Summary	There was an incident when all services suddenly stopped responding. After investigating, it was discovered there was a DDoS attack through a flood of incoming ICMP packets. The attack was blocked and critical network services where restored.
Identify	There was an ICMP flood attack that affected the entire internal network, which then needed to be secured and restored to a functional state.
Protect	A new firewall limit to the number of incoming ICMP packets was implemented, as well as an IDS/IPS system to filter out suspicious ICMP traffic. .
Detect	The firewall was configured anew, to check for suspicious IP addresses on incoming ICMP packets. Also, network monitoring software to detect abnormal traffic patterns was installed.
Respond	To prevent future attacks, the network will be segmented and baselining procedures for restoring to a previous healthy state will be followed. Also, there will be SIEM tools to record and analyse logs to be able to detect suspicious activity.
Recover	Recovering the system means to restore it at a previous functional state. After the stopping of operations, they need to restart, with priority to the critica services, followed by the non-critical ones.