

网络安全

网络通信基础设施安全

- 链路加密
- 窃听攻击

通信协议的安全概念

- Ipssec
 - 传输模式 — 传输层载荷加上ipsec头部的和尾部，然后加上原ip头，此时不保护ip头部
 - 隧道模式 — 将网络层的报文（ip头部和ip有效载荷），加上ipsec的头部和尾部，然后再加上新生成的ip头部
 - 两种安全协议
 - 鉴别头部AH协议 — 提供源端鉴别和数据完整性，但不提供保密性
 - 封装安全载荷ESP协议 — 提供源端鉴别，数据完整性和保密性
- VPN — 虚拟专用网
- SSL — 安全套接字协议

防火墙

- 访问控制
- 入侵检测