**Incident Report Analysis**

**Identify:**

The organization’s internal network was compromised as the result of a Distributed Denial of Service (DDoS) attack that overwhelmed the network with a flood of Internet Control Message Protocol (ICMP) packets.

**Protect:**

To prevent this type of attack from occurring in the future the organization should improve the rules in the firewall to place limits on the amount of ICMP packets that are permitted to access the network. Additionally, firewall rules that validate the source IP addresses of incoming traffic should be implemented to prevent IP spoofing.

**Detect:**

A variety of tools can be utilized to assist in preventing these kinds of attacks in the future. An IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) can be utilized to constantly monitor the traffic coming in and out of the internal network. Additionally, use of SIEM tools such as Splunk or Chronicle can aid security professionals in identifying suspicious activity quickly.

**Respond:**

The organization’s security team can effectively respond to security incidents by regularly backing systems to ensure in the event of an attack systems can be restored quickly, utilizing network segmentation so in the result of a security breach the only part of the internal network requires being taken offline as well as preventing other systems on the internal network from becoming corrupted.

**Recover:**

Regular system backups will ensure that the organization is prepared to restore systems in a timely manner if a security breach occurs. Additionally, data necessary for business operations is preserved and not at risk of being permanently lost.