Compound & Termes Explanations:

Firewalls: Firewalls are added to control and filter network traffic, allowing only authorized and safe data to pass through. They serve as a barrier against unauthorized access and potential attacks, ensuring network security.

Traffic Served over

HTTPS: HTTPS encrypts data transmitted between clients and servers, ensuring confidentiality and integrity. It prevents sensitive information from being intercepted or tampered with during transmission.

Monitoring: Monitoring tools are used to track system performance, detect anomalies, and address security threats proactively. They provide insights into the infrastructure's health, performance, and potential vulnerabilities.

Monitoring Data Collection:

Monitoring tools collect data by:

Gathering Logs: Collecting logs from servers, applications, and network devices.

Analyzing Metrics: Capturing performance metrics like CPU usage, memory, network traffic, etc.

Parsing Events: Tracking system events and errors for anomaly detection and security monitoring.

Monitoring Web Server QPS:

To monitor Web Server QPS (Queries Per Second):

Utilize monitoring tools to track and analyze the number of queries hitting the web server per second.

Set up specific alerts for unusual spikes or drops in query traffic to promptly investigate potential issues.

Issues with the Infrastructure:

Terminating SSL at the load balancer: exposes decrypted data within the internal network. If breached, it could compromise sensitive information, as encrypted data is converted to plaintext before reaching the servers.

Single MySQL Server Accepting Writes: Having only one MySQL server capable of accepting writes creates a single point of failure. If this server fails, it can disrupt write operations and compromise data availability.

Homogeneous Server Components (Database, Web Server, and Application Server): Uniform server components might lead to a lack of diversity in the infrastructure. A vulnerability affecting one component could potentially impact all servers, increasing the risk of widespread failure due to a shared weakness.