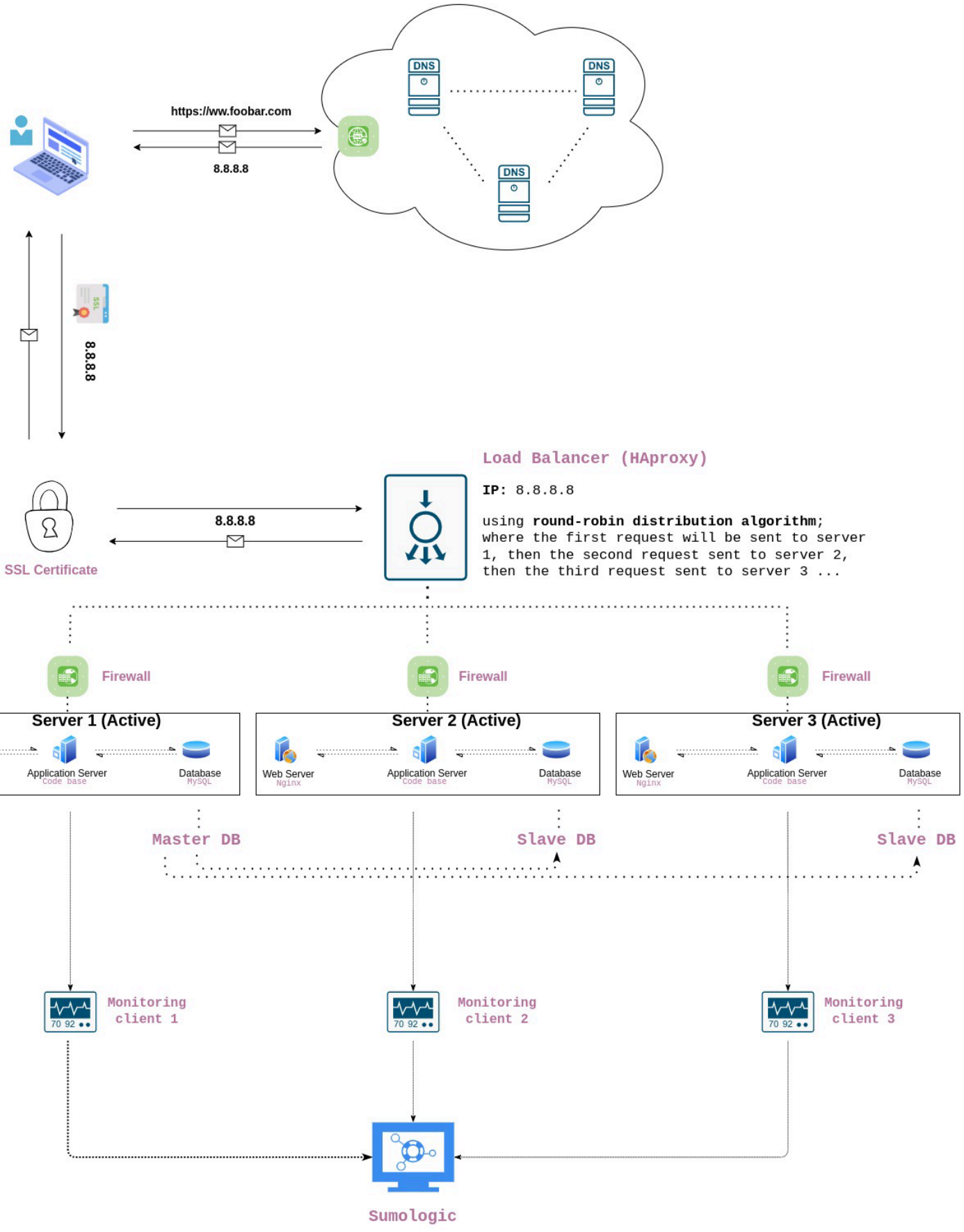
ALX - 0x09. Web Infrastructure Design

Task 2: Secured and Monitored Web Infrastructure

1. **For every additional element, why are adding it**; we have added three new components; a firewall for each server to protect them from being attacked and exploited, 1 SSL certificate to server www.foobar.comover HTTPS, and three monitoring clients that will collect logs and send them to our data collector Sumologic.
2. **What are firewalls for**; is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It establishes a barrier between a trusted network and an untrusted network.
3. **Why is the traffic served over HTTPS**; previously, the traffic was passed over Hypertext Transfer Protocol (**HTTP**) which transfers data in plain text, while **HTTPS** is secure where the data is encrypted using Transfer Layer Security (**TLS**).
4. **What monitoring is used for**; it can detect and diagnose any web application performance issues proactively.
5. **How the monitoring tool collects data**; it collects logs of the application server, MySQL Database, and Nginx web server. A log in a computing context is the automatically produced and time-stamped documentation of events relevant to a particular system.
6. **Explain what to do if you want to monitor your web server QPS**; one web server handles 1K queries per second (**QPS**), I would basically monitor it from the network and application level.

Issues:

A. **Why terminating SSL at the load balancer level is an issue**; it is an issue because decryption is resource and CPU-intensive. Placing the decryption burden on the load balancer enables the server to spend processing power on application tasks but to be honest, I don't know to see the issue to be honest (I will update this).
B. **Why having only one MySQL server capable of accepting writes is an issue**; because once it is down it means no data can be added or updated, meaning some features of the application won't work.
C. **Why having servers with all the same components (database, web server, and application server) might be a problem** because once you have a bug in one of the components in one of the servers, the bug will be valid in the other servers.


DNS
DNS
DNS
https://ww.foobar.com
8.8.8.8
SSL
8.8.8.8
Load Balancer (HAproxy)
IP: 8.8.8.8
using round-robin distribution algorithm;
where the first request will be sent to server
1, then the second request sent to server 2,
then the third request sent to server 3 ...
8.8.8.8
SSL Certificate
Firewall
Firewall
Firewall
Server 1 (Active)
Server 2 (Active)
Server 3 (Active)
Web Server
Nginx
Application Server
Code base
Database
MySQL
Master DB
Slave DB
Slave DB
Monitoring
client 1
Monitoring
client 2
Monitoring
client 3
Sumologic