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: The server has stopped responding to requests to connect because it is out of available resources. The logs show that: A single external IP address is sending multiple requests to connect to the server every second and is not completing the connection handshake. This event could be: A SYN flood attack resulting in Denial of Service.

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 client sends a request to the server to connect (SYN request) 2. The server replies with an acknowledgement (ACK) accepting the request to connect. 3. The client responds to the ACK with its own ACK establishing the connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: Each time the server acknowledges the request to connect it allocates resources in anticipation of establishing the connection and providing service. When too many requests are sent at once this can quickly overwhelm the server by consuming too many resources resulting in the server not responding to any more requests. Explain what the logs indicate and how that affects the server: The logs indicate one external unrecognized IP (203.0.113.0) sending several requests a second and not acknowledging to establish a connection. As the requests grew in number legitimate users started experiencing timeouts when loading the website. The attack began and only took about 3 seconds to start having a noticeable effect on operations and after about 17 seconds the server became completely overwhelmed and stopped responding to any new requests at all. Possible mitigation strategies could include:

1. Not allocating memory until an actual ACK (acknowledgment) response is received from the client
2. Shorten timeout on responses
3. Rate limiting SYN packets
4. New Firewall rules
5. Cloud DDos protection