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 a SYN attack. The logs show that there are rapid SYN requests being sent to the server from one IP. This event could be a DoS SYN flood attack. A SYN attack is one that simulates TCP connection. Malicious actors take advantage of the fact that it is part of a three-way handshake, to send numerous SYN packets at a go knowing that for each SYN packet sent to a server, the server reserves system resources for the response of the connection. Since the malicious actor does not fulfill the final step of the handshake, the excessive reservation of the system resources by the server causes it to eventually be unable to function properly.

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 visitor sends a [SYN] packet requesting to connect to the web server.It's like saying,"Hey I'd like to communicate with you." 2. The web server then responds with a [SYN/ACK] packet agreeing to the connection. It then sets aside resources for the final step of the handshake. 3. The visitor's machine sends a [ACK] packet to acknowledge the permission to connect. After this step a TCP connection is established. When a malicious actor sends a large number of SYN packets all at once, a lot of system resources of the web server are reserved for each of the many SYN packets. This reduces the number of system resources used by legitimate visitors to the site until eventually visitors can no longer access the site. The logs indicate that numerous SYN packets were sent from a single IP address, together with known IP addresses of visitors. There were two errors: 1. Gateway timeout - which is sent by the gateway server to the requesting browser to indicate that the web server took too long to respond. 2. A [RST/ACK] packet - which would be sent to the requesting visitor if the [SYN/ACK] packet is not received by the web server