Incident report analysis

Summary	Our company experienced a DDoS attack that made our internal network go down for about two hours. The attack flooded our systems with ICMP packets, which caused everything to stop working. It happened because the firewall didn't have the right settings to block that kind of traffic. Once the team noticed the issue, they blocked the ICMP traffic, turned off non-important services, and brought back the main systems.
Identify	This was a DDoS attack using ICMP flood. The problem was that our firewall didn't have any rules to limit or block ICMP traffic. This caused the whole network to go down. The main systems that were affected were all internal services like internet access, servers, and tools people use every day to do their jobs.
Protect	To protect the company in the future, we need to set up the firewall better so it can stop too many ICMP packets from coming in. We should also add IP address checks and make sure only trusted traffic gets through. The team should review firewall settings more often and train employees on how to spot signs of these types of attacks early on.
Detect	We can use network monitoring tools to keep an eye on traffic and get alerts when something unusual happens. These tools can help us see when there's a sudden spike in ICMP packets. We should also use IDS/IPS systems to help find suspicious traffic before it becomes a problem.
Respond	If this happens again, the team should block the bad traffic fast and take non essential systems offline so the important stuff can keep working. We should also have a plan to tell everyone what's going on and log everything so we can learn from it. After things are under control, we should look at what happened

	and improve our response steps.
Recover	To recover, we can restart systems slowly and check everything to make sure it's running normally. If needed, we can use backup systems. Once things are fixed, the team should review what happened, fix the firewall settings, and update the plan so we’re more prepared next time.
