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 DoS attack. The logs show that a huge number of SYN requests which are used to establish connection with the server are coming from the 203.0.113.0 ip address and the server is unable to handle these huge requests. This is an SYN flood attack coming from 203.0.113.0

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. The handshake consists of three steps: A SYN packet is sent from source to destination to establish connection. Then the SYN/ACK packet is sent from destination to source as an acknowledgement to the connection request. And at last the source sends an ACK packet to the destination and then starts requesting information. When a malicious actor sends huge SYN requests to flood the server so that it won't be able to handle huge traffic and stops working. This is a type SYN flood attack on the server. The logs indicate that 203.0.113.0 is attacking the servers with SYN flood attack causing a connection timeout message. So our next step of action should be to block 203.0.113.0 and investigate for the root cause.