常见网络安全防护技术

防火墙

- 技术原理：通过对入栈、出栈的数据包分析包内的IP地址、端口，看IP地址和端口是否符合预先设定的安全策略，并根据策略对数据包做出放行或者丢弃动作
- 缺点和不足：
  - 防火墙不能抵御最新的未设置策略的攻击漏洞
  - 防火墙的并发连接限制容易导致拥堵或者溢出，成为性能瓶颈
  - 防火墙对服务器合法开放的端口的攻击，无法阻止
  - 防火墙对内部主动发起的攻击一般无法阻止
  - 无法做到设备级的安全策略

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