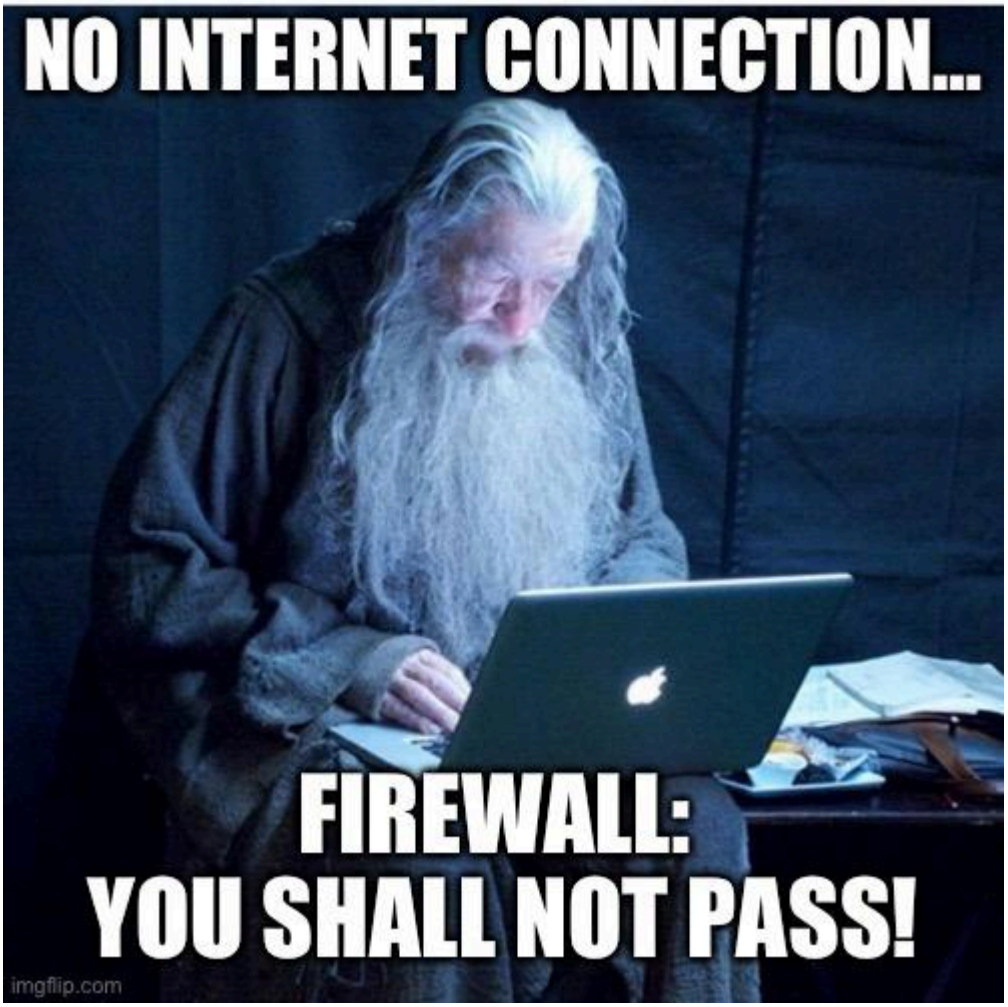
Issue Summary:

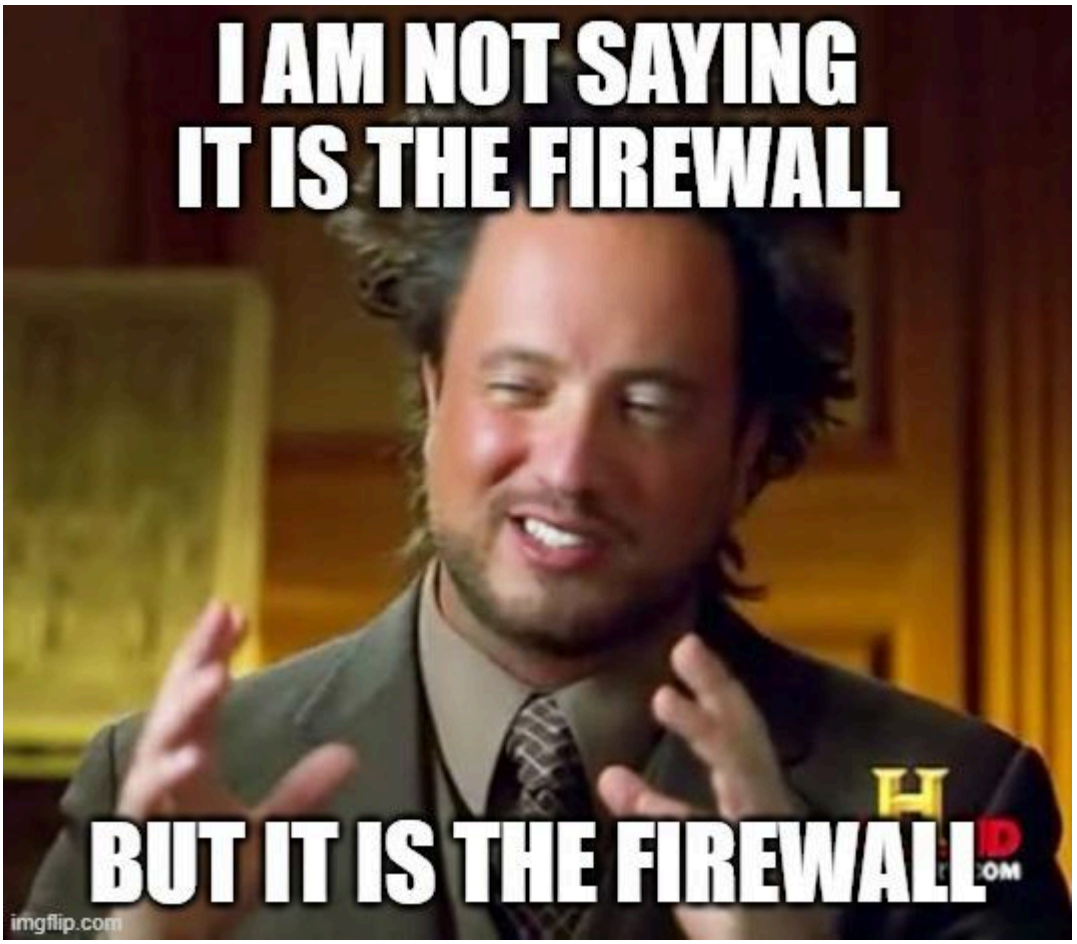
- **Duration:** The outage occurred from February 16, 2024, at 10:00 AM to February 16, 2024, at 11:30 AM (UTC).
- **Impact:** During the outage, all incoming traffic on port 443 was blocked, affecting the availability of the web service. Approximately 30% of users experienced connectivity issues or were unable to access the service.
- **Root Cause:** The root cause of the issue was the misconfiguration of the firewall settings, specifically the Uncomplicated Firewall (UFW), where an intern mistakenly executed a command that blocked incoming traffic on port 443.
- 

Timeline:

- **10:00 AM (UTC):** The issue was detected when users began reporting connectivity problems and error messages related to the web service.
- **10:05 AM:** Engineers noticed a spike in error logs and a decrease in incoming traffic metrics, indicating a potential issue with the server.
- **10:10 AM:** Initial investigation focused on server logs and network configurations to identify any anomalies.
- **10:20 AM:** Assumptions were made that the issue might be related to a recent software update or a network issue.

- **10:30 AM:** As the investigation progressed, it was discovered that the firewall settings were blocking incoming traffic on port 443.
- **10:45 AM:** The incident was escalated to the DevOps team for further assistance in resolving the firewall configuration issue.
- **11:00 AM:** Engineers reconfigured the firewall settings to allow incoming traffic on port 443, restoring connectivity to the web service.
- **11:30 AM:** The issue was fully resolved, and normal service operations resumed.

Root Cause and Resolution:

- **Root Cause:** The root cause of the issue was the execution of a command in the UFW by an intern, which inadvertently blocked incoming traffic on port 443.
- **Resolution:** To fix the issue, engineers reconfigured the firewall settings to allow incoming traffic on port 443, restoring normal service operations.
- 

Corrective and Preventative Measures:

- **Improvements/Fixes:**
    1. Implement stricter access controls and permission management for critical server configurations to prevent unauthorised changes.
    2. Enhance training and onboarding procedures for new team members to emphasise the importance of double-checking commands before execution.
    3. Implement automated configuration validation checks to detect and alert on any unauthorised changes to firewall settings or other critical configurations.

- **Tasks to Address the Issue:**
    1. Review and update documentation regarding firewall configuration and best practices.
    2. Conduct a comprehensive audit of all server configurations to ensure consistency and accuracy.
    3. Implement regular security training sessions for all team members to raise awareness of potential risks and best practices for system management.

In conclusion, the outage was caused by a misconfiguration of the firewall settings, which resulted in the blocking of incoming traffic on port 443. Through prompt detection and effective collaboration, the issue was resolved, and corrective measures were implemented to prevent similar incidents in the future.