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 that the server is experiencing a DoS attack. The logs indicate that the server was flooded with SYN messages from a host with the IP address 203.0.113.0, causing it to run out of resources and stop responding to other requests. This incident appears to be a type of DoS attack known as SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction
When website visitors attempt to establish a connection with the web server, the TCP protocol initiates a three-way handshake. The three steps of this handshake are as follows: 1. The client (host) sends a SYN packet to the server, requesting a connection. 2. The server responds with a SYN-ACK packet, acknowledging the request and waiting for confirmation from the client. 3. The client then sends an ACK packet, completing the handshake and establishing the connection. In the case of a SYN flood attack, a malicious actor sends numerous SYN packets without responding to the server's SYN-ACK packets. As a result, the server's resources are consumed, rendering it unable to handle legitimate TCP connections. The logs indicate that the server has become overwhelmed and is unable to process visitors' TCP connections because it is stuck waiting for the completion of the handshake. This is why visitors receive a timeout message. To mitigate a SYN flood attack, I recommend configuring firewall rules to limit the number of SYN requests that can be sent by the same host. Implementing an Intrusion Prevention System (IPS) would also be an effective solution.