# 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 a Denial of Service (DoS) attack, specifically a SYN flood attack.  
  
The logs show that a large number of TCP SYN requests were being sent from a single, unfamiliar IP address. The high volume of SYN requests overwhelmed the server’s resources, preventing it from completing the handshake process and establishing legitimate connections with employees trying to access the website.  
  
This event could be classified as a direct DoS attack, rather than a Distributed Denial of Service (DDoS) attack, since the attack appears to originate from a single source rather than multiple distributed sources.

## 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. The handshake involves the following steps:  
  
1. SYN (Synchronize) – The client sends a SYN request to initiate a connection with the server.  
2. SYN-ACK (Synchronize Acknowledge) – The server responds with a SYN-ACK, acknowledging the request and reserving resources for the connection.  
3. ACK (Acknowledge) – The client replies with an ACK to complete the handshake, establishing a connection for data transmission.  
  
A SYN flood attack occurs when a malicious actor sends a large number of SYN packets all at once, but does not complete the handshake by sending the final ACK. This leaves the server waiting for the final acknowledgment and tying up resources in the process. Since the server can only handle a limited number of pending connections, legitimate requests cannot be processed, causing service degradation or total unavailability.  
  
The logs indicate that the attacker’s IP address (203.0.113.0) repeatedly sent SYN packets without completing the handshake, preventing normal traffic from being processed. Over time, the server was overwhelmed and stopped responding to legitimate requests. This resulted in employees encountering connection timeout errors and being unable to access the company’s website.

## Section 3: Impact on the Organization

The negative impacts of this SYN flood attack include:  
  
- Service downtime: Employees and customers were unable to access the website, potentially leading to lost business opportunities.  
- Operational disruption: Employees could not search for vacation packages, delaying customer service and sales operations.  
- Resource exhaustion: The server’s resources were occupied by malicious SYN requests, preventing legitimate traffic from being processed.  
- Potential financial loss: If the attack persists, the company may suffer financial losses due to downtime and lost transactions.  
- Security concerns: An ongoing attack raises the risk of further intrusions, necessitating immediate action to mitigate and prevent future occurrences.

## Section 4: Suggested Preventative Measures

To prevent future SYN flood attacks, the following security measures should be implemented:  
  
1. Rate Limiting: Restrict the number of SYN requests from a single IP within a given time frame.  
2. TCP SYN Cookies: Enable SYN cookies to prevent half-open connections from exhausting resources.  
3. Firewall and IPS Rules: Configure firewalls and Intrusion Prevention Systems (IPS) to detect and block abnormal SYN traffic.  
4. Blackhole Routing: Redirect traffic from malicious IP addresses to a null route, effectively dropping attack packets.  
5. Load Balancing and Redundancy: Distribute traffic across multiple servers to prevent a single point of failure.  
6. Traffic Monitoring: Continuously monitor network traffic to detect and respond to suspicious activity in real-time.  
  
By implementing these measures, the organization can mitigate the risk of future SYN flood attacks and ensure the website remains accessible to employees and customers.