# 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 that the webserver is overwhelmed and thus unable to respond to user requests. Indeed, the log shows increasing SYN packet requests from the same unrecognized IP address (203.0.113.0) simulating legitimate TCP activity, along with the requests of recognized employee IP addresses (198.51.100.0/24); which gradually resulted in the web server being overwhelmed with SYN requests, and thus becoming unable to acknowledge and complete any requests. This abnormal event is very likely a DoS SYN flood attack, and requires immediate action to mitigate damage. | |
|

| **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 user sends a [SYN] (synchronize) packet to request a connection to the webpage hosted on the company web server.  2. The web server answers with a [SYN, ACK(acknowledge)] packet accepting the connection and reserves its system until the final part of the “handshake”.  3.The user’s device acknowledges the connection with a [ACK (acknowledge)] packet, thus establishing the connection and accessing the web server system.  When a malicious actor sends a large number of SYN packets all at once, if the servers can’t process the amount of packets, it will become overwhelmed and thus unable to complete any request. That is why employees are being given the error message “HTTP/1.1 504 Gateway Time-out (text/html)”, which in more technical terms means that the server instead of acknowledging the connection, asks the user to reset it with the [RST, ACK] packet.  The log indicates an increasing and abnormal amount of SYN packets sent by an unrecognized IP (203.0.113.0), along with the SYN packet requests by employee addresses (198.51.100.0/24). The increasing amount of requests gradually taxes the web server capacity, thus at first slowing down the [SYN, ACK] packets and later outright causing the server to be overwhelmed and instead return [RST,ACK] packets. Eventually, if proper action is not taken the server will crash and business continuity will not be possible. This is dire since it would cost the company money, time and possibly reputation. |