Section 1: Identify the Type of Attack

One potential explanation for the website's connection timeout error message is that the company's web server is being flooded with TCP connection requests, resulting in an overload that prevents legitimate users from establishing new sessions.

The logs show that a large number of repetitive TCP SYN packets are being sent to the web server's port 443 (HTTPS) from a single external IP address (`203.0.113.0`), without completing the three-way handshake. These SYN requests continue at an abnormally high rate, overwhelming the server.

This event could be a TCP SYN Flood Attack, which is a type of **Denial-of-Service (DoS)** attack. This occurs when an attacker sends numerous SYN packets without completing the handshake, forcing the target to maintain half-open connections and exhaust server resources.

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 over TCP. The three steps are:

1. **SYN:** The client sends a SYN packet to the server to initiate a connection.
2. **SYN-ACK:** The server responds with a SYN-ACK packet to acknowledge the request.
3. **ACK:** The client replies with an ACK packet, completing the connection setup.

When a malicious actor sends a large number of SYN packets all at once:
In a SYN flood attack, the attacker sends thousands of SYN packets rapidly but never responds with the final ACK. The server allocates memory and processing resources for each half-open connection, only to wait for an ACK that never arrives. This causes the server's connection queue to fill up, leaving no capacity to process legitimate connection requests.

The logs indicate how that affects the server:

The packet logs show continuous SYN packets from the same IP (`203.0.113.0`) without corresponding ACK responses. The server repeatedly sends SYN-ACK packets but receives no replies, indicating that the handshake is incomplete. This results in a backlog of half-open connections, causing the server to time out, drop connections, and eventually become unresponsive.

Section 3: Describe the Attack Impact

Description of the Attack:

This is a **TCP SYN Flood DoS attack**, which exploits the TCP handshake mechanism to consume system resources. It prevents legitimate users from connecting to the website by overwhelming the target's connection handling capacity.

Impact on Network Performance:

- The web server becomes slow, unstable, or completely unavailable.
- Employees cannot access the company's sales page to search for vacation packages.
- Customers experience timeouts or "Service Unavailable" errors when visiting the website.
- Server CPU and memory utilization spike abnormally due to queued connection attempts.

Potential Consequences for the Organization:

- Temporary website downtime leading to loss of sales and customer trust.
- Reduced employee productivity since internal operations depend on the website.
- Potential exposure to secondary attacks while the system is under stress.
- Negative reputation impact due to website inaccessibility.

Section 4: Recommended Preventive Measures (Optional)

To prevent future SYN flood or similar DoS attacks:

- **Deploy Intrusion Detection and Prevention Systems (IDS/IPS)** to monitor abnormal traffic patterns.
- **Enable SYN cookies** on web servers to handle half-open connections.
- **Rate-limit incoming connections** using firewalls or load balancers.
- **Use a DDoS mitigation service** such as Cloudflare or AWS Shield.
- **Implement IP blacklisting and connection timeouts** for repeated offenders.

✅ **Summary:**

The network interruption was caused by a **TCP SYN Flood DoS attack**, which overwhelmed the company's web server with incomplete TCP connection requests. The excessive SYN packets prevented legitimate users from accessing the site, resulting in slow performance and timeout errors.