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 DoS attack **The logs show that:** Many repeated SYN requests by the same source **This event could be:** A SYN flood 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.A device sends a SYN request to server. 2. The server then responds with SYN/ACK packet acknowledgement and opens the port for a final step to the handshake. 3. Once final ACK packet has been received then a TCP connection is established. **Explain what happens when a malicious actor sends a large number of SYN packets all at once:** The server would become overwhelmed and crashed. **Explain what the logs indicate and how that affects the server:** The logs indicate that source IP, 203.0.113.0, is sending masses of SYN requests through port 54770 to the destination IP, 192.0.2.1. Ultimately, regular customers are unable to access the destination IP.