Projeto de VPC para CANES Ltda

Grupo: Erick Calazães | Raphael Henrique | Gabriel Marques | Thalles Nascimento

1. O que é uma VPC ?

VPC é a “rede” onde você coloca seus servidores, bancos de dados, aplicações etc., com controle total sobre IPs, sub-redes, rotas e regras de segurança.

2. Visão Geral

A CANES Ltda é uma empresa que mantém um site hospedado em uma instância EC2. Seus dados de clientes são sensíveis e armazenados em um banco de dados, exigindo controle rigoroso de acesso.

Com base nisso, projetamos uma **VPC escalável, segura e altamente disponível**, que separa logicamente os recursos e implementa camadas de segurança robustas.

3. Componentes e Arquitetura da VPC

CIDR da VPC: `10.0.0.0/16`
Essa faixa foi escolhida para possibilitar criação de múltiplas sub-redes no futuro.

Sub-redes criadas:

Tipo de Sub-rede	CIDR	Função	Zona de Disponibilidade
Pública 1	10.0.0.0/24	Servidor Web (EC2)	us-east-1a
Pública 2	10.0.1.0/24	Servidor Web (EC2)	us-east-1b
Privada 1	10.0.2.0/24	Banco de Dados (RDS/EC2)	us-east-1a
Privada 2	10.0.3.0/24	Banco de Dados (RDS/EC2)	us-east-1b

Decisão: Cada sub-rede possui 256 endereços IP (prefixo /24), conforme a exigência. O uso de duas Zonas de Disponibilidade (AZs) oferece **alta disponibilidade e tolerância a falhas**.

4. Conectividade e Acesso

- **Internet Gateway (IGW):** Associado à VPC para permitir que as instâncias nas sub-redes públicas se comuniquem com a internet.
- **NAT Gateway:** Posicionado em uma sub-rede pública para que o banco de dados, que está em uma sub-rede privada, possa acessar a internet com segurança (para atualizações e patches).
- **Route Tables:**
    - Sub-redes públicas têm rotas para o IGW.
    - Sub-redes privadas têm rotas para o NAT Gateway.

Decisão: O uso do **NAT Gateway**, em vez de uma NAT Instance, garante melhor desempenho, alta disponibilidade automática e menor manutenção.

5. Segurança e Firewalls

- **Security Groups (SG):**
    - Web Server SG:
        - Libera as portas **80 (HTTP)** e **443 (HTTPS)** para acesso público.
        - Acesso SSH (**porta 22**) limitado ao IP fixo do administrador.
    - DB Server SG:
        - Só permite conexões vindas do Web Server SG.
        - Não aceita acessos diretos da internet.
- **NACLs (Network ACLs):**
    - Personalizadas para permitir/recusar tráfego de sub-redes específicas.
    - Controlam tráfego de entrada e saída por IP e porta.

Decisão: Implementar **dupla camada de segurança** com SGs e NACLs cria uma estrutura de defesa em profundidade, seguindo boas práticas da AWS.

6. Alta Disponibilidade

A arquitetura distribui os recursos entre **duas Zonas de Disponibilidade (AZs)**:

- Web Servers em us-east-1a e us-east-1b.
- Banco de Dados em us-east-1a e us-east-1b.

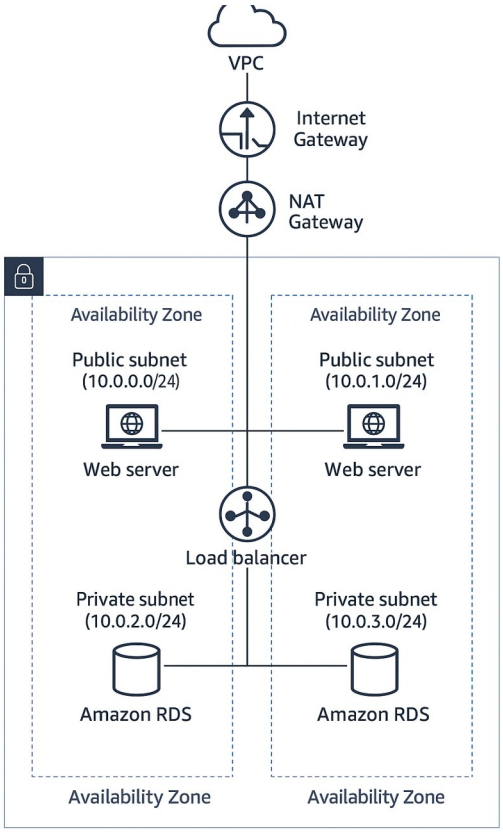
Decisão: Essa estratégia permite que, caso uma zona falhe, a outra continue funcionando, reduzindo o downtime e aumentando a confiabilidade do ambiente.

7. Recursos AWS Envolvidos

- Amazon VPC
- Sub-redes Públicas e Privadas
- Internet Gateway e NAT Gateway
- Security Groups e NACLs
- Tabelas de Roteamento
- Amazon EC2 para o servidor Web
- Amazon RDS ou EC2 para o banco de dados (dependendo da escolha final da arquitetura)

8. Diagrama da Arquitetura

- Sub-redes distintas para Web e Banco de Dados
- Cada sub-rede com 256 IPs (/24)
- Web acessível ao público
- Banco com acesso à internet via NAT Gateway
- Alta disponibilidade com uso de múltiplas AZs
- Camadas de firewall personalizadas (SG + NACL)



9. Conformidade com os Requisitos

✔ Servidor web e banco em sub-redes separadas
✔ Rede começa em 10.0.0.0 com sub-redes de 256 IPs
✔ Acesso público ao servidor web
✔ Banco com acesso à Internet via NAT Gateway
✔ Alta disponibilidade e firewalls personalizados

10. Observações Finais

Segurança foi prioridade: separação de camadas, uso de NAT e camadas de firewall.

Escalabilidade: A VPC foi criada com um bloco grande (/16) para permitir expansão futura.

Manutenção simplificada: Uso de recursos gerenciados (NAT Gateway, RDS) quando possível.

Alta disponibilidade e redundância: Uso de AZs distintas e estrutura pronta para balanceamento de carga (caso necessário no futuro).