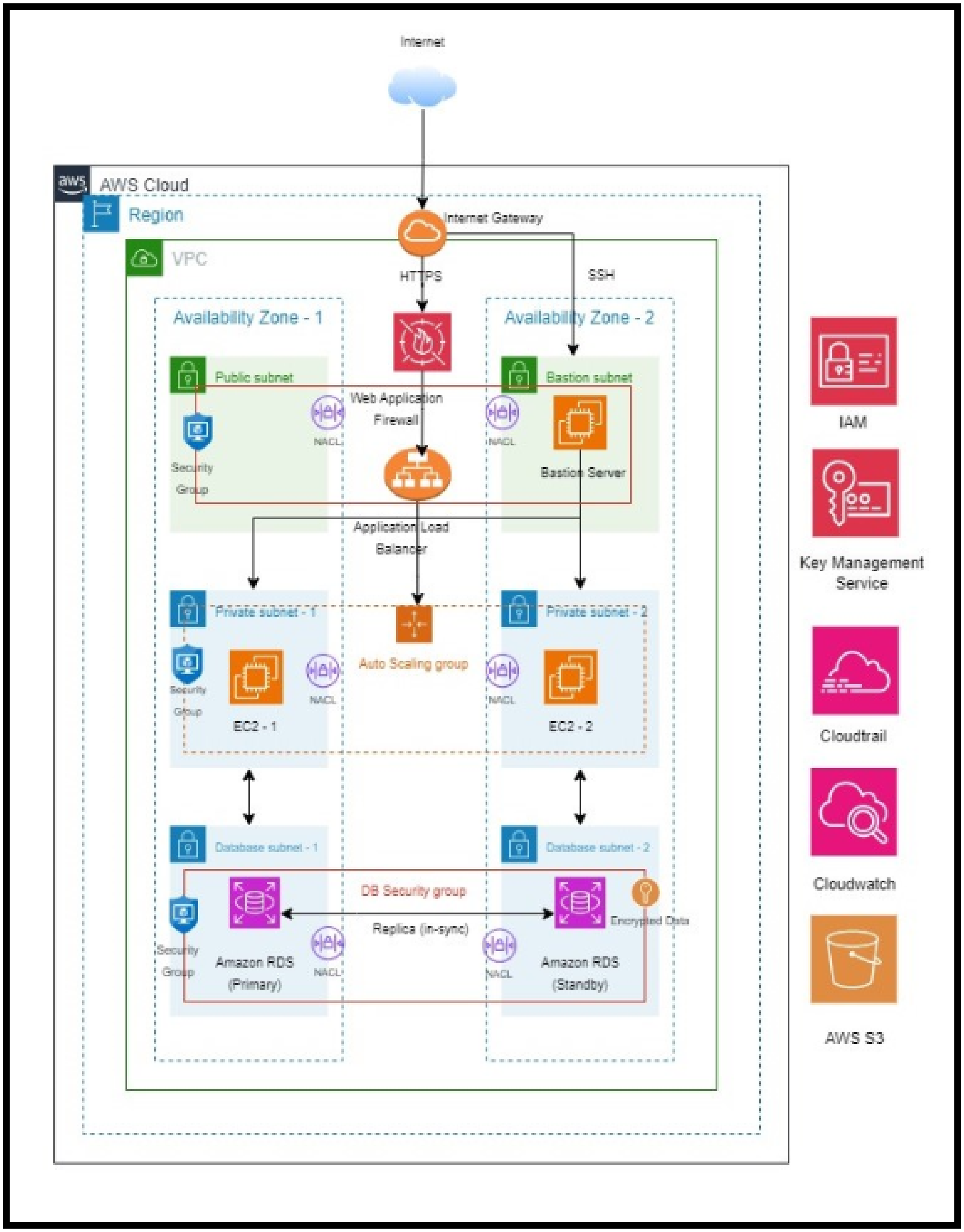
AWS Architecture

Architecture Diagram

A detailed architecture diagram showcasing the various components, their interactions, and the security mechanisms in place.



Description

This architecture sets up a VPC inside an AWS Region with total 6 subnets in two Availability Zones (AZs). Each AZ contains two Public, two Private, and two Database subnets. It includes an Application Load Balancer (ALB)-based web access mechanism and a secure access way through a Bastion host for instances in private subnets.

Components

1. **VPC:** A virtual private cloud that offers a private area of the AWS cloud.
2. **Subnets:**
   - **Public Subnets:** Exposed to the internet and contains an ALB and the Bastion Server.
   - **Private Subnets:** Isolated from the internet and contains the EC2 instances.
   - **Database Subnets:** Specifically dedicated for the RDS database instances.
3. **Security Groups:** Control inbound and outbound traffic by acting as virtual firewalls.
   - **public_sg:** Allows inbound HTTPS and SSH.
   - **private_sg:** Receives traffic from the ALB and the Bastion Server.
   - **db_sg:** Secures database instances by limiting access only from the linked private subnet.
4. **NACLs (Network Access Control Lists):** Act as an additional layer of security, working at the subnet level.
5. **EC2 Instances:** Virtual servers in the AWS cloud.
   - **Bastion Host:** Serves as a jump server for securely accessing instances in private subnets.
   - **Application Instances:** Located within the private subnets.
6. **ALB (Application Load Balancer):** Distributes incoming HTTP/HTTPS traffic among application instances.
7. **WAF (Web Application Firewall):** Provides a firewall to protect the application from web-based threats.
8. **RDS (Relational Database Service):** Managed relational database service with primary and backup instances spread across two subnets for high availability.
9. **Additional AWS Services:**
   - **KMS (Key Management Service):** Manages cryptographic keys.
   - **IAM (Identity and Access Management):** Manage access of AWS resources.
   - **CloudTrail:** Records AWS API calls, delivering log files.
   - **CloudWatch:** Monitors AWS applications and resources.
   - **S3:** Store logs and other important files.

Step-by-step Working of the Application

1. User Request

1. **HTTPS Request:** A user sends an HTTPS request to the application using their web browser.
2. **SSH Request:** Alternatively, a system administrator would initiate an SSH request if they wanted to SSH into an EC2 instance for maintenance or checks.

2. Internet Gateway

The Internet Gateway is where incoming traffic to the VPC initially arrives. It serves as a link between the public Internet and the internal network of AWS.

3. Traffic Filtering with WAF (for HTTPS Requests)

1. If the request is HTTPS, it is first routed through the Web Application Firewall (WAF).
2. WAF inspects the traffic for malicious patterns. If something suspicious is identified, the request may be blocked according to the restrictions in place.

4. Application Load Balancer (ALB)

1. The ALB receives the inspected HTTPS traffic from the Web Application Firewall (WAF).
2. ALB then distributes & routes the incoming traffic to the EC2 instances situated within the private subnets.

5. IAM Authentication & Authorization

1. IAM roles tied to resources (such EC2 instances or RDS) decide the permissions these resources have as they interact within AWS. For example, an EC2 may have access to read from an S3 bucket or write to an RDS instance.
2. IAM users will have specific rights, responsibilities, and rules that govern what AWS resources they may access and actions they can do.

6. Data Encryption with KMS

1. It is necessary to encrypt data before it is written to or stored on the RDS instances.
2. KMS is a cryptographic key management system. KMS supplies the encryption key when data is encrypted. KMS supplies the decryption key when data needs to be read or decrypted.
3. This ensures that even if the data is accessed maliciously, it remains secure and unreadable in the absence of the relevant key.

7. Security Groups & NACLs

1. Security Groups serve as a firewall at the EC2 instance level. What traffic is allowed in and out is defined by them.
2. NACLs are an extra security layer that operates on a subnet level. Depending on the situation, they can approve or reject traffic.

8. EC2 Instances & Database Interaction

1. **Public Subnet:** For SSH requests, users can connect to the Bastion Server to securely SSH into instances inside the private subnets.
2. **Private Subnet:** HTTPS requests reach one of the EC2 instances. The application handles the request and, if necessary, interfaces with the associated database.
3. **RDS Operation:** The database request is handled by the RDS instance. Changes are copied to the other RDS instance to ensure data persistence.

9. Response to User

1. The EC2 instance prepares a response. It is routed back through the ALB, optionally inspected by the WAF, and then routed out through the Internet Gateway.
2. The received data is shown in the user's browser.

10. Monitoring & Logging

1. **CloudTrail:** Logs all AWS API calls and activities and stores in S3.
2. **CloudWatch:** Monitors resources, like EC2 instances and RDS, and can alert based on given conditions.