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

常见网络安全防护技术

Single Packet Authorization(SPA)

- SPA是一种对单个数据包进行授权的技术，他可以用于增强服务器的安全性，因为很自由知道特定信息的人/设备才能访问到服务器开放的端口，SPA技术可以拦截未经授权的端口扫描，从而增强了服务器的安全性
- SPA技术作用域SDP客户端和SDP网关之间，已实现强大的服务隐蔽性
- 优点：
  - SPA技术可以拦截掉未授权的端口扫描，从而增强了服务器的安全性
  - SPA技术可以隐藏服务，缩小攻击面
  - SPA技术可以缓解DDOS攻击，使服务只对授权的用户可见
- 缺点：
  - 需要防火墙策略的配合
  - 涉及业务流程的改造