Incident report analysis

Summary	The organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The network services suddenly stopped responding due to a flood of ICMP packets and normal internal traffic could not access any network resources. The incident management team responded by blocking ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The company's cybersecurity team investigated the security event and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. The entire internal network was affected, all critical network resources needed to be secured and restored to a functioning state.
Protect	The security team implemented: an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics, and a new firewall rule to limit the rate of incoming ICMP packets.
Detect	To detect abnormal traffic patterns, the security team has implemented network monitoring software, and source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	The team will create a backup system for future events so any critical systems and services that go down can be restored quickly to their working states. The team will analyze network logs to check for suspicious and abnormal activity. The team will do regular firewall rules maintenance to ensure that all of the unused ports are disabled to eliminate unwanted communications.
Recover	The critical network services will need to be recovered immediately to ensure

	business continuity in the event where the server is under DDoS attack. External ICMP flood attacks can be blocked at the firewall. Any non-critical network services should be stopped to reduce internal network traffic.

Reflections/Notes: