# 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 website is taking too long to respond to a request sent or TCP handshake not completing. The logs show that an unfamiliar IP address is sending too many SYN requests to the server. This event could be: a SYN flood attack |

| 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:<br>1. A synchronize(SYN) request is sent to the server by the browser.<br><br>2. The server receives the request and sends back an acknowledgment(ACK) plus SYNC to the browser.<br><br>3. Then the browser receives the ACK + SYN from the server, then responds with an ACK to the web server, establishing the connection established.<br><br>Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets at once, the web server gets exhausted in receiving further SYN packets as it's waiting to complete the handshake process for the larget number of packets. Resulting in the web server not being able to accept more packets.<br><br>The logs show one unknown IP address sending too many SYN packets to the server. This results in the server receiving th SYN and responding with ACK+SYN packets to the IP, but the IP does not send the ACK back to the server, leaving the server waiting for the ACK for ever, not been ablee to receive new packets. The organizational server can not serve the employees, resulting in them not being able to continue with their work.<br><br>To present SYN flood in the future, a stateful firewall or next-generation firewall can be used. |
| |