2. Secured and monitored web infrastructure

1. Additional Elements:

3 Firewalls: To control and secure incoming and outgoing traffic to and from the servers.

SSL Certificate: To serve www.foobar.com over HTTPS, ensuring encrypted communication between clients and the server.

3 Monitoring Clients: To collect data on server performance, security, and availability.

2. Reasoning for Each Element:

Firewalls: Added to enforce security policies, restrict unauthorized access, and protect against various cyber threats.

SSL Certificate: HTTPS encrypts traffic between clients and the server, preventing interception and manipulation of sensitive data during transmission.

Monitoring Clients: Used to monitor server performance, detect anomalies, troubleshoot issues, and ensure high availability of the web infrastructure.

3. Specifics about the Infrastructure:

Traffic over HTTPS: HTTPS encrypts data transmitted between clients and the server, preventing eavesdropping and data tampering. It's essential for securing sensitive information such as login credentials, payment details, etc.

Monitoring Purpose: Monitoring tools collect data on various metrics such as server CPU usage, memory usage, disk space, network traffic, error logs, etc., to ensure optimal performance, identify potential issues, and facilitate troubleshooting.

Data Collection by Monitoring Tool: Monitoring tools collect data by deploying agents or clients on servers, which continuously gather metrics and send them to a centralized monitoring server or cloud platform for analysis and visualization.

4. Monitoring QPS (Queries Per Second):

To monitor web server QPS, you can configure monitoring clients to collect and analyze metrics related to incoming HTTP requests and responses.

Monitoring tools can track the number of requests received by the web server per second, response times, error rates, etc., to assess server performance and identify potential bottlenecks.

5. Issues with the Infrastructure:

Terminating SSL at Load Balancer Level: Terminating SSL at the load balancer exposes decrypted traffic within the internal network, potentially compromising data security.

Single MySQL Server Handling Writes: Having only one MySQL server capable of accepting writes introduces a single point of failure and may lead to data loss or service interruptions in case of server failure.

Identical Components Across Servers: Having servers with identical components (database, web server, and application server) might lead to a lack of fault tolerance and scalability. Introducing diversity in server roles and configurations can enhance resilience and optimize resource utilization.