**Cybersecurity Incident Report: SYN Flood Attack**

**Part 1: Description of the Attack**

**Attack Type:**  
The network attack observed in this scenario is a **SYN Flood Attack**, a type of Denial of Service (DoS) attack. This attack involves an attacker sending a large number of TCP SYN requests to a target server. These SYN requests are the first step in the three-way handshake process that establishes a TCP connection.

**Symptoms and Characteristics:**  
The primary symptom of a SYN Flood Attack is an overwhelming number of SYN packets sent to the target server from one or more IP addresses. In this case, the packet sniffer detected an abnormally large number of SYN requests from an unfamiliar IP address. The server became overwhelmed by the volume of incoming traffic, leading to a connection timeout error when attempting to access the company’s website.

**Part 2: Impact on the Organization’s Network**

**Effect on Network Performance:**  
The SYN Flood Attack affected the company’s network by overwhelming the web server with excessive connection requests, exhausting its resources and preventing it from processing legitimate requests. This resulted in the server becoming unresponsive, causing a connection timeout error when employees and customers attempted to access the website. The attack interrupted the normal functioning of the website, which is critical for the company’s operations, especially since the site is used to advertise sales and promotions.

**Potential Consequences:**  
The immediate consequence of this attack was a disruption of service, preventing employees from accessing the sales webpage to assist customers. This could lead to a loss of revenue, as potential customers might be unable to view or purchase vacation packages. Furthermore, if the attack persists, it could lead to prolonged downtime, damaging the company’s reputation and customer trust.

**Suggested Mitigations:**  
To prevent future SYN Flood attacks, the following measures can be considered:

1. **Implement SYN Cookies:** This technique helps manage incoming SYN requests without allocating resources until the handshake is completed, mitigating the impact of a SYN Flood attack.
2. **Deploy a Web Application Firewall (WAF):** A WAF can filter and block malicious traffic before it reaches the server.
3. **Rate Limiting:** This can be configured to limit the number of SYN requests that any single IP address can send, reducing the likelihood of a successful attack.