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 malicious actor performing a SYN flood attack on the web server. The logs show that numerous SYN requests are coming from an unfamiliar IP address. A SYN flood attack is when a threat actor uses the SYN request flag of the TCP handshake an abnormal amount of times to potentially slow down and even crash a server

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 first step of the TCP handshake is the SYN request. This is a request by the source address to the destination address to open a channel of communication.

2. The second step is the SYN-ACK flag. A SYN-ACK flag comes from the destination address recognizing that the source address would like to open a channel of communication.

3. The final step of the handshake is the ACK flag. This flag signifies the acknowledgement of the original address that a channel for communication has been opened for traffic.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets too quickly the receiving server might have trouble setting aside appropriate system resources for each request coming in all at once. This along with regular valid traffic would at the very least bottleneck resources on the server and can even cause a complete server crash.
The logs indicate an abnormal amount of SYN request packets being sent from the same malicious IP to the web server and, because of the amount and rapidity of the requests, the web server simply cannot handle the malicious traffic and regular traffic simultaneously.

To prevent attacks similar to this from happening in the future the company could introduce a stateful firewall with explicit rules to block potentially malicious traffic.