Incident report analysis

Summary	Recently, the organization experienced a **Distributed Denial of Service (DDoS)** attack that disrupted internal network services for approximately two hours. The attack was carried out using a **flood of ICMP packets**, which overwhelmed the network and rendered it unresponsive. The root cause was identified as an **unconfigured firewall**, which allowed the malicious traffic to penetrate the network. The incident caused a complete halt of internal communications, service availability, and access to shared resources. The incident response team mitigated the attack by blocking incoming ICMP traffic, shutting down non-critical services, and restoring critical operations. The estimated impact includes temporary business disruption, potential loss of client trust, and operational delays.
Identify	Type of attack occurred: Distributed Denial of Service (DDoS) via ICMP Flood Affected System: Internal network infrastructure
Protect	To better protect the organization moving forward, the following actions are necessary: • Implement a new firewall rule to limit the rate of incoming ICMP packets • Enable source IP address verification on the firewall to block spoofed ICMP packets

Detect	Detection methods must focus on identifying abnormal traffic early: ● Deploy network monitoring software to analyze real-time traffic flows and detect anomalies. ● Use Intrusion Detection and Prevention Systems (IDS/IPS) to flag and block suspicious ICMP traffic patterns.
Respond	A clear and tested response plan is vital: ● Blocking incoming ICMP packets ● Stopping all non-critical network services offline ● Use playbooks for DDoS-specific incidents
Recover	To return to normal operations and improve recovery time: ● Restore all affected network services after ensuring the threat is fully neutralized. ● Verify integrity of data and configurations before bringing systems online. ● Update and harden firewall rulesets and device configurations based on lessons learned. ● Conduct a recovery drill to simulate response to similar attacks in the future. ● Document the incident and integrate findings into a refined incident response and recovery plan. ● Notify leadership and legal/compliance teams as required.