Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
After reviewing the data provided from the packet sniffer I utilized, there are two potential explanations for the timeout error message. Those being: An HTTP/1.1 504 Gateway Time-Out error message, and an [RST, ACK] packet. In the case of the former, the web server is taking too long to respond. In the case of the latter, the packet is sent to the requesting visitor since the [SYN, ACK] packet is not received by the web server. However, further analysis of the logs indicate that this is undoubtedly a SYN flood 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. The first step is the [SYN] packet is an initial request from a visitor trying to connect to a web page hosted on the web server. The second step is the {SYN, ACK] packet is the web server's response to the visitor's request agreeing to the connection. The final step is the {ACK} packet is the visitor's machine acknowledging the permission to connect. When a malicious actor sends a large number of [SYN] packets all at once they are performing a denial of service attack, which is furthermore classified as an IP spoofing attack. By overloading the server, they are disrupting the service which can lead to a variety of consequences for the company. One IP address in particular is injecting multiple SYN packets after an initial and normal request with the server. The web server has stopped responding to legitimate employee visitor traffic, and from log item number 125 onwards the web server stops responding. Only logging attempts to inject more [SYN] packets from this single particular IP address.