Secured and Monitored Web Infrastructure - Essential Concepts

1. Secured and Monitored Web Infrastructure:

Design:
- 3 Servers
- 3 Firewalls
- 1 SSL Certificate (HTTPS)
- 3 Monitoring Clients (Sumo Logic or similar)

2. Firewalls:

Purpose:
- Protect servers from unauthorized access and cyber threats.
- Filter incoming and outgoing network traffic based on predefined rules.

3. SSL Certificate (HTTPS):

Purpose:
- Encrypts data exchanged between users and the website, enhancing security.
- Verifies the authenticity of the website, ensuring user trust.

4. Monitoring:

Purpose:
- Monitors infrastructure health, performance, and security.

- Detects issues proactively and aids in timely troubleshooting.

Monitoring Clients:

- Data Collectors: Gather system metrics, logs, and performance data.
- Sumo Logic or Similar: Analyze and visualize collected data for insights.

Monitoring Web Server QPS:

- Track the query per second (QPS) metric through monitoring tools.
- Identify patterns and potential issues in traffic volume.

Issues with this Infrastructure:

1. Terminating SSL at Load Balancer Level:

- Decryption at the load balancer can expose data to potential attacks.
- Recommend end-to-end encryption from user to the application server.

2. Single MySQL Server for Writes:

- Single point of failure if the MySQL server fails.
- Implement a replication setup to ensure redundancy and failover.

3. Uniform Server Components:

- Similar server components lack diversification.
- Vulnerability in one component may affect all servers.