AWS 3-TIER ARCHITECTURE

External Browser

AWS Region

Route 53

Cloud Front → S3

I/Gw

VPC

Availability Zone 1

Public Subnet 1

NAT G/w or Instance

Internet Facing ALB

Listen: 80, 443

Availability Zone 2

Public Subnet 2

Bastion Host

Private Subnet 1

EC2

Auto scaling group - web tier

Private Subnet 2

EC2

Internal Facing ALB

Listen: 1234

EC2

Auto scaling group - app tier

EC2

RDS (primary)

Synchronization
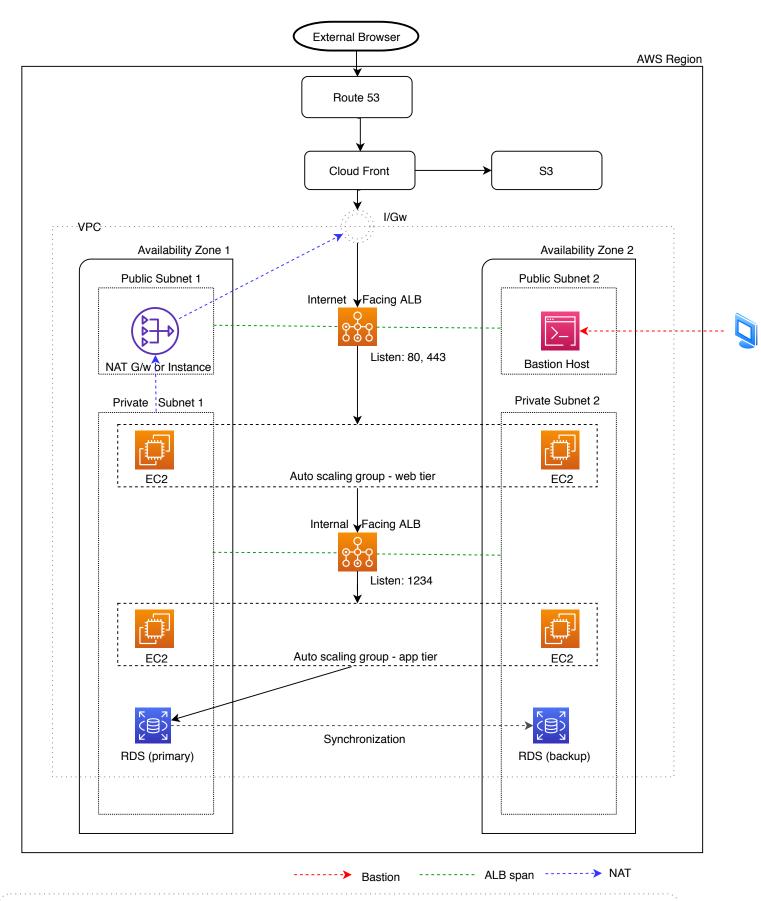
RDS (backup)

--------→ Bastion   --------- ALB span   --------→ NAT

Security Group 1 - Bastion - Port 22; All Inbound
Security Group 2 - Web tier ALB - Port 80, 443; All Inbound
Security Group 3 - App tier ALB - Port 1234 (Backend port example); SG2 Inbound
Security Group 4 - DB tier - Port 3306 (MySQL RDS example); SG3 Inbound