访问控制技术

- 防火墙
  - 基本概念
    - 在被保护网络和其他网络之间实施访问控制的一组设备
  - 设计目标
    - 所有的通信，无论是从内部到外部还是从外部到内部，都必须经过防火墙
    - 只有授权的通信才能通过防火墙，这些授权将在本地安全策略中规定
    - 不同类型的防火墙将实现不同的安全策略
    - 防火墙本身对于渗透必须是免疫，这意味着必须使用运行安全操作系统的可信系统
  - 防火墙不可以做什么
    - 需要用户定义访问控制规则，没有缺省配置
    - 不能防止内部恶意的攻击者
    - 无法控制没有经过它的连接
    - 不能很好地防止病毒和信息扩散
    - 不能替代内部网络系统的安全管理
    - 无法防范全新的威胁和攻击
  - 防火墙的屏蔽子网结构
  - 争论
    - 破坏了Internet端到端的特性，阻碍了新应用的发展
    - 先天不足：没有解决网络内部的安全问题，“防外不防内”
    - 给人一种误解，降低了人们对主机安全的意识