Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is an overwhelming volume of incoming traffic causing the server to be under excessive stress The logs show that: from log item number 125 due to the large requests made from 1 IP address, the server cannot process the requests and subsequently times out connection attempts from legitimate employees included. This event could be a SYN Flood attack, a type of DoS attack.

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake: 1. A website visitor sends a request to the server for permission to access the website (SYN) 2. The server acknowledges the request coming from the website visitor and sends the acknowledgement to access the website (SYN, ACK) 3. The website visitor then acknowledges the acknowledgement from the server and proceeds into the website (ACK) The large number of SYN packets flood the first step of the TCP handshake and continuously send requests till all the server ports are unavailable. This causes the server to become unable to function. The logs indicate that initially the server was able to acknowledge and complete some requests on port 443, but some website visitors were still receiving timeout errors and prompted to refresh as seen in log 77, 80 & 121 (RST, ACK). Requests were taking about 7 seconds to be completed. By the 20 second mark, the server was unable to acknowledge requests on port 443 and this carried on for another 9 seconds. This inability caused the server to be unable to function and would need to be temporarily brought down to help return it to a normal operating state.

The company may have faced a lot of negative reputation backlash as both employees and website visitors were unable to access the website and could therefore not move forward in the sales process, ultimately impacting our profit margins.

To help secure the system against future attacks we should configure the firewall to automatically block a large number of requests from the same IP address and setup SYN attack thresholds on the firewall. We can also install an intrusion prevention system (IPS) to detect anomalous traffic patterns.