Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The logs indicate that shortly after a successful connection from the external IP (198.51.100.23) to the internal sales page (192.0.2.1), traffic was detected from another external client (203.0.113.0). While the initial packets completed the TCP handshake, the following 138 requests from this IP repeatedly sent SYN packets. This behavior suggests: A potential SYN flood attack.

Section 2: Explain how the attack is causing the website to malfunction
When visitors attempt to connect to a web server, a three-way handshake occurs using the TCP protocol. The client first sends a synchronization (SYN) packet to the server, indicating a desire to establish a connection. The server then responds with both a SYN and Acknowledgment (SYN/ACK) packet, acknowledging the request. Finally, the client sends an acknowledgment (ACK) packet, completing the handshake and establishing a successful connection. However, when a malicious actor floods the server with a large number of SYN packets without allowing time for the server to respond with the necessary SYN/ACK, the system becomes overwhelmed. This leads to the server being unable to handle the traffic, causing the website or domain to become unavailable. The logs indicate that IP address 203.0.113.0 is sending an excessive number of SYN requests, resulting in the firewall responding with a 504 Gateway Timeout error, signaling that the server cannot complete the connection due to the flood of requests.