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 the gateway server was waiting for a response from the web server. If the web server takes too long to respond, the gateway server will send a timeout error message to the requesting browser. The logs show that there was an abnormal amount of SYN requests coming from a single IP address causing the web server to struggle and eventually fail.This event could be evidence of a 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.The SYN packet is sent from someone trying to connect to a web page hosted on a web server. 2. The SYN, ACK packet is how the web server responds to the person's request agreeing to the connection. 3.The ACK packet is the person's machine acknowledging the permission to connect. When a threat actor attempts to flood a web server with SYN packet requests it causes stress on the web server. If the web server does not have enough resources to handle all of the incoming requests, then the server will become overwhelmed and unable to respond to all the requests. The logs indicate that an abnormal amount of SYN packet requests came from a single IP address and in turn causing the web server to try and respond to all these requests and causing the web server to go down. It is safe to assume that this was a malicious attack known as a DOS attack on the web server.