Incident report analysis

Summary	This morning, our company experienced a DDOS attack which compromised the internal network for two hours until it was resolved. The attack occurred when our organization's network services suddenly stopped responding, which the cybersecurity team assumed to be a type of smurf attack.
Identify	After a thorough investigation, the cybersecurity team found an incoming flood of ICMP packets being sent to our organization's network service. A malicious actor is believed to have sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed attackers to overwhelm the company's network using the DDOS attack.
Protect	To prevent future DDOS attacks, we implement a new firewall rule that limits the rate of incoming ICMP packets. Also, we use the source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Detect	To make sure we can detect suspicious packets faster, we will use network monitoring software such as Wireshark to detect abnormal traffic patterns.

	Furthermore, we will invest in an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	The incident management team responded by blocking ICMP packets by isolating the network service from the internet. We only stopped all non-critical network services offline to minimize the attack surface, the critical network service will still remain operational with extra monitoring.
Recover	After two hours of isolating the network service from the internet, the malicious attacker had stopped flooding ICMP packets into the network. After that, The incident management team restored the critical network services and enabled the non-critical services to start operating online gradually.

Reflections/Notes: