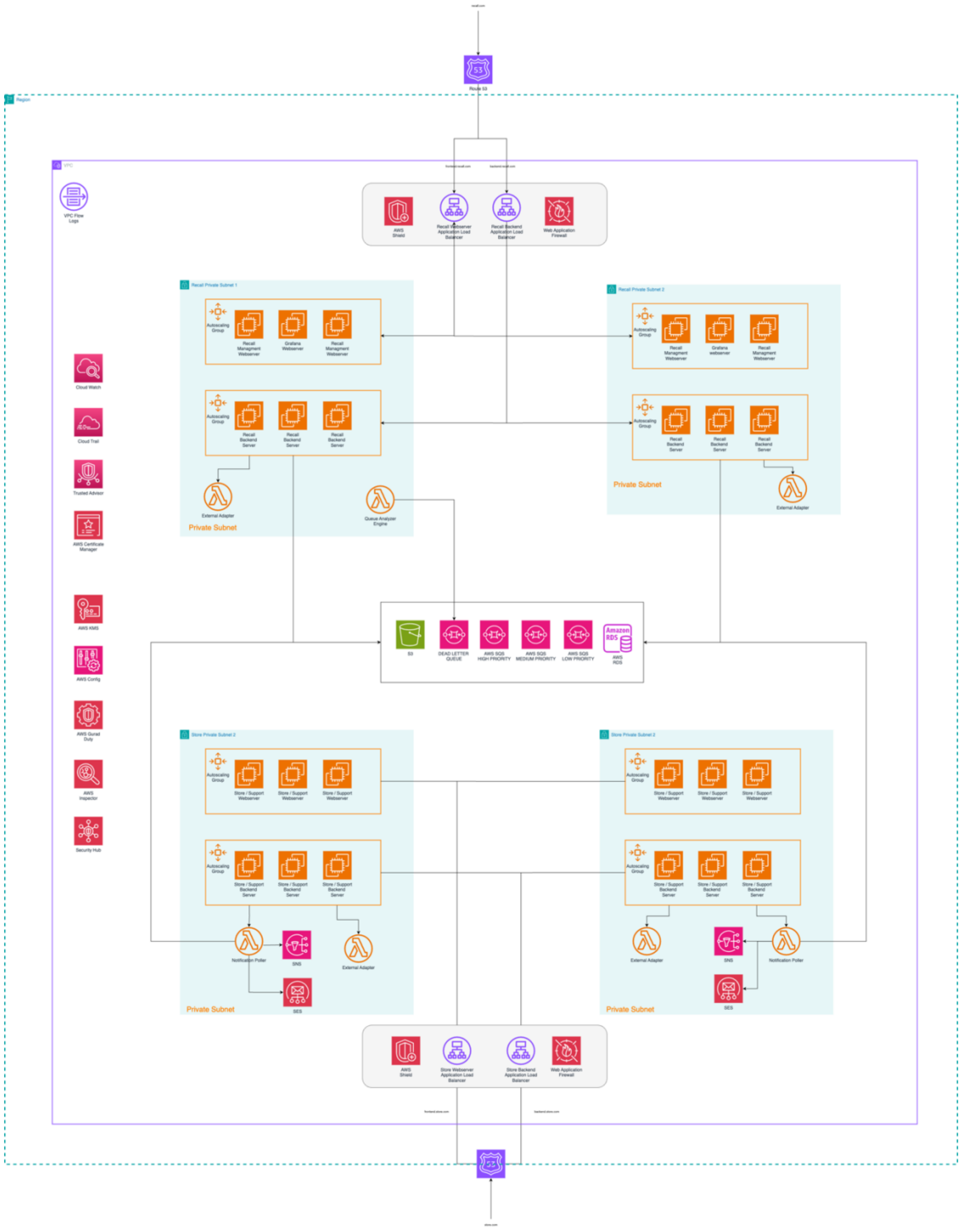
SECURITY OVERVIEW



1. Identity and Access Management (IAM): AWS IAM would be used to control who is authenticated (signed in) and authorized (has permissions) to use resources. IAM policies would grant permissions to actions and resources at a granular level for users, groups, and roles.

2. Amazon Virtual Private Cloud (VPC): The entire system would be housed within a VPC, creating a secure, isolated section of the AWS Cloud. Network Access Control Lists (NACLs) and Security Groups would be employed to control inbound and outbound traffic to the subnets and instances, respectively.

3. Subnetting and Network Segmentation: The system would be architected using both public and private subnets, ensuring that the public-facing components (like the ALBs) are isolated from the back-end systems that manage the recall process.

4. Encryption:

- **At Rest:** AWS services like RDS, S3, and EFS would be configured to use encryption-at-rest to protect stored data. AWS Key Management Service (KMS) would manage keys for this purpose.
- **In Transit:** All data transmitted over the internet would be protected using SSL/TLS, possibly managed with AWS Certificate Manager (ACM).

5. AWS WAF and AWS Shield: Web Application Firewall (WAF) and Shield would be used to protect the application from common web exploits and DDoS attacks, respectively.

6. Amazon Cognito: For user-facing components, Cognito would provide user sign-up, sign-in, and access control to web and mobile apps quickly and securely.

7. CloudTrail: AWS CloudTrail would log and retain account activity related to actions across the AWS infrastructure, providing a history of AWS API calls for the account.

8. CloudWatch: For monitoring the operational health of AWS services and applications, providing logs, metrics, and event data.

9. Route 53 DNSSEC: Protects the domain names of the application's endpoints using DNS Security Extensions (DNSSEC) to authenticate responses to domain name lookups.

10. AWS Config: To assess, audit, and evaluate the configurations of AWS resources, providing a detailed view of the configuration of AWS resources in the AWS account, including how resources are related to one another and how they were configured in the past.

11. AWS GuardDuty: It's a threat detection service that continuously monitors for malicious or unauthorized behavior to protect your AWS accounts and workloads. GuardDuty analyzes events across multiple AWS data sources, such as VPC flow logs, CloudTrail, and DNS logs.

12. AWS WAF: This is an application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules.

13. AWS Shield: A managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

14. AWS Inspector: An automated security assessment service that helps improve the security and compliance of applications deployed on AWS. AWS Inspector automatically assesses applications for vulnerabilities or deviations from best practices, including exposure to open ports and detection of common vulnerabilities and exposures.

15. AWS Security Hub: This service provides a comprehensive view of your security state within AWS and helps you check your environment against security industry standards and best practices. Security Hub aggregates, organizes, and prioritizes security alerts or findings from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie.

16. VPC Flow Logs: Capture information about the IP traffic going to and from network interfaces in your VPC. Flow logs can be created at the VPC, subnet, or network interface level and used to monitor and troubleshoot connectivity and security issues, and to make sure that network traffic is in compliance with your security policies.