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 Flood attack. The logs show an abnormally large number of TCP SYN requests from an unfamiliar IP address. This event overwhelms the web server, preventing it from responding to legitimate traffic. The server was temporarily taken offline to recover, and the malicious IP was blocked via the firewall. Further measures are needed to prevent recurrence.

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. 1. The client sends a SYN packet to the server to initiate the connection. 2. The server responds with a SYN-ACK packet to acknowledge the request. 3. The client sends an ACK packet back to the server to confirm the connection is established. When a malicious actor sends a large number of SYN packets all at once, it can overwhelm the server, preventing it from processing legitimate requests. The logs indicate a flood of SYN requests from an unfamiliar IP address, leading to the server being unable to respond to legitimate traffic, causing connection timeouts for users.