If your network has both a firewall and an IDS deployed, would you consider it to be fully secure? Why or why not?

**Firewall**

Through a firewall, a network security device, incoming and outgoing network traffic is monitored and filtered based on previously established security policies for the company. At its most basic level, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

Firewalls employ broad or specific parameters to function, allowing some types of communication while blocking others. The operation of a firewall is frequently controlled by a set of strict rules that either permit or prohibit the entry of particular computer connections. These guidelines are flexible and can be changed to meet any need on practically any device that can connect to the internet.

Step 2 of 3

**An intrusion detection system (IDS)**

A monitoring system called an intrusion detection system (IDS) looks for abnormal activity and sends out alarms when it does. A security operations center (SOC) analyst or incident responder can analyze the problem and take the necessary steps to eliminate the threat based on these notifications.

IDS is a server protection tool. IDS is a visibility technology that aids in traffic monitoring at numerous different points and provides visibility into the network's security posture. The IDS enters the network at great depth and examines what is occurring in terms of safety.

Step 3 of 3

The protected servers are too close to firewalls and IDS systems, but they still aren't the first line of defense. However, this is the exact area where DDoS attacks need to be reduced. As a result, DDoS attacks get through the restricted data center unnoticed by the standard system security methods.

Explanation

Without a doubt, DDoS attacks have transformed the security landscape. There is no doubt that the technologies organizations use must continue to adapt as firms modify their security structure architecture to effectively minimize the surge in availability-based assaults. Modern cyber threats demand a comprehensive approach that can defend at the network and application level and effectively distinguish between legitimate and illicit traffic to keep businesses safe and operational. While firewalls and intrusion prevention systems (IPS) are important for system security.

**Final Answer**

However, putting all of your trust in firewall technology could make you feel insecure. The firewall is incapable of resolving the issue on its own, regardless of how it is designed or implemented. Enterprises utilize IDS and IPS services in addition to firewalls to safeguard their data from threats and assaults, but they do not offer full security for your company.