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 become overloaded with requests, which has caused the server to lose the ability to respond to legitimate requests and throw a timeout error. The logs show that multiple SYN requests from the same IP address are being sent every second, causing the server to become overwhelmed. This event could be a type of Denial of Service (DoS) called SYN flooding from a malicious actor due to the requests coming from a single IP address.

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. This happens in three steps:

1. A SYN request is sent from a device to the server to begin to establish a connection.
2. The server then responds to this request with a SYN/ACK packet to acknowledge the receipt of the device's request. The destination will reserve resources for the source to connect.
3. A TCP connection is then established once the server receives the final ACK packet from the source.

When a malicious actor sends a large number of SYN packets at once to a server, the server becomes overwhelmed and can no longer reserve resources for the connection. The result of this is that no legitimate connections can access the server.

The logs indicate that multiple SYN packets are being sent to the server every second from the same source IP address, eventually causing the server to crash. This results in users seeing a Gateway time-out error when attempting to access the server.

Possible defenses against similar future attacks would be to configure the firewall to block multiple incoming requests from the same IP address before the server becomes overwhelmed.