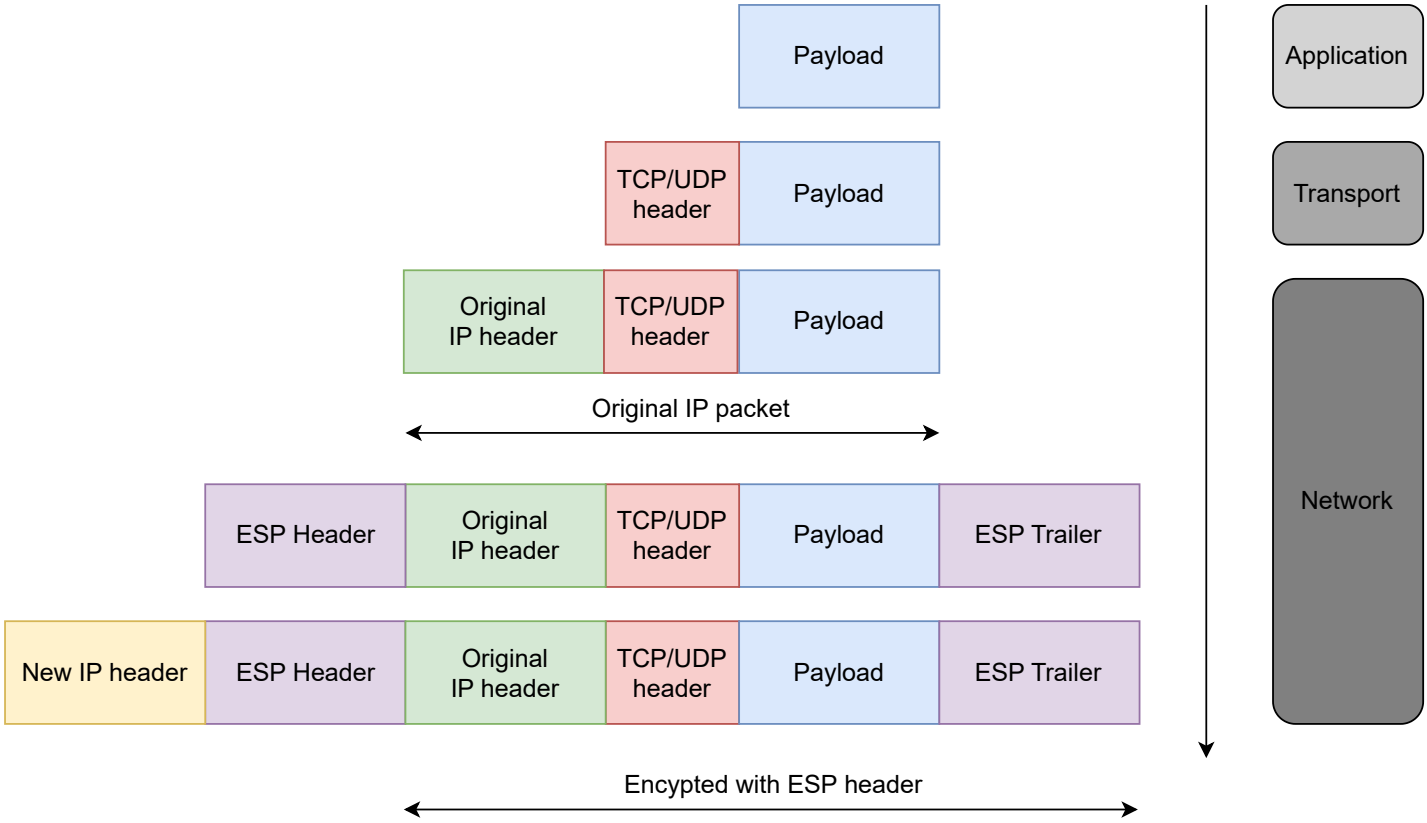
IPSec ESP Tunnel Mode – Packet Encapsulation



This diagram illustrates how data is encapsulated and encrypted in IPSec ESP Tunnel Mode. In this mode, IPSec ensures the secure transmission of the original IP packet. It applies both encryption and integrity protection. The encapsulation process follows these four steps:

1. Original Packet Encapsulation: The original IP packet, which consists of the original IP header, UDP/TCP header, and payload, is encapsulated within a new packet structure.
2. ESP Header and Trailer Addition: IPSec encryption adds an ESP header and ESP trailer around the original packet to ensure confidentiality and data integrity.
3. Encryption: The ESP header encrypts the original IP packet, including the original headers and payload, establishing that the content is hidden from unauthorized viewers.
4. New IP Header: A new outer IP header is added to the encapsulated data to facilitate secure routing over the network.

The far right section of the diagram presents three layers of the OSI model which match the data encapsulation process.