HW4

✓作业

1. 简述防火墙的功能。
2. 防火墙对数据流的拒绝和丢弃有何区别?
3. 静态包过滤防火墙工作于OSI模型的哪一层，检测IP数据包的哪些部分?
4. 与包过滤防火墙相比，应用代理防火墙有哪些特点?
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?

T1

防火墙遵循的是一种允许或禁止业务来往的网络通信安全机制，也就是提供可控的过滤网络通信，只允许授权的通信。具体包括：

- 访问控制功能：作为最基本且重要的功能，通过禁止或允许特定用户访问特定资源，保护内部网络资源和数据，集中执行强制性信息安全策略，对网络数据进行不同深度监测以决定数据出入
- 内容控制功能：防止非法用户进入内部网络，禁止内网用户访问外网不安全服务（如恶意网站），可关闭存在安全漏洞的服务端口，在应用层过滤不良信息（如色情、暴力信息），抵御邮件炸弹、蠕虫病毒等攻击
- 日志功能：记录通过防火墙的信息内容和活动，为分析可能的攻击、防范风险提供重要信息，还能统计正常网络使用情况，助力优化网络资源使用
- 对网络攻击的检测和告警功能：当出现可疑动作时，进行适当报警，并提供网络是否受监测和攻击的详细信息
- 集中管理功能：针对不同网络情况和安全需求指定不同安全策略并集中实施，且易于管理，方便管理员操作
- 其他功能：如流量控制、网络地址转换（NAT）、虚拟专用网（VPN）等

T2

二者核心区别在于是否向数据流发送方反馈信息：

- 拒绝：防火墙会向发送方回复一条消息，通过 ICMP 包告知数据源数据包被拒绝的原因，让发送者明确知晓该数据流已被拒绝
- 丢弃：防火墙不对数据包进行任何处理，也不向发送者发送任何提示信息，发送者只能等待回应直至通信超时

T3

- 静态包过滤防火墙工作在 OSI 模型的网络层
- 静态包过滤防火墙仅检查当前数据包，判决是否允许通过仅依赖当前数据包内容，具体包括源 IP 地址、目的 IP 地址、应用或协议号、源端口号、目的端口号

T4

- 优点：
  - 安全性更高：避免服务器和客户机之间直接连接，可对服务（如 HTTP、FTP）的命令字过滤、实现内容过滤甚至病毒过滤，在已有安全模型中安全性较强
  - 认证功能强大：在应用层实现认证，可实现的认证方式比电路级网关更丰富
  - 日志功能超强：能详细记录用户网络行为，如通过 HTTP 访问的网站页面、FTP 上传下载的文件、SMTP 邮件的主题和附件等
  - 规则配置简单：针对不同协议实现过滤，管理员只需关注应用服务，无需像包过滤防火墙那样考虑规则顺序问题
- 缺点：

- 灵活性差：对每一种应用都需设置一个代理，通常需集成电路级网关或包过滤防火墙以满足灵活性需求
- 配置烦琐：各种应用代理设置方法不同，网络规模较大时，管理员工作量大
- 性能不高：性能远无法满足大型网络需求，超负荷时可能停机导致整个网络中断，易成为网络瓶颈

T5

堡垒主机是一种配置了较为全面的安全防范措施的网络上的计算机，它为网络间的通信提供了一个阻塞点，特征如下：

- 硬件平台运行较为安全的操作系统，成为可信任的系统
- 仅安装网络管理员认为必要的服务（如代理、用户认证等）
- 允许用户访问代理服务时，可能要求额外认证，且每个代理服务可能需要相应鉴别机制
- 每个代理仅支持标准应用服务命令集中的一个子集
- 每个代理只允许访问指定主机的通信，支持对通信进行详细审计
- 每个代理模块是为网络安全设计的小型软件包
- 各代理之间相互独立
- 需进行完善的防御，以保障其作为网络安全中心主机的安全性