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 because the system does not have the bandwidth to handle all the requests, including the request from the legitimate employee. Because the gateway server did not receive a response from the web server for an extended period of time, the gateway server returned a timeout error to the requesting browser. The logs show that the server initially could handle both legitimate and non-legitimate requests, but within a few seconds, the server increasingly received more SYN packets from someone other than the employee. This event could be a SYN flood initiated by a malicious actor.

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: 1. The requesting web browser sends a [SYN] (synchronized) packet to the web server asking to connect. 2. The web server receives the [SYN] packet and returns a [SYN, ACK] (SYN, acknowledge) packet agreeing to the connection and allocates system resources to prepare for response from the web browser. 3. The requesting web browser sends an [ACK] packet acknowledging the connection, and the TCP connection is secured. When a malicious actor sends a large number of SYN packets all at once to a server (i.e., SYN flood, a DoS attack), this overwhelms the server resources, leading to disruption in normal operations as the server cannot process legitimate requests. It is advised that the firewall should be configured to filter out this (and other malicious/unknown IP addresses). This is shown in the logs in the info column: we see that the client (port 42584) successfully connects to the server, and around four seconds later the server begins to receive an abnormal amount of SYN packets from port 54770, blocking the requests made by the client.