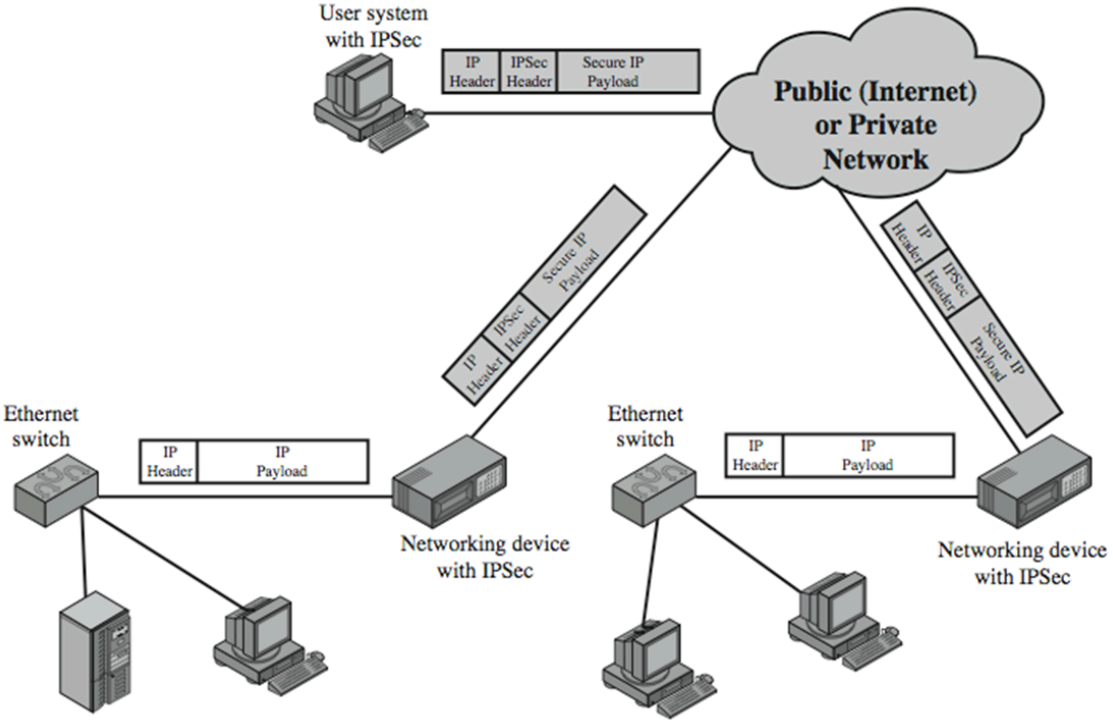
IP安全（IPSec）

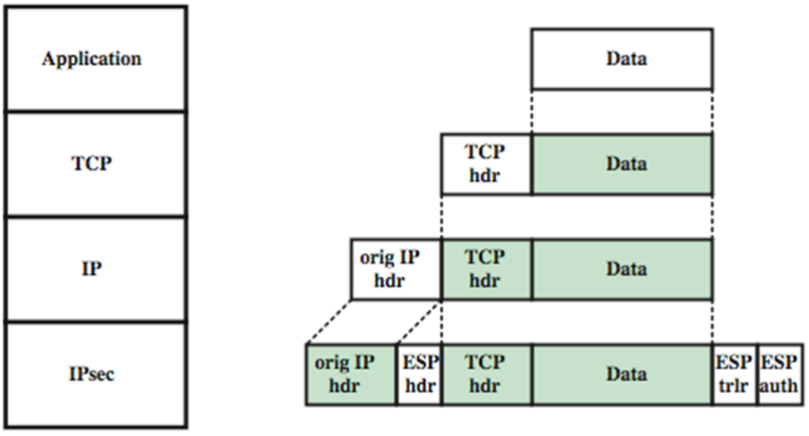
- 出现的原因：存在跨协议层的安全问题
- 提供的功能：认证、保密和密钥管理
- 应用场景：LAN、公共和私有WLAN以及互联网
- 使用



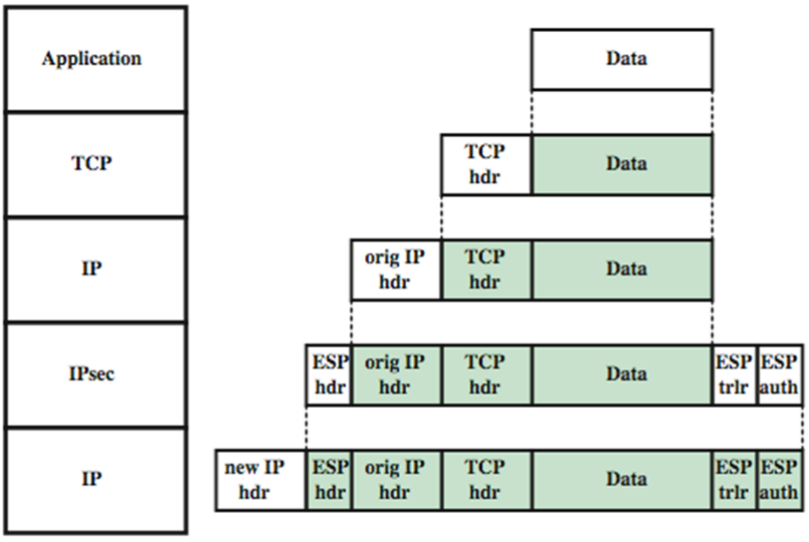
- 优点
  - 在防火墙/路由器中，为跨越周边的所有流量提供强大的安全性
  - 在防火墙/路由器中能抵抗旁路流量
  - 在传输层以下，因此对应用程序是透明的
  - 可以对最终用户透明
  - 可以为个人用户提供安全保障
  - 保证路由架构安全
- 提供的服务
  - 访问控制
  - 无连接的完整性
  - 数据源认证
  - 拒绝重播数据包：部分序列完整性的形式
  - 保密（加密）
  - 有限的通信流量保密
- 模式
  - **运输模式**
    - 加密和（可选地）验证IP数据
    - 可以做流量分析，但效率很高

- 有利于ESP主机对主机流量

- **隧道模式**
  - 加密整个IP包
  - 为下一跳添加新标题
  - 路由器上没有路由器可以检查内部IP头
  - 适用于VPN，网关到网关安全



(a) Transport mode



(b) Tunnel mode