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 Distributed Denial of Service (DDoS) attack. The logs show a significant influx of TCP SYN requests originating from an unfamiliar IP address, overwhelming the web server. This event could be indicative of a coordinated attack aimed at disrupting the normal functioning of the website by flooding it with malicious traffic.

Section 2: Explain how the attack is causing the website to malfunction
When website visitors attempt to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. 1. SYN (Synchronize): The client initiates the connection by sending a SYN packet to the server, indicating its intention to establish communication. 2. SYN-ACK (Synchronize-Acknowledgment): Upon receiving the SYN packet, the server responds with a SYN-ACK packet, acknowledging the client's request and indicating readiness to establish a connection. 3. ACK (Acknowledgment): Finally, the client sends an ACK packet to confirm receipt of the server's acknowledgment, completing the three-way handshake and establishing the connection. However, when a malicious actor sends a large number of SYN packets simultaneously, without completing the handshake process, it results in a SYN flood attack. These incomplete connection requests consume server resources, causing it to become overwhelmed and unable to respond to legitimate connection requests. In the case described, the logs indicate a barrage of SYN requests from an unfamiliar IP address, indicating a SYN flood attack. This attack disrupts the normal functioning of the web server, leading to connection timeouts for legitimate users attempting to access the website. In response to the attack, the server was temporarily taken offline to allow it to recover and return to normal operation. Additionally, the company's firewall was configured to block the IP address responsible for the abnormal SYN requests. However, it's noted that this blocking solution may not be a permanent fix, as attackers can easily spoof other IP addresses to circumvent the block. It is imperative to alert management about the severity of the attack and discuss further steps to mitigate future attacks, possibly by implementing more robust DDoS protection measures such as rate limiting or traffic filtering.