Incident report analysis

Summary	On [September 13th 2025, 1:40 PM], the organization’s internal network was disrupted for approximately two hours due to a Distributed Denial of Service (DDoS) attack. The attack was carried out using a flood of ICMP (ping) packets that overwhelmed the company’s unconfigured firewall. This caused the network to become unresponsive, preventing normal traffic from accessing internal services. The incident management team responded by blocking ICMP packets, shutting down non-critical services, and restoring essential network functions. The investigation revealed the firewall lacked proper configuration to limit ICMP traffic, which made the network vulnerable to this type of attack.
Identify	● **Type of attack:** Distributed Denial of Service (DDoS) attack using ICMP flooding ● **Attack source:** Malicious external actor leveraging multiple distributed systems ● **Systems impacted:** ○ Firewall (unconfigured, allowed excessive ICMP packets) ○ Internal network infrastructure (routers/switches) ○ Critical business services hosted on internal servers
Protect	**To further secure organizational assets and prevent recurrence:** ● **Implement firewall rules to limit ICMP packet rates and block**

	unnecessary ICMP traffic. ● **Require regular firewall configuration reviews and audits.** ● **Apply network segmentation to isolate critical assets from public-facing services.** ● **Provide staff training on recognizing DDoS patterns and escalation procedures.**
Detect	To improve early detection of similar incidents: ● Deploy **network monitoring software** to identify abnormal traffic spikes. ● Configure IDS/IPS systems to detect and alert on suspicious ICMP floods or traffic anomalies. ● Implement **log aggregation with SIEM tools** to correlate unusual patterns across firewalls, routers, and servers. ● Establish baselines of normal traffic for comparison to detect anomalies faster.
Respond	Response procedures for future incidents should include: ● Immediate containment by rate-limiting or dropping malicious traffic at the firewall/router level. ● Collaboration with the internet service provider (ISP) for upstream traffic filtering. ● Activation of an incident response playbook specifically for DDoS attacks. ● Preservation of log data and packet captures for forensic analysis. ● Post-incident debriefs to refine detection and prevention measures.

Recover	Steps to ensure business continuity and resilience: ● Restore normal network services once malicious traffic has been blocked. ● Validate that all critical systems (web servers, internal apps, DNS) are fully operational. ● Perform integrity checks to ensure no data loss or system compromise occurred during the attack. ● Update firewall baselines and document lessons learned. ● Consider deploying a DDoS protection service (e.g., Cloudflare, Akamai) to reduce downtime in the event of future attacks.

Reflections/Notes: