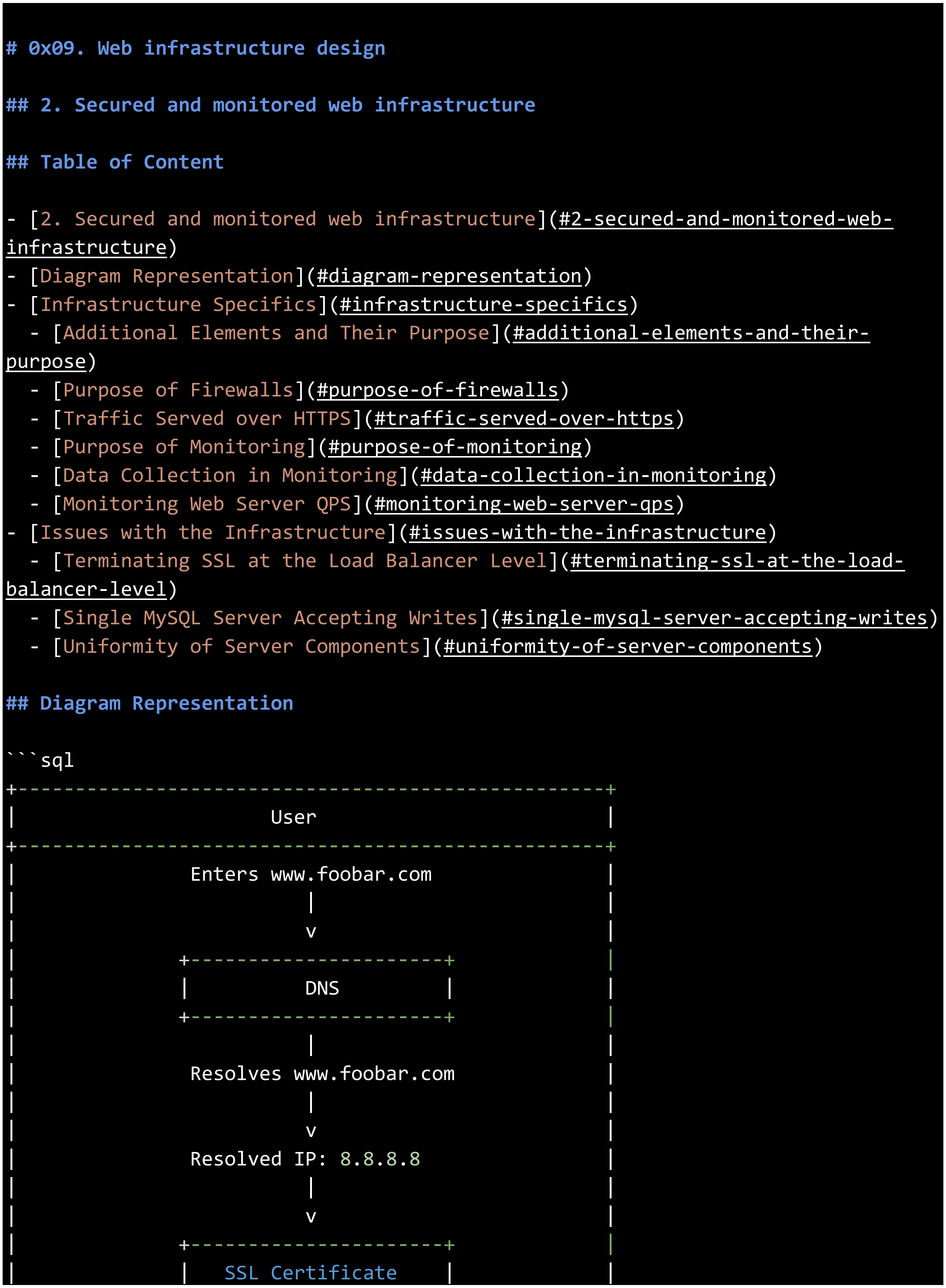
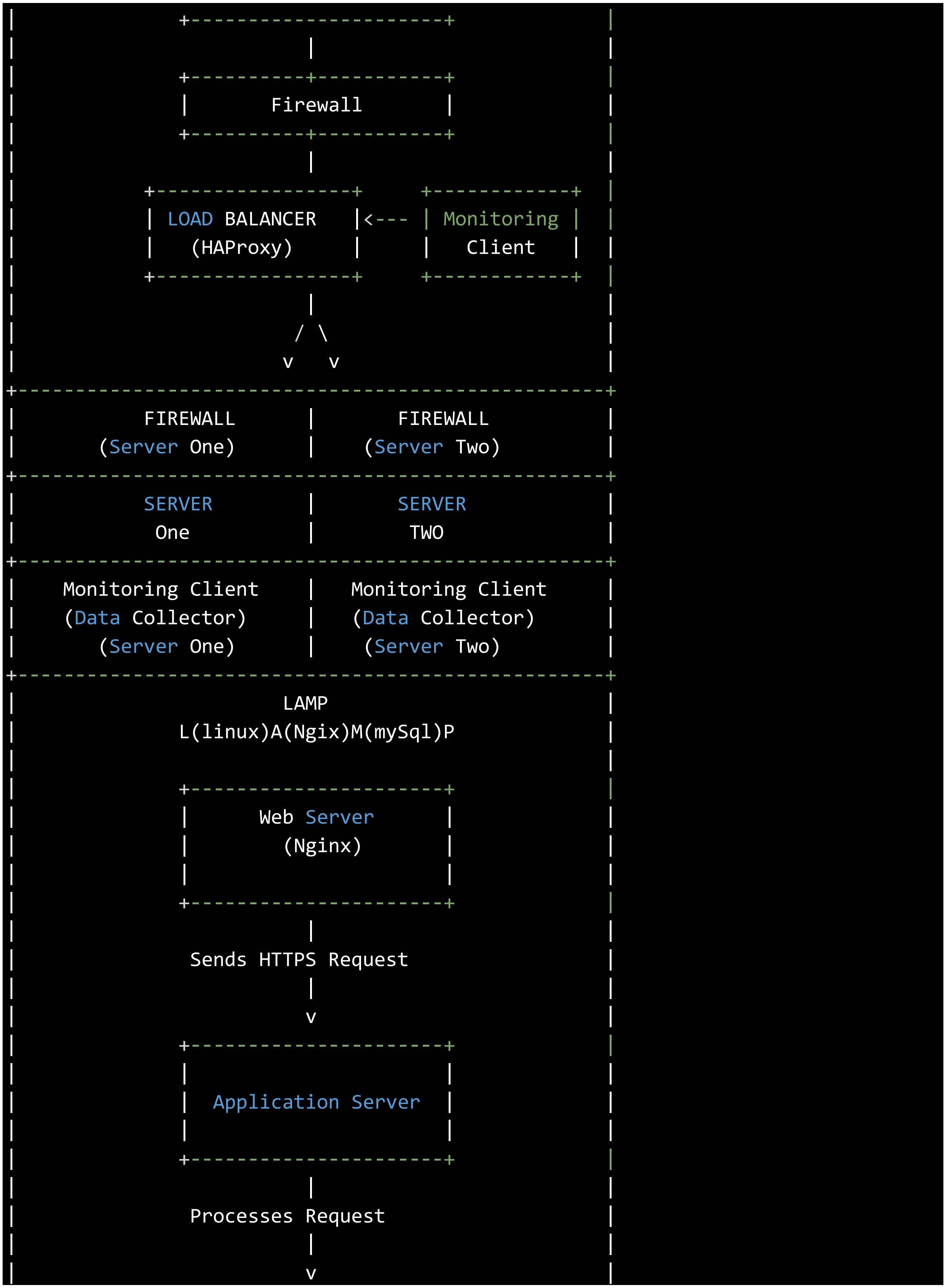
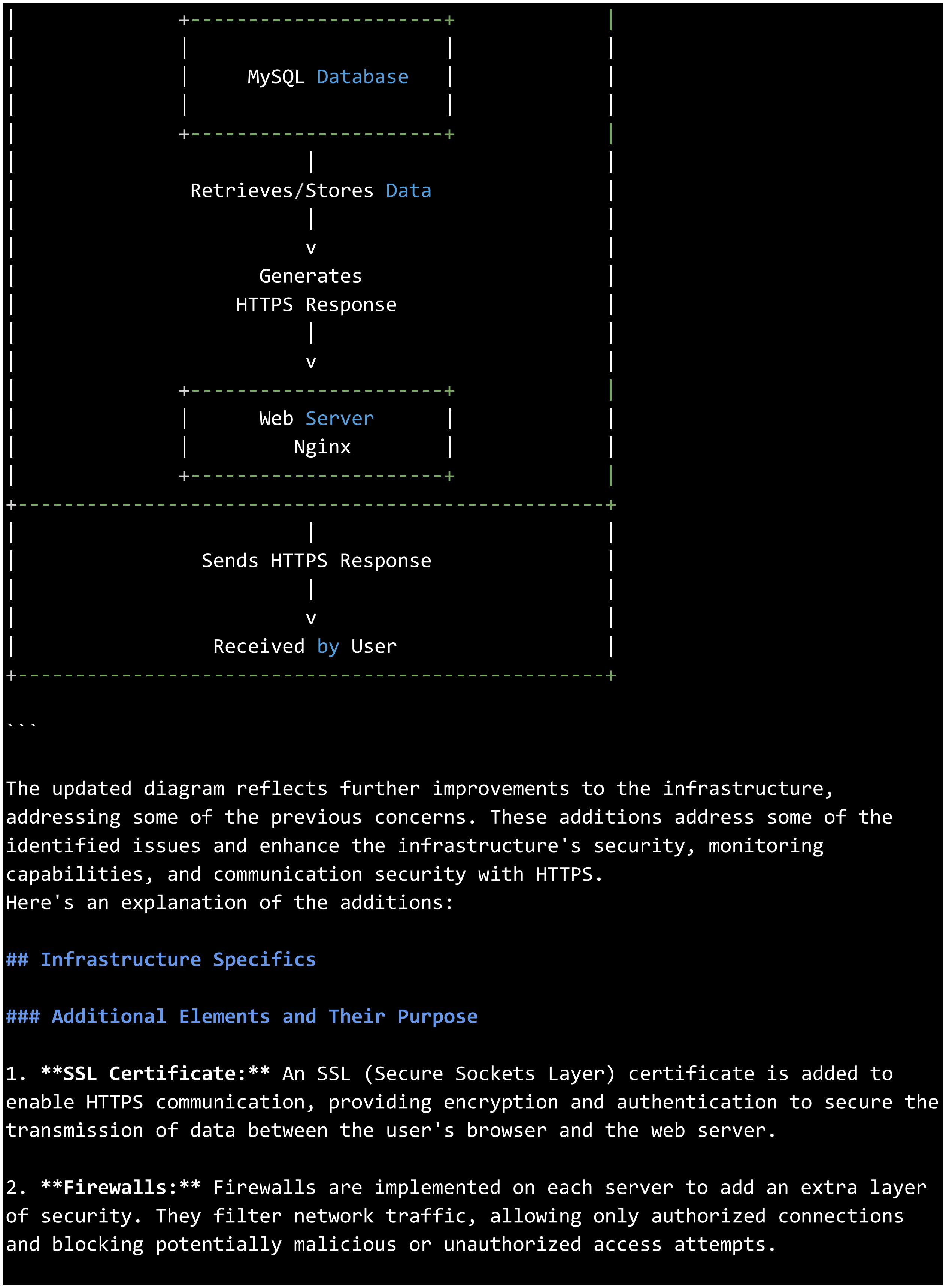


~~~
# 0x09. Web infrastructure design

## 2. Secured and monitored web infrastructure

## Table of Content

- [2. Secured and monitored web infrastructure](#2-secured-and-monitored-web-infrastructure)
- [Diagram Representation](#diagram-representation)
- [Infrastructure Specifics](#infrastructure-specifics)
  - [Additional Elements and Their Purpose](#additional-elements-and-their-purpose)
  - [Purpose of Firewalls](#purpose-of-firewalls)
  - [Traffic Served over HTTPS](#traffic-served-over-https)
  - [Purpose of Monitoring](#purpose-of-monitoring)
  - [Data Collection in Monitoring](#data-collection-in-monitoring)
  - [Monitoring Web Server QPS](#monitoring-web-server-qps)
- [Issues with the Infrastructure](#issues-with-the-infrastructure)
  - [Terminating SSL at the Load Balancer Level](#terminating-ssl-at-the-load-balancer-level)
  - [Single MySQL Server Accepting Writes](#single-mysql-server-accepting-writes)
  - [Uniformity of Server Components](#uniformity-of-server-components)

## Diagram Representation

```sql
+----------------------------------------------------+
|                      User                          |
+----------------------------------------------------+
|               Enters www.foobar.com                |
|                         |                          |
|                         v                          |
|              +-----------------------+             |
|              |          DNS          |             |
|              +-----------------------+             |
|                         |                          |
|               Resolves www.foobar.com              |
|                         |                          |
|                         v                          |
|               Resolved IP: 8.8.8.8                 |
|                         |                          |
|                         v                          |
|              +-----------------------+             |
|              |   SSL Certificate     |             |
~~~



```
|              +----------------------+             |
|                         |                         |
|              +----------+-----------+             |
|              |       Firewall       |             |
|              +----------+-----------+             |
|                         |                         |
|           +-----------------+     +------------+  |
|           | LOAD BALANCER   |<--- | Monitoring |  |
|           |   (HAProxy)     |     |   Client   |  |
|           +-----------------+     +------------+  |
|                         |                         |
|                        / \                        |
|                       v   v                       |
+---------------------------------------------------+
|           FIREWALL      |       FIREWALL          |
|       (Server One)      |    (Server Two)         |
+---------------------------------------------------+
|           SERVER        |       SERVER            |
|            One          |        TWO              |
+---------------------------------------------------+
|    Monitoring Client    |   Monitoring Client     |
|    (Data Collector)     |   (Data Collector)      |
|       (Server One)      |    (Server Two)         |
+---------------------------------------------------+
|                       LAMP                        |
|              L(linux)A(Ngix)M(mySql)P             |
|                                                   |
|              +----------------------+             |
|              |      Web Server      |             |
|              |        (Nginx)       |             |
|              |                      |             |
|              +----------------------+             |
|                         |                         |
|               Sends HTTPS Request                 |
|                         |                         |
|                         v                         |
|              +----------------------+             |
|              |                      |             |
|              |  Application Server  |             |
|              |                      |             |
|              +----------------------+             |
|                         |                         |
|               Processes Request                   |
|                         |                         |
|                         v                         |
```



~~~
|              +----------------------+             |
|              |                      |             |
|              |     MySQL Database   |             |
|              |                      |             |
|              +----------------------+             |
|                          |                        |
|               Retrieves/Stores Data               |
|                          |                        |
|                          v                        |
|                      Generates                    |
|                    HTTPS Response                 |
|                          |                        |
|                          v                        |
|              +----------------------+             |
|              |      Web Server      |             |
|              |         Nginx        |             |
|              +----------------------+             |
+---------------------------------------------------+
|                          |                        |
|                Sends HTTPS Response               |
|                          |                        |
|                          v                        |
|                 Received by User                  |
+---------------------------------------------------+

```

The updated diagram reflects further improvements to the infrastructure,
addressing some of the previous concerns. These additions address some of the
identified issues and enhance the infrastructure's security, monitoring
capabilities, and communication security with HTTPS.
Here's an explanation of the additions:

## Infrastructure Specifics

### Additional Elements and Their Purpose

1. **SSL Certificate:** An SSL (Secure Sockets Layer) certificate is added to
enable HTTPS communication, providing encryption and authentication to secure the
transmission of data between the user's browser and the web server.

2. **Firewalls:** Firewalls are implemented on each server to add an extra layer
of security. They filter network traffic, allowing only authorized connections
and blocking potentially malicious or unauthorized access attempts.
~~~

```
3. **Monitoring Clients:** Monitoring clients ("Monitoring Client (Server One)"
and "Monitoring Client (Server Two)") are introduced to collect data about the
infrastructure's performance, health, and metrics, which can be utilized by the
monitoring system. These clients communicate with the monitoring system to
provide real-time insights and enable proactive monitoring, alerting, and
troubleshooting.

4. **Monitoring System:** A monitoring system ("Monitoring Client") is introduced
to collect and analyze data from the monitoring clients. It helps monitor the
infrastructure's health, performance, and availability, providing visibility into
system metrics and enabling timely detection and resolution of issues.

### Purpose of Firewalls

Firewalls are used to protect the servers and network by monitoring and
controlling incoming and outgoing network traffic. They act as a barrier between
the internal network and external sources, preventing unauthorized access,
filtering malicious traffic, and enforcing security policies.

### Traffic Served over HTTPS

Traffic is served over HTTPS to ensure secure communication between the user's
browser and the web server. HTTPS encrypts the data exchanged, preventing
eavesdropping, data tampering, and unauthorized access to sensitive information,
such as passwords, personal data, and financial details.

### Purpose of Monitoring

Monitoring is used to track and analyze various aspects of the infrastructure's
performance, health, and availability. It helps detect and resolve issues
proactively, optimize resource utilization, identify trends, and ensure optimal
user experience. Monitoring also aids in capacity planning, troubleshooting, and
maintaining service level agreements.

### Data Collection in Monitoring

The monitoring tool collects data from the monitoring clients by utilizing
various mechanisms, such as agent-based monitoring or remote monitoring
protocols. Agents installed on the monitored servers gather information about
system metrics, resource utilization, application performance, and network
traffic. The collected data is then transmitted to the monitoring system for
storage, analysis, and visualization.

### Monitoring Web Server QPS
```

```
To monitor the web server's QPS (Queries Per Second), you can utilize the
monitoring tool's capabilities. Configure the monitoring tool to track the web
server's incoming request rate and measure the number of queries served per
second. The monitoring system will collect and display this information, allowing
you to monitor the QPS trends, set thresholds for alerts, and identify any
performance bottlenecks or deviations from expected behavior.

## Issues with the Infrastructure

### Terminating SSL at the Load Balancer Level

Terminating SSL at the load balancer level can be an issue if the communication
between the load balancer and the backend servers is not adequately secured. If
the traffic is transmitted in plain HTTP between the load balancer and the
backend servers, it poses a security risk, as the data can be intercepted or
manipulated. It is recommended to ensure secure communication (HTTPS) between the
load balancer and the backend servers to maintain end-to-end encryption.

### Single MySQL Server Accepting Writes

Having only one MySQL server capable of accepting writes introduces a single
point of failure. If the primary MySQL server fails, it can result in data
unavailability and impact the application's functionality. Implementing a
replication setup with multiple MySQL servers, where changes are synchronized
between them, can provide redundancy and high availability.

### Uniformity of Server Components

Having servers with all the same components (database, web server, and
application server) can lead to a lack of diversity and increased risk. If a
vulnerability or issue affects one component, it may affect all servers
simultaneously. Introducing variations in the technology stack or employing
different types of servers can help mitigate the risk of widespread failures and
provide flexibility for specific workload requirements.
```