Delve into the world of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), essential components of modern cybersecurity. Investigate their roles, functionalities, and deployment strategies within network environments.

Answer: IDS is a detection system that will give you alarms for you network; in the way you configure it. IPS is a Prevention system that will attempt to block network connections or anything else you configure it to.

Compare and contrast their strengths and limitations, and then design a network scenario where both an IDS and an IPS are strategically employed to detect and prevent potential cyber threats.

Answer: The strength of the IDS is that it is more granular from an alarm system standpoint. You can place this in a network with a strong defense in-depth concept. You can place the IDS at the edge of a network as a proxy of sorts to create a strong perimeter.

Conclude by evaluating the effectiveness of this layered defense approach and its impact on overall security resilience.

Answer: If the IDS and the IPS are implemented in a network that implements a defense in depth concept, you will have a very secure network. If you decided to have a defense in depth solution without the IDS or IPS, you would have a less secure network. The IDS and IPS only serve to strengthen your overall security resilience.