Incident report analysis

Summary	Recently the company's internal network was ICMP flooded, bringing down the internal network for two hours. The initial security team response was blocking the traffic and restoring services.
Identify	A critical firewall on a cloud service had been left unconfigured allowing for this DDOS. All critical network resources needed to be secured and restored to a functioning state.
Protect	A new firewall rule to limit the rate of incoming ICMP packets was applied and source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets was additionally configured.
Detect	Network monitoring software to detect abnormal traffic patterns was added as well, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	In the future, the responding team should first isolate the affected network and systems. Attempt to restore any critical services that had been brought down. Identify the root issue or attack vector by reviewing logs, dashboards, investigating, etc.
Recover	Finally, incident responders restored all systems to normal operational functionalities.

Reflections/Notes: