2. Secured and monitored web infrastructure

Infrastructure Design:

Additional Elements and Reasons:

1. **Three Firewalls:**

Reason: Added for enhanced security by controlling incoming and outgoing traffic, preventing unauthorised access and potential threats.

2. **SSL Certificate for HTTPS:**

Reason: Implemented to encrypt data between clients and servers, ensuring secure and private communication, particularly important for sensitive information.

3. **Three Monitoring Clients:**

Reason: Deployed to actively observe and collect performance metrics, system health, and potential issues for proactive troubleshooting and maintenance.

Specifics About Each Element:

Firewalls:

Purpose: Firewalls are added to control and filter incoming and outgoing network traffic, serving as a barrier against unauthorised access and potential security threats.

SSL Certificate (HTTPS):

Purpose: HTTPS encrypts data transmitted between clients and servers, ensuring confidentiality and integrity, especially crucial for protecting user data during sensitive transactions.

Monitoring:

Purpose: Monitoring tools track system performance, detect anomalies, and provide insights into resource utilisation. This proactive approach helps prevent potential issues and ensures optimal performance.

Monitoring Tool Data Collection:

Method: Monitoring tools like Sumo Logic collect data through agents installed on servers, actively gathering information on metrics, logs, and events.

Web Server QPS Monitoring:

Action: To monitor Web Server QPS (Queries Per Second), set up monitoring tools to track incoming requests, analyse traffic patterns, and identify performance bottlenecks.

Issues with the Infrastructure:

SSL Termination at Load Balancer:

Issue: Terminating SSL at the load balancer might expose unencrypted traffic within the internal network, compromising security. SSL termination is ideally performed at the web servers.

Single MySQL Server for Writes:

Issue: Relying on a single MySQL server for write operations introduces a Single Point of Failure (SPOF), where a failure in the MySQL server could lead to data inconsistency or loss.

Identical Components on All Servers:

Issue: Having servers with identical components may lead to a lack of diversity and redundancy, making the entire infrastructure vulnerable to simultaneous failures or issues affecting all servers.