How it works :

Key Components & Justifications

1. Firewalls (3+)

- Purpose:
  - Network Firewall (Firewall 1) : Filters incoming/outgoing traffic at the perimeter (e.g., block non-HTTP/HTTPS ports).
  - Host-Based Firewalls (Firewalls 2–4) : Restrict access to services on each server (e.g., allow only SSH and HTTP/HTTPS).
- Why : Firewalls prevent unauthorized access, block malicious traffic, and enforce security policies.

2. SSL Certificate & HTTPS

- Implementation : Terminate SSL at the load balancer using a single certificate for www.foobar.com.
- Why HTTPS :
  - Encrypts data in transit, preventing eavesdropping.
  - Ensures integrity and authenticity of communications.
  - Required for modern security standards (e.g., PCI compliance).

3. Monitoring Clients

- Tool Example : Sumo Logic or Datadog agents installed on each server.
- Purpose:
  - Collect metrics (CPU, memory, disk I/O).
  - Track application logs and network traffic.
  - Alert on anomalies (e.g., high error rates).
- Data Collection: Agents send metrics/logs to a centralized dashboard via HTTPS/API.

Critical Infrastructure Details

Monitoring Web Server QPS

1. Use tools like Prometheus or Datadog to track requests per second (QPS).
2. Configure the load balancer to log request rates.

3. Set alerts for QPS spikes/drops (e.g., using Sumo Logic’s anomaly detection).

Issues with This Design

1. SSL Termination at the Load Balancer

- Risk : Traffic between the load balancer and backend servers is unencrypted (HTTP), exposing data if the internal network is compromised.
- Fix : Use end-to-end TLS (HTTPS between LB and servers) or mutual TLS.

2. Single MySQL Write Server

- Risk : A single point of failure. If the master database crashes, writes are blocked.
- Fix : Implement a master-replica setup with automatic failover.

3. Identical Components on All Servers

- Risk :
  - Resource contention (e.g., database and web server competing for CPU).
  - Difficult to scale individual layers (web vs. app vs. database).
- Fix : Separate services into dedicated tiers (web servers, app servers, database cluster)