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 due to a malicious actor using a SYN flooding attack on the server. The logs show that an unfamiliar IP address is sending an abnormal amount of SYN requests which eventually resulted to a failed connection from a legitimate employee and the gateway server sent a timeout error message to the requesting browser. In this case, it is safe to assume that it is an on-going DoS attack or more specifically, a SYN flooding 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 in the handshake is when a SYN (synchronize) packet is requested and sent from a client (source) to a server (destination). The next step is when the server agrees to the request to connect and responds by setting up a SYN-ACK (synchronize-acknowledge) packet to prepare for the final step. The last step in the handshake is when the designated server sends back an ACK packet to “acknowledge” the connection and thus the connection is established and the handshake is completed. When a malicious actor sends a large number of SYN packets all at once, it floods the server with requests to initiate a handshake and the server can only hold a limited amount of resources that can handle these requests. The server would then be overwhelmed and unable to take in requests if the threshold of resources has been reached. The logs indicate that an unfamiliar IP address sent multiple rapid requests for SYN packets that overwhelms the server resulting in the timeout error message for a legitimate employee connecting to the website.