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: there are an abnormal number of SYN requests coming in at a rapid pace which may indicate a DoS attack. The logs show that: There are HTTP/1.1 504 Gateway Time-out (text/html) error messages and [RST, ACK] packets being sent to the requesting visitor. This shows the visitor is receiving timeout error messages in their browser and the connection is dropped. The web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack. As there is only one IP address attacking the web 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: 1. The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. 2. The [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. 3. The [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server will become overwhelmed and unable to respond to the SYN requests. Explain what the logs indicate and how that affects the server: The logs indicate an abnormal number of SYN packets which overloaded the server. This prevented legitimate employee visitor traffic to occur. The potential consequences of this attack include a pause

to business operations which may result in a loss of revenue for the company. To prevent this type of attack in the future, implement a firewall by configuring it to refuse unauthorized IP packets and suspicious traffic.