常见网络安全防护技术

VPN

- 技术原理：通过在公用网络上建立专用网络，将远程站点或用户连接到一起的专用网络。VPN可以通过加密和隧道协议来保护数据的安全性和隐私性
- 优点：
  - 安全性、隐私性好
  - 防止ISP监视
- 缺点：
  - 普遍性能比较差
  - 对IT服务的访问颗粒度比较粗放，无法做到精细控制，也无法提供基于多重信任要素的安全认证
  - 无法抵御内部攻击

常见网络安全防护技术

端口敲门(Port Nocking)

- 技术原理：客户端以一定顺序尝试连接防火墙上处于关闭状态的端口，防火墙或其他程序监视防火墙日志，当这些尝试符合预先设定的顺序后，防火墙或监视程序会在防火墙上添加一条策略，允许该客户的IP地址在短时间访问指定的TCP端口
- 优点：
  - 解决了防火墙无法动态设置安全策略的弊端
- 缺点：
  - 防火墙的缺点都有
  - 端口敲门过程，额外增加了建立TCP会话的延时
  - 需要修改业务系统的访问IT服务的逻辑