Incident report analysis

Summary	A DDoS attack on the company's network caused a two-hour outage. The attack exploited an unconfigured firewall, allowing a flood of ICMP packets to overwhelm network resources. Mitigation measures included firewall rule changes, IP verification, network monitoring, and IDS/IPS deployment.
Identify	The attack primarily impacted network services, infrastructure (including the firewall and internal servers), and disrupted operations for both internal teams and external clients.
Protect	**Moving forward, stricter firewall rules with source IP verification are essential. Regular security training for employees, data backups with encryption, and updated incident response procedures are critical. Additionally, ongoing firewall maintenance and the deployment and maintenance of IDS/IPS systems will significantly improve network security.**
Detect	The attack highlighted a need for better real-time monitoring and fine-tuning of existing systems to detect anomalies like the abnormal ICMP traffic surge. Implementing 24/7 network monitoring is a priority.
Respond	A comprehensive DDoS response plan should be developed, including clear escalation procedures, communication protocols, and effective mitigation strategies. Post-incident analysis will be crucial to identify the root cause, evaluate response effectiveness, and recommend improvements. Exploring cloud-based DDoS protection services should be considered as an additional layer of defense.

Recover	Formalized procedures for restoring services and data from backups are necessary. Regular testing of these processes will ensure their effectiveness. Establishing clear communication channels will keep stakeholders informed about service restoration and potential impacts.

Reflections/Notes: This incident underscores the importance of proactive security measures, continuous monitoring, and employee awareness training. Implementing additional security measures like rate limiting and considering cloud-based DDoS protection can further fortify the network against future attacks.