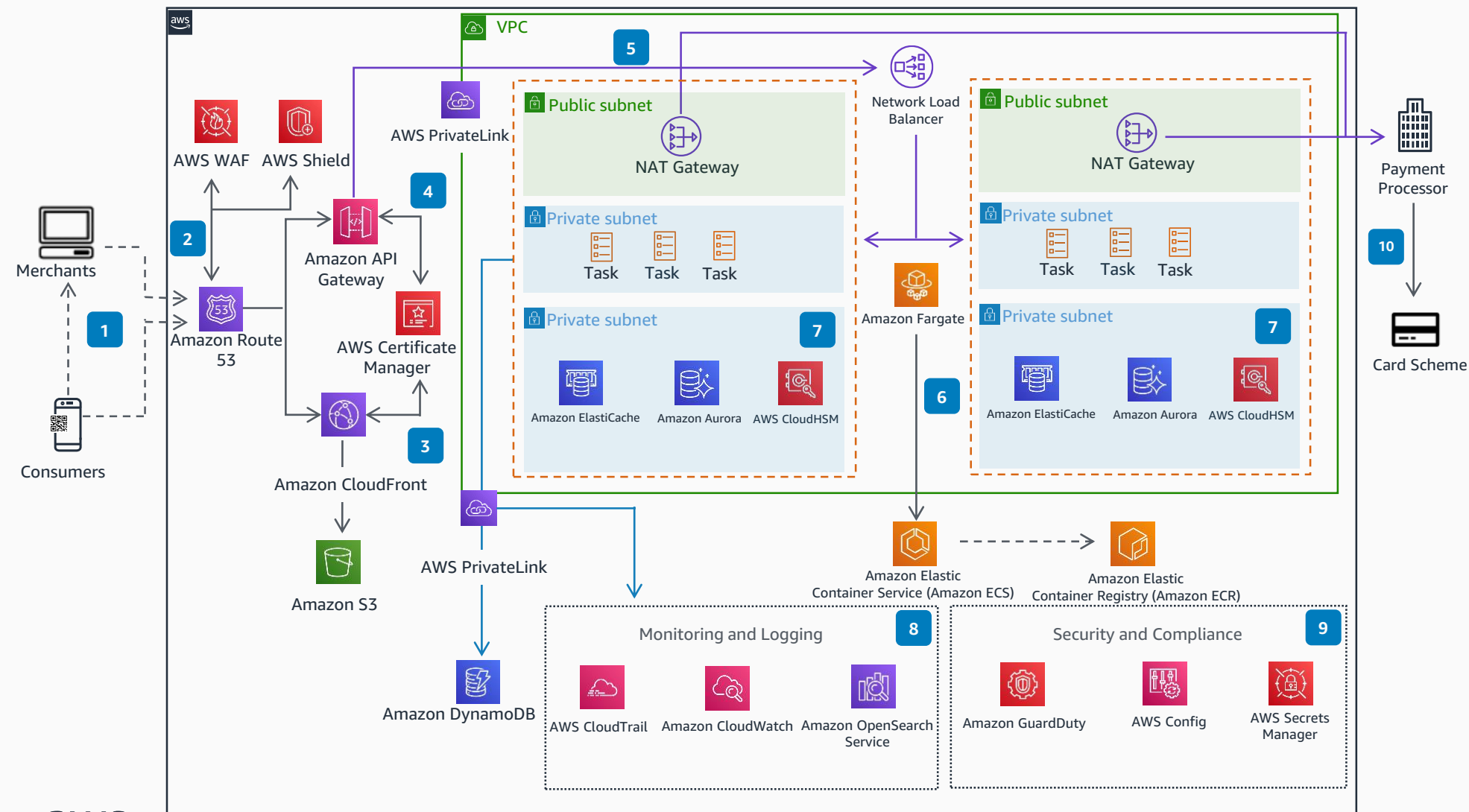


Guidance for Payment Connectivity, Gateway, Orchestration, and Routing on AWS

This reference architecture displays how a quick response (QR) or wallet payment traverses through various components.



- 1 To start, customers scan the business QR code displayed at the checkout page on a website or at the point of sale (POS) terminal.
- 2 **Amazon Route 53** routes traffic to an **Amazon API Gateway** endpoint where **Amazon CloudFront** distributes dynamic and static content. AWS security services such as **AWS WAF** and **AWS Shield** protect the web applications from common application-layer exploits and against distributed denial-of-service (DDoS) attacks.
- 3 **CloudFront** content delivery network (CDN) is used to return resources found in its cache and static resources from **Amazon Simple Storage Service** (Amazon S3).
- 4 **Amazon API Gateway** and **Amazon CloudFront** can be seamlessly integrated with **AWS Certificate Manager**. These services manage the complexity of creating, storing, and renewing public and private SSL/TLS X.509 certificates and keys that protect your applications.
- 5 The request is routed through a Network Load Balancer to distribute incoming traffic across its healthy registered targets.
- 6 Payment request is processed at application layer using **Amazon Elastic Container Service** (Amazon ECS) that deploys tasks on **AWS Fargate**.
- 7 Payment transaction information is stored in **Amazon Aurora** or **Amazon DynamoDB**. **Amazon ElastiCache** is used as a session store to manage session information in payment processing. **AWS CloudHSM** is a cryptographic service for creating and maintaining hardware security modules (HSMs).
- 8 Service logs are collected in **Amazon S3** and analyzed and monitored using **Amazon OpenSearch Service**.
- 9 At the security and compliance layer, **AWS Config** evaluates, assesses, and audits configurations of resources. **Amazon GuardDuty** monitors for malicious activity and unauthorized behavior, protecting AWS accounts and workloads. **AWS Secrets Manager** helps protect secrets needed to access applications, services, and IT resources.
- 10 Payment request outbound traffic is sent to the payment processor through a NAT Gateway that is connected to card schemes for verification.

