

Incident Report Analysis: ICMP Flood DoS Incident

Summary	The company experienced a security event when all network services suddenly stopped responding due to a Denial of Service (DoS) attack caused by an incoming flood of ICMP packets. An unconfigured edge firewall permitted the malicious traffic into the internal network, completely blocking legitimate employee access to network resources for two hours. The incident management team contained the event by blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical services. Following containment, the security team updated firewall rules, enabled source IP verification, deployed network monitoring tools, and implemented an IDS/IPS system.
Identify	**Attack Type:** Denial of Service (DoS) attack using an ICMP packet flood (ping flood). **Vulnerability:** Unconfigured network firewall allowing unfiltered incoming ICMP traffic. **Impacted Systems:** The entire internal network, including critical business services, non-critical services, and employee access to network resources during the two-hour outage.
Protect	Implemented a new firewall rule to limit the rate of incoming ICMP packets and prevent bandwidth congestion. Deployed an IDS/IPS system to filter out suspicious ICMP traffic based on packet characteristics and anomaly signatures. Established routine audits of firewall configurations and access policies to ensure security controls remain properly configured.
Detect	Configured source IP address verification on the firewall to check for and drop spoofed IP addresses on incoming ICMP packets.

	Implemented network monitoring software to detect abnormal traffic patterns and alert analysts to unusual volumetric spikes. Established continuous network traffic logging to monitor incoming external packets from non-trusted sources.
Respond	**Containment:** Take non-critical network services offline immediately during an incident to conserve bandwidth for essential functions and isolate impacted network segments. **Neutralization:** Block incoming ICMP packet floods at the perimeter firewall to stop active disruption. **Analysis & Communication:** Analyze network logs to investigate traffic behavior, identify source vectors, and brief management and legal teams on incident status.
Recover	**Restoration Strategy:** Stop non-critical network services to reduce internal traffic, then restore critical network services first to resume key business operations. **System Verification:** Confirm that ICMP flood traffic has timed out and firewall filters are blocking malicious traffic before bringing non-critical systems back online. **Post-Incident Process:** Conduct a post-incident review to refine recovery workflows and improve future response procedures.

Reflections/Notes: This security incident demonstrates the risks associated with unconfigured firewall boundaries [cite: 5]. Applying the NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, Recover) ensures the organization shifts from reactive troubleshooting to an organized, proactive defense strategy.