# Incident report analysis

| | |
|---|---|
| **Summary** | On July 27, 2024, a distributed denial-of-service (DDoS) attack caused a two-hour network outage, severely impacting internal operations and client services. The root cause was identified as an unconfigured firewall, which allowed a flood of ICMP packets to overwhelm network resources.<br><br>The attack underscored critical vulnerabilities in the company's security posture. Immediate actions included firewall rule adjustments, source IP verification, and deployment of network monitoring and IDS/IPS systems. However, a comprehensive review of security practices is necessary to prevent future incidents.<br><br>Moving forward, the following key areas require attention: |
| Identify | The attack primarily impacted network services, and infrastructure (including the firewall and internal servers), and disrupted operations for both internal teams and external clients. |
| Protect | **Implement stricter firewall configurations, regular employee security training, encrypted data backups, and updated incident response procedures. Ongoing firewall maintenance and IDS/IPS systems are essential for proactive defense.** |
| Detect | Enhance real-time monitoring and fine-tune existing systems to rapidly detect traffic anomalies. 24/7 network monitoring is now a priority. Implementing 24/7 |

| | |
|---|---|
| | network monitoring is a priority. |
| Respond | Develop a detailed DDoS response plan, including escalation protocols, communication strategies, and mitigation procedures. Post-incident analysis will be crucial to identify the attack's root cause and inform future improvements. |
| Recover | Formalized procedures for restoring services and data from backups must be established and regularly tested. Clear communication channels with stakeholders are vital to manage expectations and minimize disruption. |

---

| |
|---|
| 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. |