Incident report analysis

Summary	This morning our security team discovered that our organization’s internal network was down and inaccessible and we could not access any internal network resources.
Identify	Our team then investigated this event and found out that a threat actor had sent a flood of ICMP pings into the company’s network through a firewall that was not properly configured. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The the team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets has timed out, all non-critical network systems and services can be brought back online.