



Incident report analysis

Summary	The organization recently experienced an attack in which the network was flooded with ICMP packets, causing the network services to suddenly become unresponsive. This attack halted business operations for two hours. The cybersecurity team investigated the event and found that a malicious actor sent the ICMP packets into the network through an unconfigured firewall. The team responded by blocking incoming ICMP packets, stopping non-critical network services, and restoring critical network services.
Identify	The malicious actor performed a distributed denial of service (DDoS) attack by exploiting an unconfigured firewall and flooding the organization's network with ICMP pings. All network services were affected as they could no longer access network resources.
Protect	The security team has configured the firewall to prevent similar attacks in the future. They implemented a new firewall rule that limits the rate of incoming ICMP packets. They will use an intrusion prevention system (IPS) to filter out ICMP traffic with suspicious characteristics.
Detect	They team implemented a network monitoring software to detect abnormal network traffic patterns. They implemented source IP address verification on the firewall to check incoming ICMP packets for spoofed IP addresses. They will also use an intrusion detection system (IDS) to monitor incoming ICMP traffic.
Respond	The team should respond to future incidents more easily with the new detective and preventive controls. They will block incoming ICMP traffic to mitigate the impact of the attack. The team will analyze network logs to investigate abnormal activity and update the firewall rules to block incoming traffic from known IP addresses involved in previous incidents. All incidents will

	be reported to upper management and stakeholders.
Recover	After blocking all incoming ICMP packets, the team will stop all non-critical network services in order to save network resources. They will restore critical services to a functioning state first, and then they will bring the non-critical services back online.
