Incident report analysis

Summary	DDOS Attack
Identify	This morning, it was reported that many members of the company were not able to use the internet and their networks could not connect. After an investigation, it was found that a ICMP flood was occurring to our networks. We quickly responded by halting ICMP packets, and shut down non critical network functions. After the incident and an investigation, the ICMP attack occurred through a vulnerability found through a firewall that was not configured to our typical standards. We immediately configured the firewall and brought the networks running again.
Protect	The team has implemented improved methods on a consistent schedule to follow up and keep track of our current and new firewalls.
Detect	To keep our firewalls configured properly and to detect other possible vulnerabilities , our team will do frequent checks and updates
Respond	The team halted all incoming ICMP packets and shutdown non critical network functions.
Recover	Vulnerability was found and configured correctly. Networks were brought up again.

Reflections/Notes: New/ Updated firewalls need to have a procedure to configure before use. With diligence and awareness, this incident will not occur once more.