**Definitions and Explanations**

Reason for Additional Components: Three new components have been introduced to enhance the system's security and performance. These include individual firewalls for each server to protect against attacks, an SSL certificate to enable HTTPS for server www.foobar.com, and three monitoring clients that gather logs for analysis in Sumo Logic.

Function of Firewalls: Firewalls serve as network security systems that monitor and regulate incoming and outgoing network traffic based on predefined security rules. Their purpose is to establish a protective barrier between a trusted network and an untrusted network.

Importance of HTTPS Traffic: Transitioning to HTTPS is essential because previous traffic was transmitted using Hypertext Transfer Protocol (HTTP), which exposed data in plain text. HTTPS ensures security by encrypting data through Transport Layer Security (TLS).

Role of Monitoring: Monitoring offers the capability to proactively identify and diagnose potential performance issues within web applications.

Data Collection by Monitoring Tool: The monitoring tool gathers logs from various components such as the application server, MySQL Database, and Nginx web server. A log, in this context, refers to automatically generated and timestamped records of system-relevant events.

Monitoring Web Server QPS: To monitor a web server's Query Per Second (QPS), especially when handling 1K queries per second, the process involves conducting assessments from both network and application perspectives.

**Issues**

A. Issue with SSL Termination at Load Balancer: Terminating SSL at the load balancer level can pose a concern due to the computational demands of decryption. This setup can offload processing from the application server but may introduce performance challenges. (Note: The original response acknowledges potential concerns without explicitly defining the issue.)

B. Issue with Single MySQL Write-Accepting Server: Relying solely on one MySQL server for write operations becomes problematic because if it goes down, data addition or updates are impossible. Consequently, certain application features might become inoperable.

C. Challenge with Uniform Server Components: Deploying servers with identical components (database, web server, and application server) introduces a risk. If a bug surfaces in one component of a server, the same bug could affect other servers, leading to widespread issues.