防火墙、包过滤、NAT、VPN技术的含义

防火墙能实现的哪些功能

防火墙的不足（包括不能实现的具体功能

防火墙发展的趋势

入侵检测、漏洞扫描、漏洞、补丁的含义

IP协议：互联网协议 TCP协议：传输控制协议

防火墙的概念：

防火墙是一种高级访问控制设备，置于不同网络安全域之间，通过相关的安全策略来控制（允许、拒绝、记录）进出网络的行为

防火墙的分类：网络防火墙（专用设备），计算机防火墙（软件）

防火墙的基本功能：NAT功能VPN功能，包过滤，日志审计，时间控制策略

包过滤技术：基于IP地址来监视并过滤网络上流入和流出的IP包，只允许与指定的IP地址通信，起到了保护内部网络的作用

缺点：安全性低如IP欺骗，不能处理网络层上的信息（传输、绘画、表示、应用层

NAT技术：网络地址转换，防火墙能够提供一对一及多对一的地址转换，使内部IP无需变动也能与外界相同，可保护及隐藏内部网络资源，减少IP地址变动从而方便网络管理，并可以解决IP地址不足的问题

Vpn技术：虚拟专用网，通过一个公共网络，建立一个临时的、安全的连接，能提供与专用网络一样的安全和功能保障

防火墙的不足：

1. 虚假的安全感
2. 传输延迟、单点失效
3. 不能实现来自内部的攻击
4. 不能防范不通过它的连接
5. 不能防范利用标准协议缺陷、本身安全漏洞的攻击
6. 不能防范数据驱动式的攻击

防火墙技术的趋势

多功能话，性能，分布式防火墙，强大的审计和自动分析，与其他网络安全技术相结合

入侵检测系统（IDS）

对网络内部进行实时的检测，记录、分析网络数据，主动发现入侵行为或非法行为

IPS入侵防御系统，使IDS和防火墙走向统一，检测+相应，实时地中止入侵行为

漏洞扫描系统：自动检测远程或本地主机系统再安全性方面地弱点和隐患的软件

漏洞：硬件、软件或策略下存在的安全缺陷，从而使得攻击者能在未授权情况下访问和控制系统

补丁：为堵塞安全漏洞，开发的与原软件结合或对原软件升级的程序

当前打补丁是堵漏洞最有效的方法