Homework3

吴承泽 SA23011083

Chapter5

1、简述防火墙的定义

防火墙的定义：防火墙是位于两个(或多个)网络之间执行访问控制的软件和硬件系统，它根据访问控制规则对进出网络的数据流进行过滤。

2、防火墙对数据流的拒绝和丢弃有何区别?

当数据流被拒绝时，防火墙要向发送者回复一条消息，用ICMP包告知数据源数据包被拒绝的原因，提示发送者该数据流已被拒绝。

当数据流被丢弃时，防火墙不会对这些数据包进行任何处理，也不会向发送者发送任何提示信息。丢弃数据包的做法加长了网络扫描所花费的时间，发送者只能等待回应直至通信超时。

3、简述数据包过滤器和状态防火墙。

数据包过滤器和状态防火墙工作在IP层（网络层），也用到了传输层的协议端口号等信息。根据访问控制策略的实现机制的不同，又可以分为静态包过滤和动态包过滤。静态包过滤防火墙也称为数据包过滤器（防火墙），动态包过滤防火墙也称为状态（检测）防火墙。

数据包过滤器通过数据包的头部信息来判断是接受还是拒绝数据包，它并不查看数据包载荷中的应用数据。这种防火墙检查流经它的每个数据包，根据数据包本身所带的信息决定它的去留，而不用参考其他数据包的内容。

状态防火墙会通过对流经的数据包的分析查找通信中的数据流，根据数据流的信息来帮助判断是否让数据包通行。数据流提供了数据包的上下文。状态防火墙有时还会检测一些常用协议的应用数据（虽然可以检测的数据量是有限的），通过这些数据来识别和跟踪相关的数据流。

4、与包过滤防火墙相比，应用代理防火墙有哪些特点?

优点如下:

- 由于应用代理避免了服务器和客户机之间的直接连接，在已有的安全模型中安全性较高。

由于工作于应用层，因此应用级网关防火墙的安全性取决于厂商的设计方案。应用级网关防火墙完全可以对服务(如HTTP、FTP等)的命令字过滤，也可以实现内容过滤，甚至可以进行病毒的过滤。

- 具有强大的认证功能。

由于应用级网关在应用层实现认证，因此它可以实现的认证方式比电路级网关要丰富得多。

- 具有超强的日志功能。

包过滤防火墙的日志仅能记录时间、地址、协议、端口，而应用级网关的日志要明确得多。例如，应用级网关可以记录用户通过HTTP访问了哪些网站页面、通过FTP上传或下载了什么文件、通过SMTP给谁发送了邮件，甚至邮件的主题、附件等信息，都可以作为日志的内容。

- 应用级网关防火墙的规则配置比较简单

由于应用代理必须针对不同的协议实现过滤，所以管理员在配置应用级网关时关注的重点就是应用服务，而不必像配置包过滤防火墙一样还要考虑规则顺序的问题。

缺点如下：

- 灵活性很差。

• 对每一种应用都需要设置一个代理。
• 在实际工作中，应用级网关防火墙中集成了电路级网关或包过滤防火墙，以满足人们对灵活性的需求。

- 配置烦琐，增加了管理员的工作量。

• 各种应用代理的设置方法不同。
• 当网络规模达到一定程度的时候，其工作量很大。

- 性能不高，有可能成为网络的瓶颈。

目前，应用级网关的性能依然远远无法满足大型网络的需求，一旦超负荷，就有可能发生停机，从而导致整个网络中断。

5、在防火墙的典型部署中，堡垒主机是一个组织机构网络安全的中心主机，它应该具备哪些主要特征?

- 堡垒主机硬件平台运行较为安全的操作系统，成为可信任的系统。
- 只有网络管理员认为必要的服务(代理和用户认证等)才会安装在堡垒主机上。
- 当允许一个用户访问代理服务时，堡垒主机可能会要求进行额外认证。另外，每一个代理服务都可能需要相应的鉴别机制。
- 每一个代理都只能支持标准应用服务命令集中的一个子集。
- 每一个代理只允许访问指定主机的通信，支持对通信进行详细的审计。
- 每一个代理模块都是一个为网络安全设计的一个很小的软件包。
- 代理之间相互独立。
- 代理通常无需进行磁盘访问，不需要读取初始配置文件。这使得入侵者很难在主机上安装Trojan horse、sniffers或其他危险的文件。
- 堡垒主机是一个组织机构网络安全的中心主机