Incident report analysis

Summary	Recently, our company was subject to a DDoS attack in which the internal network was compromised for about two hours. All network services suddenly stopped responding and normal internal network traffic could not access any network resources.
Identify	The incident management team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a DDoS attack.
Protect	The team has implemented several new features to mitigate risk for any future attacks. First, a new firewall rule to limit the rate of incoming ICMP packets was put in place. Then, source IP verification on the firewall was also added to check for spoofed IP addresses on incoming ICMP packets. Finally, an IDS/IPS system was implemented to filter out some ICMP traffic based on suspicious characters.
Detect	To detect such an attack in the future, the team introduced network monitoring software to detect abnormal traffic patterns.
Respond	The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Recover	Now that new firewall rules and network monitoring software have been implemented, critical network services have been restored and remain operational.