# 第六讲 网络隔离技术

## 测试点 6-1

**1. 集线器能作为网络隔离设备吗？请说明理由？**

不可以

集线器工作于物理层，每个端口相当于一个中继器，原理很简单，只对物理电信号放大中继，所有端口同属一个冲突域，主要用来延伸网络访问距离，扩展终端数量。交换机工作于数据链路层，它的每个端口相当于一个集线器，原理是根据数据帧头的 MAC 地址转发帧到合适的端口，每个端口是一个独立的冲突域。

**2. 简述 Vlan 划分的不同方式及特点**

①基于端口划分：简单，一次定义但灵活性差

②基于 MAC 地址划分：支持用户动态前一，但配置工作量大，执行效率低

③基于 IP 层划分：支持用户动态迁移，可按协议类型划分，但效率低，需要交换机支持

④基于 IP 组播划分：可通过路由器扩展，支持广域网，但效率低，不适合局域网

## 测试点 6-2

**1. 简述防火墙的典型技术分类与特点。**

① 分组过滤防火墙：基于源地址和目的地址、应用、协议类型以及每个 IP 包的端口来作出通过与否的判断。

特点：容易实现，费用少，对性能的影响不大，对流量的管理较出色。过滤规则表管理复杂，随着规则表规模加大出现漏洞的可能性也会增加；只对数据包头进行检查，没有身份验证机制，不能分辨用户；
不能进行应用层的深度检查，因此不能发现传输的恶意代码及攻击数据包；容易遭受源地址欺骗，源地址改为内部地址往往可以绕过包过滤防火墙。

② 应用代理防火墙：应用代理可以对数据包的数据区进行分析，并以此判断数据是否允许通过。

特点：可以提供更细致的日志；可以执行诸如身份验证等功能，同时能隐藏内部 IP 地址；能够进行应用级的过滤。例如，应用代理防火墙可以禁止 FTP 的“put”命令，从而保证用户不能往匿名 FTP 服务器上写入数据。工作在 OSI 模型最高层，因此开销较大；对每项服务必须使用专门设计的代理服务器；配置的方便性较差，对用户不透明。例如使用 HTTP 代理，需要用户配置自己的 IE，从而使之指向代理服务器。

③ 状态检测防火墙：状态检测可以结合前后数据包里的数据信息进行综合分析决定是否允许该包通过。

特点：比分组过滤技术安全性高，比应用代理技术效率高。
大多数状态检测防火墙的规则仍然与普通的包过滤相似。也有的状态检测防火墙对应用层的信息进行检查。例如可以通过检查内网发往外网的 FTP 协议数据包中是否有 put 命令来阻断内网用户向外网的服务器上传数据。但只检测特定字符串，不能实施代理功能，不能隐藏客户端地址。

④ 链路层代理（SOCKS）防火墙：链路层代理可以对客户端连接请求进行分

析，依据客户身份和请求此判是否否允许建立连接。

特点：可以支持不同的应用层协议（Sock4 支持 TCP，Socks5 支持 TCP/UDP）；支持用户级的认证，可针对具体会话进行安全管理。对客户端不透明；无法针对特定的应用协议进行安全管理。

**2. 简述防火墙的典型体系架构及特点。**

① 包过滤路由器模型

包过滤防火墙是用一个软件查看所流经的数据包的包头(header)，由此决定整个包的命运。它可能会决定丢弃（DROP）这个包，可能会接受（ACCEPT）这个包（让这个包通过），也可能执行其它更复杂的动作。

② 单宿主堡垒主机模型

防火墙由一台过滤路由器和一台堡垒主机构成，防火墙会强迫所有外部网络对内部网络的连接全部通过包过滤路由器和堡垒主机，堡垒主机就相当于是一个代理服务器，也就是说，包过滤路由器提供了网络层和传输层的安全，堡垒主机提供了应用层的安全，路由器的安全配置使得外网系统只能访问到堡垒主机，这个过程中，包过滤路由器是否正确配置和路由表是否收到安全保护是这个体系安全程度的关键，如果路由表被更改，指向堡垒主机的路由记录被删除，那么外部入侵者就可以直接连入内网。

③ 双宿主堡垒主机模型

这种防火墙主要有 2 个接口，分别连接着内部网络和外部网络，位于内外网络之间，阻止内外网络之间的 IP 通信，禁止一个网络将数据包发往另一个网络。两个网络之间的通信通过应用层数据共享和应用层代理服务的方法来实现，一般情况下都会在上面使用代理服务器。这种体系结构是存在漏洞的，比如双重宿主主机是整个网络的屏障，一旦被黑客攻破，那么内部网络就会对攻击者敞开大门，所以一般双重宿主机会要求有强大的身份验证系统来阻止外部非法登陆的可能性。

④ 子网屏蔽防火墙模型

这是最安全的防火墙体系结构，由两个包过滤路由器和一个堡垒主机构成，与屏蔽主机体系结构相比，它多了一层防护体系就是周边网络，周边网络相当与是一个防护层介于外网和内网之间，周边网络内经常放置堡垒主机和对外开放的应用服务器，比如 web 服务器。在屏蔽子网体系结构中，堡垒主机位于周边网络，为整个防御系统的核心，堡垒主机运行应用级网关，比如各种代理服务器程序，如果堡垒主机遭到了入侵，那么有内部路由器的保护，可以使得其不能进入内部网络

**3. 如果允许 IP 地址为 192.168.1.212 的内网主机访问外部网络的 Web 服务，但禁止该主机使用邮件服务（SMTP，POP3），请给出防火墙应当配置的规则**

①开启 web 服务器端口

先关闭所有的 80 端口

开启 ip 段 192.168.1.0/24 端的 80 口

```
# iptables -I INPUT -p tcp --dport 80 -j DROP
# iptables -I INPUT -s 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT
# iptables -I INPUT -s 192.168.1.212/24 -p tcp --dport 80 -j ACCEPT
```

②关闭邮件服务端口

先用 iptables 屏蔽全部 IP 连接 25 端口：

```
iptables -I FORWARD -p tcp --dport 25 -j DROP
```

iptables -I INPUT -p tcp --dport 25 -j DROP
iptables -I OUTPUT -p tcp --dport 25 -j DROP
只允许特定 ip 连接 25 端口：
iptables -I FORWARD -s 192.168.1.212 -p tcp --dport 25 -j ACCEPT
重新禁止此 ip 连接 25 端口，删除上述许可记录就可以了：
iptables -D FORWARD -s 192.168.1.212 -p tcp --dport 25 -j ACCEPT

## 测试点 6-3

1. **NAT 有几种转换方式？简述其工作原理与特点。**

①静态转换（Static NAT）：是指将内部网络的私有 IP 地址与公有 IP 地址进行一一对应的转换。

②动态转换（Dynamic NAT）：是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址是不确定的，是随机的。

③网络地址端口转换(NAPT)：是指改变外出数据包的源端口并进行端口转换，内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。

2. **VPN 可提供哪些基本安全功能？如果一个企业需要在分支机构间提供安全通信，以及让出差的员工访问内部资源，请给出一个基于 VPN 技术的解决方案**

功能：保证数据的完整性：接收到的数据必须与发送时的一致，要有抵抗不法分子篡改数据的能力；保证通道的机密性：提供强有力的加密手段，必须使偷听者不能破解拦截到的通道数据；提供动态密钥交换功能：提供密钥中心管理服务器，必须具备防止数据重演(Replay)的功能，保证通道不能被重演；提供安全防护措施和访问控制：要有抵抗黑客通过 VPN 通道攻击企业网络的能力，并且可以对 VPN 通道进行访问控制(Access Control)。

方案：解决方法是在内网中架设一台 VPN 服务器，VPN 服务器有两块网卡，一块连接内网，一块连接公网。外地员工在当地连上互联网后，通过互联网找到 VPN 服务器，然后利用 VPN 服务器作为跳板进入企业内网。为了保证数据安全，VPN 服务器和客户机之间的通讯数据都进行了加密处理。有了数据加密，就可以认为数据是在一条专用的数据链路上进行安全传输，就如同专门架设了一个专用网络一样。但实际上 VPN 使用的是互联网上的公用链路，因此只能称为虚拟专用网。即：VPN 实质上就是利用加密技术在公网上封装出一个数据通讯隧道。

## 测试点 6-4

1. **简述物理隔离的类型与工作模式。**

①双网双机：两台计算机共用一套外部设备，通过开关选择两套计算机系统。

②双硬盘物理隔离卡：通过增加一块隔离卡、一块硬盘，将硬盘接口通过添加的隔 离卡转接到主板，网卡也通过该卡引出两个网络接口。

③单硬盘物理隔离：增加一块隔离卡，引出两个网口，并对原有硬盘划分安全区、非安全区。（非严格的物理隔离）

④隔离网关（网闸）:内、外部主机是完全网络隔离的，支持文件、数据或信息的交换。