Incident report analysis

Summary	At 0900 hours this morning, an outage was reported that showed our organizational website was unreachable. After a review of network traffic affecting our web server we determined that the issue was a flood of ICMP packets affecting our host server, commonly referred to as a DoS attack. Incident management blocked incoming ICMP packets, making the server available for our team to prevent consecutive attacks. We observed that our firewall was not configured to rate ICMP pings to our network. The security team instantiated a new firewall rule to rate limit incoming ICMP packets, as well as instantiated source IP address verification to check for spoofed IP addresses. Additional network analysis tools have been installed to assist the security team in identifying and stopping threat actors prior to malicious activity affecting our assets. Training of employees and personnel on this method of DoS attack has been created, and new policies for firewall rule verifications has been instantiated. A review of organizational assets has been conducted to verify data integrity.
Identify	The security team assessed the assets utilized in the attack and observed faults in the organization firewall configuration with respect to rate limits on ICMP packets, as well as baseline data packet verification.
Protect	The security team instantiated a new firewall rule to rate limit incoming ICMP packets as well as configured source IP address verification to detect spoofed IP addresses on incoming ICMP packets.
Detect	SolarWinds network performance monitor was installed to allow the security team to monitor network performance for abnormal traffic patterns. An in-line intrusion prevention system was integrated to reduce attack vectors from

	known security intrusions and security threats.
Respond	The security team instantiated a quarterly review of firewall rules, and policy for employee verification of necessary patches, updates, or changes in port accessibility and employee access. New duties were assigned to observe network stability utilizing the new network performance monitor and employee training has begun.
Recover	The ICMP DoS attack was blocked by the new firewall rule changes. A review of organizational data integrity was conducted and no intrusions were detected. The server was checked for accessibility. With the server no longer under threat of the DoS attack, the organizational website was returned to public access.
