Incident report analysis

Summary	Recently, the company's cybersecurity team investigated an event that appears to be a DDoS attack coming through an unconfigured firewall, after which all network services of the company stopped responding. The network was flooded by ICMP packets. The incident response team blocked all of the incoming ICMP packets and began to restore all critical network services. After two hours, network services started to respond normally.
Identify	The cybersecurity team analyzed network traffic and realized that it was flooded with ICMP packets, to the point that all network services of the company were overwhelmed and stopped working - a classic DDoS attack. They also performed an audit of the company's network infrastructure and came to a realization that an unconfigured firewall was a possible reason why the malicious actor could successfully perform this attack.
Protect	The team has implemented a firewall configuration rule to limit the rate of incoming ICMP packets, as well as source IP address verification to check for spoofed IP addresses on them.
Detect	The team has updated their operating systems with a new network monitoring software to detect abnormal traffic patterns.
Respond	An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics was implemented on the network infrastructure.
Recover	The team will continuously monitor all of the systems, devices and network infrastructure, especially the IDS/IPS system and firewalls, in order to keep it maintained properly, which will mitigate the risk of another DDoS attack.