Incident report analysis

Here I use the NIST framework to deal with a Security Incident described in the Summary section bellow and implement measures accordingly.

Summary	The organization recently experienced a DoS attack, which compromised the internal network for two hours until it was resolved.During the attack, our network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that a malicious actor had sent a flood of ICMP pings into the company's network through a misconfigured Firewall. This allowed the malicious attacker to overwhelm the company's network through a denial of service (DoS) attack.
Protect	- A new firewall rule to limit the rate of incoming ICMP packets. - Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
Detect	- Network monitoring software to detect abnormal traffic patterns - An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics - implementing a SIEM solutions if not already in place.
Respond	- Blocking Rogue IP addresses related to the Attack using firewall rules. - Stopping all affected services. - Inform upper management of this event and they will contact affected

	customers by mail to inform them about the Network Outage. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	- Restoring critical network services back to normal Operations.