Added Elements:
a. 3 Firewalls:
Three firewalls are added to provide layers of security and control access to the servers, ensuring that only authorized traffic is allowed.
b. 1 SSL Certificate for HTTPS:
An SSL certificate is added to enable HTTPS encryption for www.foobar.com, securing the communication between clients and servers and protecting sensitive data.
c. 3 Monitoring Clients (Data Collectors):

Monitoring clients, such as data collectors for Sumo Logic or other monitoring services, are added to gather performance metrics, logs, and system health data for proactive monitoring and troubleshooting.

Specifics about the Infrastructure:

b. Purpose of Firewalls:
Firewalls are essential for enforcing security policies, filtering network traffic, preventing unauthorized access, and protecting servers and data from malicious attacks and intrusions.
c. Importance of HTTPS Traffic:
Serving traffic over HTTPS encrypts data exchanged between clients and servers, ensuring confidentiality, integrity, and authenticity of the communication, especially for sensitive information like login credentials and payment details.
d. Role of Monitoring:
Monitoring is crucial for real-time visibility into server performance, resource utilization, network activity, and application health. It helps identify issues, optimize performance, and ensure high availability and reliability.
e. Data Collection by Monitoring Tools:
Monitoring tools collect data by capturing system metrics, logs, events, and performance indicators from servers, applications, and network devices. They analyze this data to generate reports, alerts, and insights for administrators.
f. Monitoring Web Server QPS (Queries per Second):

To monitor web server QPS, you can configure monitoring tools to track incoming requests, measure response times, monitor server load, and analyze traffic patterns. Threshold alerts can be set to notify administrators of QPS spikes or anomalies.

Issues with the Infrastructure:
a. Terminating SSL at the Load Balancer Level:

Terminating SSL at the load balancer level can be an issue as it requires additional processing overhead on the load balancer and exposes decrypted traffic within the internal network, potentially increasing security risks.

b. Single MySQL Server Accepting Writes:

Having only one MySQL server capable of accepting writes creates a single point of failure for write operations, risking data loss or service disruptions if the server fails or experiences performance issues.

c. Identical Components on Servers:

Having servers with identical components (database, web server, and application server) can be problematic as it increases homogeneity and the risk of widespread failures or vulnerabilities affecting all servers simultaneously. Variability in components can improve fault tolerance and resilience.