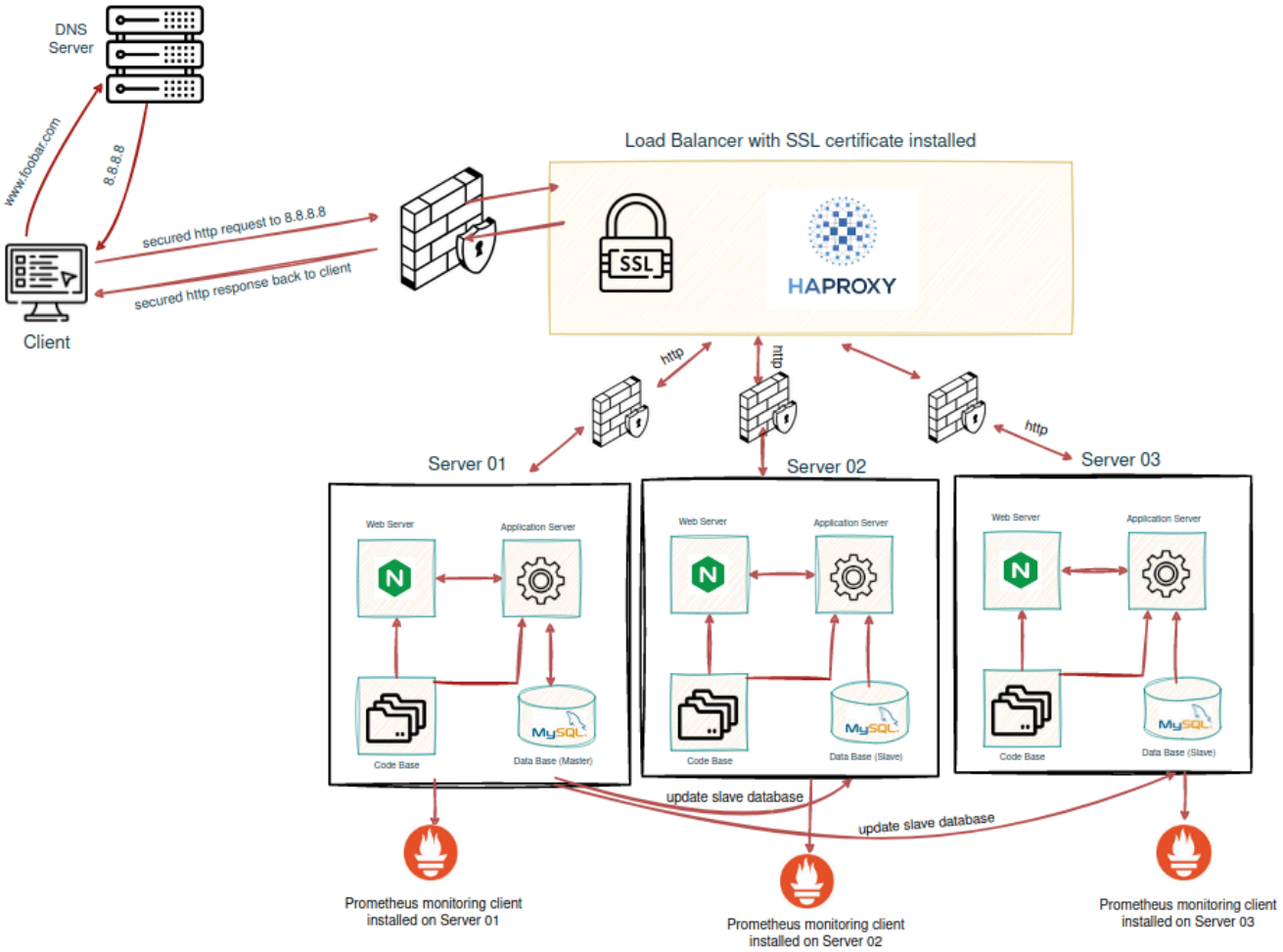

Fig 1: Three-Server Web Infrastructure for www.foobar.com with firewall and ssl

- For every additional element, why are you adding it?

Firewalls: Firewalls act as security gateways, filtering incoming traffic before it reaches the servers. They help prevent:

➔ Unauthorized Access**:** By blocking access attempts from unauthorized sources or protocols.

➔ Denial-of-Service Attacks**:** By filtering out excessive traffic volumes that could overwhelm the servers.

SSL Certificate: An SSL certificate enables HTTPS, which encrypts communication between the user's browser and the web server. This protects sensitive data.

Monitoring Clients: Monitoring clients collect data on server performance, application health, and resource utilization. This allows for:

➔ Proactive Problem Detection**:** Identifying potential issues like server overload, performance bottlenecks, or application errors before they impact user experience.

➔ Faster Troubleshooting**:** Monitoring data helps pinpoint the root cause of problems, facilitating quicker resolution.

- What are firewalls for? Firewalls play a critical role in safeguarding the servers from unauthorized access and malicious traffic.

- Why is the traffic served over HTTPS?

Security: HTTPS encrypts communication between the user's browser and the web server (Nginx). This means data transmitted in both directions (from browser to server and vice versa) is scrambled using a secure algorithm. This encryption safeguards sensitive information.

- What monitoring is used for? Monitoring is used to ensure the health, performance, and availability of systems and applications.

- How the monitoring tool is collecting data?

Monitoring tools collect data through various methods such as **agent-based** and **agentless** monitoring. Agent-based monitoring involves installing a small software component (agent) on the target system, which collects and sends data to the monitoring server. This agent can gather information about system metrics (CPU, memory, disk usage), application performance, and custom metrics.

Agentless monitoring, on the other hand, relies on protocols like SNMP, WMI, or HTTP to remotely gather data from systems and applications. Additionally, some monitoring tools use **synthetic** monitoring, where simulated transactions are performed to measure application performance and availability.

Data collected by monitoring tools is typically stored and analyzed to generate reports, alerts, and visualizations for administrators to understand the health and performance of their systems.

- Explain what to do if you want to monitor your web server QPS?

Queries-per-second (QPS) is a metric for measuring how fast a computer system can handle incoming requests. It helps assess and improve the performance of websites, databases, and network devices.

To monitor the web server's QPS, we first install a monitoring agent on the server. Then, we'll configure the agent to collect QPS metrics. Finally, we'll use a monitoring tool to visualize the QPS data and set up alerts for abnormal QPS levels.

Issues with the above setup:

SSL termination at load balancer: can be an issue because it adds an extra layer of processing for the load balancer, potentially increasing its workload and introducing a single point of failure for SSL termination.
Single MySQL server for writes: it creates a single point of failure for write operations. If this server fails, write operations will be disrupted, impacting the availability and consistency of the database.
All-in-one servers: it lacks separation of concerns, making it harder to scale and maintain different parts of the infrastructure independently.