ALX - Web Infrastructure Design
2-secured_and_monitored_web_infrastructure

Reasons for Adding Additional Elements:

Firewalls: Firewalls are added to provide a layer of security by controlling incoming and outgoing network traffic. They help prevent unauthorized access and mitigate potential threats.

SSL Certificate and HTTPS: An SSL certificate is used to establish HTTPS, ensuring encrypted communication between users' browsers and the server. This encryption enhances data privacy and security during transmission.

Monitoring: Monitoring tools are implemented to keep track of the infrastructure's performance, resource utilization, and potential issues. They aid in maintaining optimal system health and detecting and resolving problems in a timely manner.

Role of Firewalls:

Firewalls act as a barrier between a trusted internal network and potentially untrusted external networks. They regulate traffic flow, block malicious attempts, and safeguard sensitive data from unauthorized access.

Role of HTTPS:

HTTPS ensures secure communication between users and the server by encrypting data during transmission. This prevents eavesdropping and data tampering, especially critical for protecting sensitive information like login credentials and financial data.

Purpose of Monitoring:

Monitoring serves to maintain the health and performance of the infrastructure. It helps in identifying anomalies, diagnosing bottlenecks, and proactively addressing issues to ensure uninterrupted service and optimal user experience.

Data Collection by Monitoring Tool:

Monitoring tools collect data through agents or agents that are deployed on various servers. These agents gather metrics such as CPU usage, memory consumption, network traffic, response times, and more. The collected data is then sent to a centralized monitoring system for analysis and reporting.

Monitoring Web Server QPS:

To monitor web server QPS (Queries Per Second):

Install a monitoring agent on the web server.
Configure the agent to track the number of incoming requests over a specific time frame.
The agent aggregates this data and sends it to the monitoring system.
Use the monitoring system's interface to view and analyze the QPS trends.
Issues with the Infrastructure:

Terminating SSL at Load Balancer: Terminating SSL at the load balancer level can expose sensitive data within the internal network, reducing overall security. End-to-end SSL encryption ensures data protection throughout the entire communication path.

Single MySQL Server for Writes: Relying on a single MySQL server for write operations creates a single point of failure. If the server becomes unavailable, write operations cease, disrupting the application's functionality.

Uniform Servers with Same Components: Having servers with identical components creates a homogenous setup that's susceptible to widespread failures. A flaw in one component could affect all servers simultaneously, leading to extended downtime.

Addressing these issues involves deploying end-to-end encryption, implementing database replication for failover, and diversifying server components to enhance reliability and resilience.