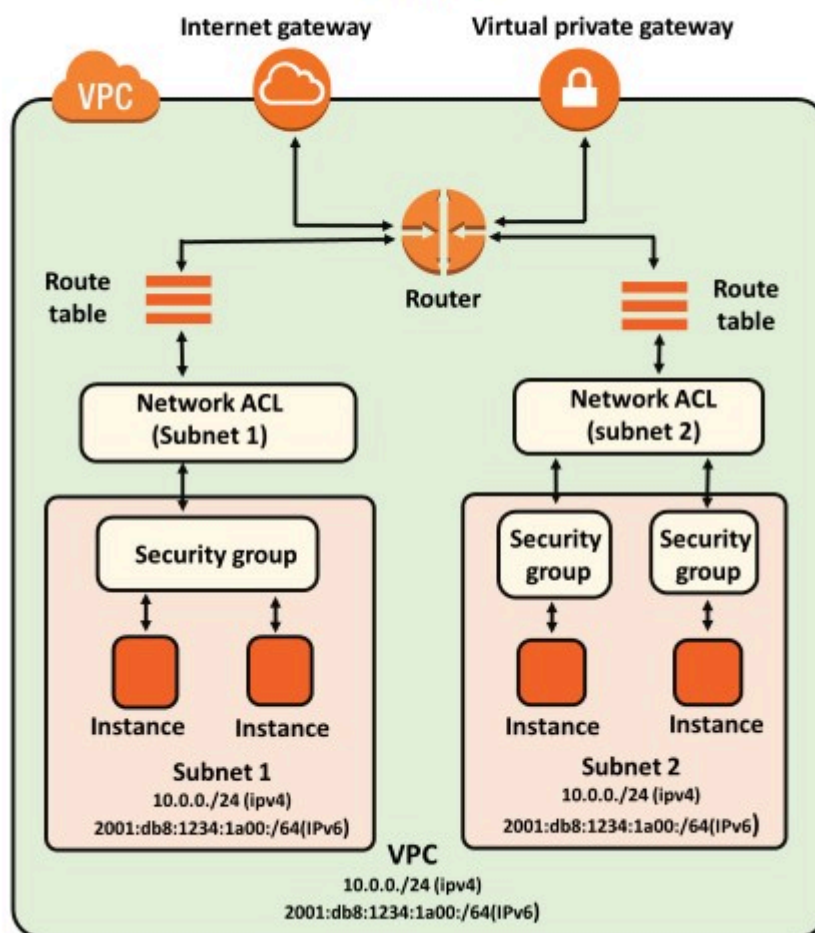
É possível que você veja uma pergunta sobre esse conceito no exame. Lembre-se de que somente o **Amazon S3 e o Amazon DynamoDB suportam o endpoint de gateway VPC**.

Todos os outros serviços que suportam VPC Endpoints usam um endpoint de interface VPC (observe que o Amazon S3 também suporta o endpoint de interface VPC).

ALERTA 2

Na VPC primeiro a ACL controla os acessos, e depois o Grupos de segurança:

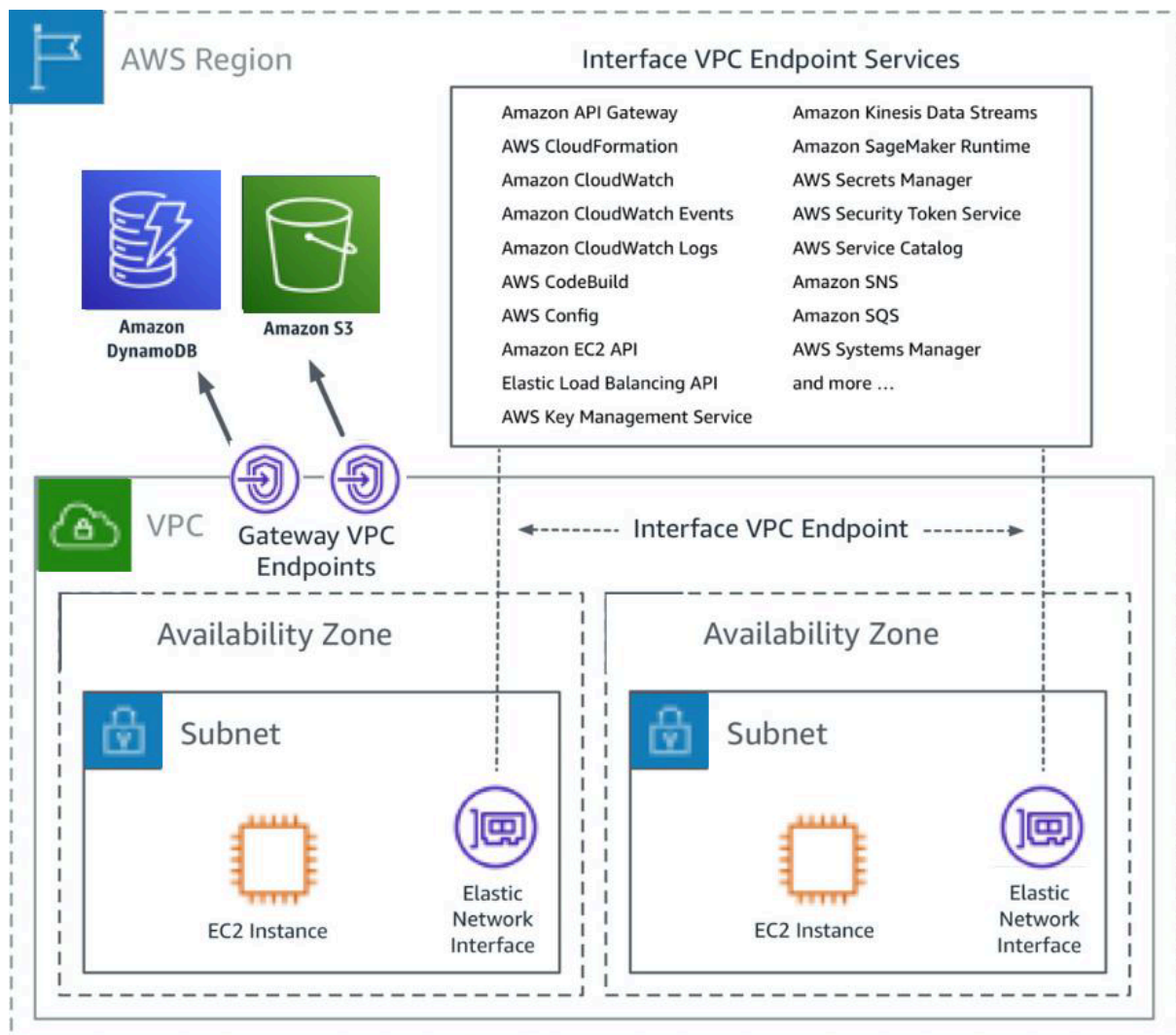
Exemplo:



Conectividade com serviços AWS usando VPC endpoints

VPC Endpoints

- Os endpoints permitem que você se conecte aos serviços da AWS usando uma rede privada em vez da rede www pública
- Isso oferece segurança aprimorada e menor latência para acessar os serviços da AWS
- Gateway de endpoint VPC: **S3 e DynamoDB**
- Interface VPC Endpoint: o resto



v3