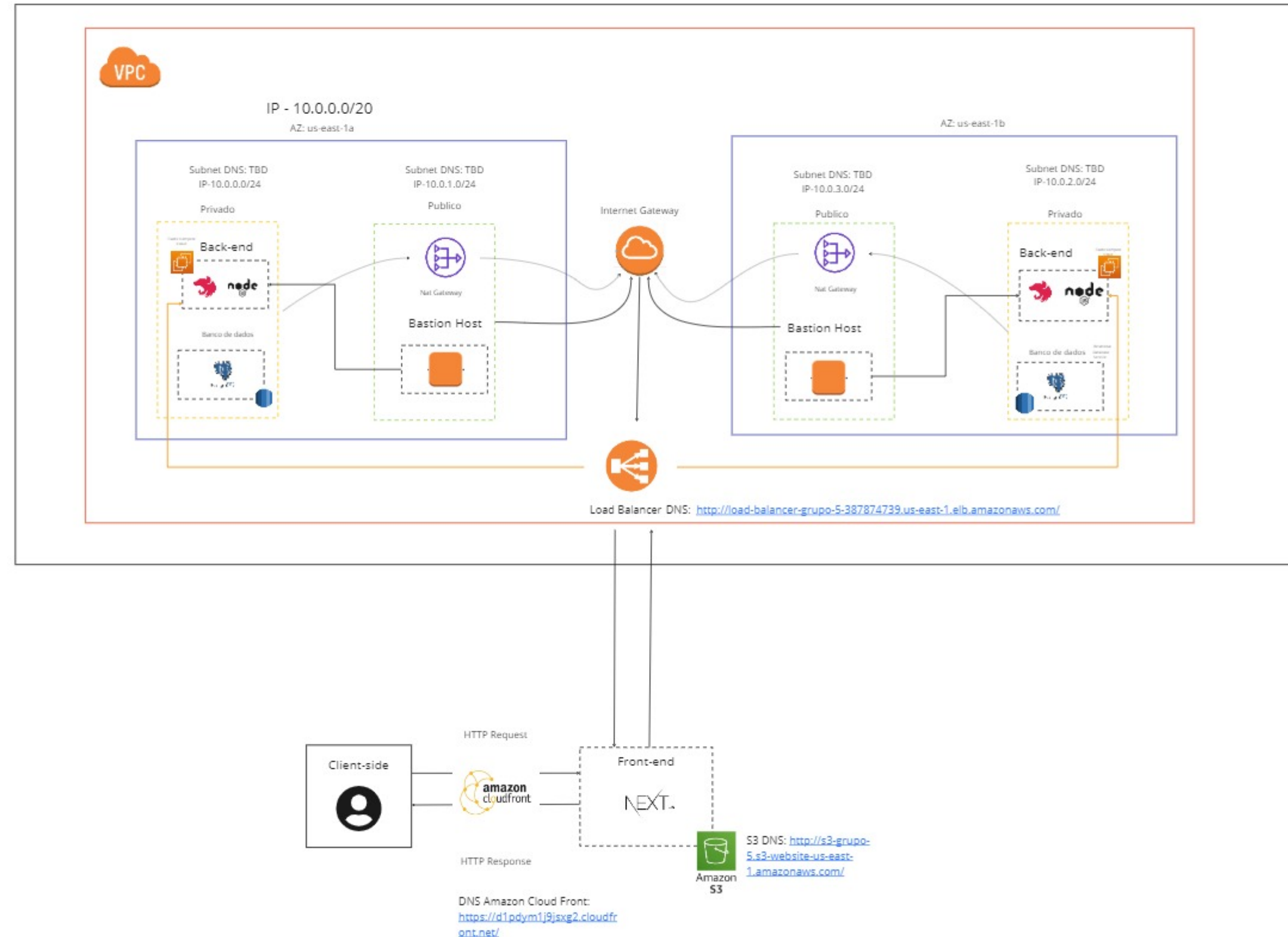


Server-side



Nessa arquitetura, temos a mesma estrutura para duas AZ's (Availability Zones), por causa da questão de escalabilidade e disponibilidade. Temos a zona um com o nome us-east-1a e a segunda com us-east-1b.

Zona 1 - us-east-1a

Zona 2 - us-east-1b

Cada subrede pública contém uma máquina virtual EC2 com uma instância de bastion host para fornecer um ponto de entrada seguro para acessar as instâncias na subrede privada.

Zona 1 - us-east-1a

- Pública: IP-10.0.0.0/24
- Privada: IP-10.0.1.0/24

Zona 2 - us-east-1b

- Pública: IP-10.0.3.0/24
- Privada: IP-10.0.2.0/24

Além disso, as redes descritas como privadas, não conseguem ser acessadas de fora da rede, já que diferente das subredes públicas, elas não possuem conexão com o Internet Gateway, e sim com o Nat Gateway, que possibilita apenas uma rota de saída para a Internet. Para acessar as instâncias privadas, onde estará o back-end e o banco de dados da aplicação, basta entrar na Máquina pública (através do ssh e da chave de segurança), e então a partir do bastion host se pode acessar ambas as Máquinas privadas (também através do ssh e uso da chave de segurança).

O bloco CIDR da VPC é 10.0.0.0/20, dessa forma teremos uma limitação de 4000 IPs para essa rede. Já suas subredes, possuem o bloco CIDR de 10.0.0.0/24, são 256 IPs.