Incident report analysis

Summary	Today the company's network services suddenly stopped working for approximately two hours. All network resources were affected during the period when the incident occurred. The cybersecurity team found that this was due to a Distributed Denial of Service attack (DDoS) which overwhelmed the company's servers with a high number of incoming ICMP packets. The team block the attack by disabling all non-critical network services so that they could restore critical services.
Identify	The incident management team audited the systems, devices, and access policies affected by the attack to identify the gaps in security. The team found that malicious actors had used a vulnerability in the firewall configuration to overwhelm the company's network with a flood of incoming ICMP packets.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets.
Detect	To detect new unauthorized access attacks in the future, the team will use a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Additionally, the team have installed a Network monitoring software to detect abnormal traffic patterns as well as an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	For future incidents, the incident management team will respond by blocking incoming ICMP packets and stopping all non-critical network services offline. They will attempt to restore critical network services so that employees are able to resume their usual work. The team will inform all internal stakeholders of the reasons of the network outage so that the management team can contact clients to make them aware of why services were down. Management will also need to inform law enforcement and other organizations as required by local laws.

Recover	To recover from a DDoS attack, all essential services need to be reinstated as soon as possible while having non-critical services disconnected to reduce traffic. Priority will be given to restoring critical services first, followed by non-critical as soon as the attack has ceased. Incoming ICMP packets will be filtered through at firewall level thanks to the new configuration.