Incident report analysis

Summary	The company experienced a DDoS attack caused by a flood of ICMP packets that overwhelmed the network, causing a two-hour outage. The vulnerability was due to an unconfigured firewall, and the company mitigated the issue with new firewall rules, source IP verification, and the installation of network monitoring software.
Identify	The company experienced a DDoS attack caused by a flood of ICMP packets that overwhelmed the network, causing a two-hour outage. The vulnerability was due to an unconfigured firewall, and the company mitigated the issue with new firewall rules, source IP verification, and the installation of network monitoring software.
Protect	Implement firewall rules to limit ICMP traffic, verify IP addresses, and strengthen security policies to prevent DDoS attacks. Ensure proper configuration of firewalls and continuous staff training on security measures.
Detect	Utilise network monitoring tools and IDS/IPS systems to detect abnormal traffic and suspicious ICMP activity, improving detection capabilities.
Respond	The incident response involved blocking incoming ICMP traffic, stopping non-critical services, and restoring essential ones. This highlights the importance of a clear and efficient incident response plan.
Recover	After responding, the team should review the event to improve procedures, and apply additional recovery steps such as refining firewall rules and updating response protocols to reduce downtime in future incidents.