Linux防火墙数据包捕获模块包过滤 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/145/2021_2022_Linux_E9_98_B2_E7_81_c103_145156.htm 一、防火墙概述 网络防火墙技术是一种用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络，访问内部网络资源，保护内部网络操作环境的特殊网 络互联设备。它对两个或多个网络之间传输的数据包按照一定的安全策略来实施检查，以决定网络之间的通信是否被允许，并监视网络运行状态。 根据防火墙所采用的技术不同，可以将它分为四种基本类型：包过滤型、网络地址转换—NAT、代理型和监测型。包过滤型产品是防火墙的初级产品，其技术依据 是网络中的分包传输技术。包过滤技术的优点是简单实用，实现成本较低，在应用环境比较简单的情况下，能够以较小的代价在一定程度上保证系统的安全。网络地 址转换是一种用于把IP地址转换成临时的、外部的、注册的IP地址标准。它允许具有私有IP地址的内部网络访问因特网。 代理型防火墙也可以被称为代理服务器，它的安全性要高于包过滤型产品，并已经开始向应用层发展。代理型防火墙的优点是安全性较高，可以针对应用层进行侦测 和扫描，对付基于应用层的侵入和病毒都十分有效。其缺点是对系统的整体性能有较大的影响，而且代理服务器必须针对客户机可能产生的所有应用类型逐一进行设 置，大大增加了系统管理的复杂性。 监测型防火墙是新一代的产品，能够对各层的数据进行主动的、实时的监测，在对这些数据加以分析的基础上，监测型防火墙能够有效地判断出各层中的非法侵入。 同时,这种检测型防火墙产品一般还

带有分布式探测器，这些探测器安置在各种应用服务器和其他网络的节点之中，不仅能够检测来自网络外部的攻击，同时对来自 内部的恶意破坏也有极强的防范作用。监测型防火墙在安全性上已超越了包过滤型和代理服务器型防火墙，但其实现成本较高。基于对系统成本与安全技术成本的综 合考虑，用户可以选择性地使用某些监测型技术。 二、基于Linux个人防火墙总体设计 本文研究的是防火墙系统的软硬件环境以及该防火墙的开发步骤和所要实现的功能，最后重点对该防火墙系统所需要的硬件和软件平台原理进行说明。尽管所有Linux系统都自带防火墙内核程序，但需要用户进行配置才能起到保护网络安全的目的。 1、防火墙系统总体设计 Linux系统下实现软件防火墙的设计与应用，实质上就是基于主机的网络安全解决方案。因此，我们完全可以选择合适的软硬件平台和相应的防火墙设计原理，自己开发出一套能够满足要求的防火墙系统。 归纳起来这里要实现的防火墙需要满足两大要求：第一，必须能够对主机提供安全保护，即对主机与局域网以外的主机进行数据传输时实施安全保护；第二，必须能够提供良好的人机接口界面，具有容易操作、容易管理的优点。 考虑到现有硬件设备的限制，在保证满足实验要求的环境下尽可能地简化了实验环境。因为该防火墙系统是基于主机设计的，故只需要一个联网的主机即可进行实 验。该系统是在Linux环境下用C语言实现包过滤型软件防火墙的设计与应用，采用Kylix开发工具进行界面设计和数据库连接。 基于Linux的个人防火墙系统主要具有以下功能：（1）全程动态包过滤 本防火墙要在Linux下实现全程动态包过滤功能，通过分析数据包的地址、协议、端口对任何网络连接当前

状态进行访问控制，从而提高系统的性能和安全性。（2）提供日志审计 本防火墙配备了日志记录系统和查询工具，用于记录系统管理、系统访问及针对安全策略的网络访问情况。（3）防火墙数据库的备份 本防火墙制作防火墙过滤数据库，并且管理员可以能动地对该数据库进行设置。