Incident report analysis

Summary	A Multi-Media Marketing company recently experienced a DDoS attack. The internal network was down for two hours because of it. The networked stopped responding due to ICMP packets flooding the network.
Identify	A flood of ICMP pings was sent into the network through an unconfigured firewall. This created the DDoS attack and the internal network was down for two hours. Normal internet network traffic could not access the network or resources.
Protect	The firewall needs to be configured. If the firewall can limit the number of incoming ICMP packets, it will prevent this particular issue from happening again. The firewall can also have a Source IP address verification to ensure there is no spoofing of IP addresses.
Detect	A network monitoring software could help detect abnormal traffic in the future. An intrusion detection system could also help with this.
Respond	In the event of similar events in the future, the team should isolate the systems being impacted. It's important to focus on restoring the critical systems that were impacted by the attack. The network logs should be reviewed to pinpoint any activity that might be causing the issue.
Recover	In the future, Using the softwares and systems described above, this type of attack can be quickly identified for a faster response. Additionally, having the firewall configured will help reduce the size of the attack if one occurs again. Implementing these procedures will help the network get functioning and will prevent further attacks of this nature. Adding these controls in as regular security measures can help mitigate current or future attacks.