如何运用包过滤技术实现个人防火墙 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/287/2021_2022__E5_A6_82_E4_BD_95_E8_BF_90_E7_c98_287050.htm 摘要：本文通过介绍如何运用包过滤技术实现个人防火墙，深入的剖析了个人防火墙中所用到的各种技术，并重点介绍了通过微软的NDIS 中间驱动程序实现网络封装包，以及驱动程序与应用程序之间的通讯方法。 随着网络的迅速发展,各种各样的网络软件也随之出现,人们的生活和学习对网络的依赖也越来越多,但问题也接踵而来,网站被攻击,病毒泛滥,个人信息被窃取,使人们面临这样一个问题:网络是否安全? 而防火墙正是网络的保护伞,形形色色的防火墙很多,本文通过介绍包过滤技术实现个人防火墙,使大家对防火墙的知识有进一步的了解。 一、防火墙和包过滤技术简介 防火墙是一种用于在两个网络间进行访问控制的设备,防火墙系统防范的对象是来自被保护的网络的外部的对网络安全的威胁,它通过检测、限制、更改跨越防火墙的数据流,尽可能的实现对外部网络的安全保护。 而包过滤技术是防火墙最基本的实现技术,具有包过滤技术的装置是用来控制内、外网络数据流入和流出,包过滤技术的数据包大部分是基于TCP/IP协议平台的,对数据流的每个包进行检查,根据数据报的源地址、目的地址、TCP和IP的端口号,以及TCP的其他状态来确定是否允许数据包通过。 二、截获网络封装包 截获数据包是实现一个防火墙的第一步，截获数据包的方法有很多种,既可以在用户态下拦截网络数据包,又可以在核心状态下进行数据包截获。 在用户态下进行网络数据包拦截有以下几种方法：（1）Winsock Layered Service Provider (LSP)。（2

）Windows 2000 包过滤接口。（3）替换系统自带的WINSOCK动态连接库。很显然，在用户态下可以很简单的进行数据包拦截,但其最致命的缺点就是只能在Winsock层次上进行，而对于网络协议栈中底层协议的数据包无法进行处理。对于一些木马和病毒来说很容易避开这个层次的防火墙。因此大多数的个人防火墙选择利用网络驱动程序来实现的。例如用中间层驱动程序来截获数据包。中间层驱动介于协议层驱动和小端口驱动之间，它能够截获所有的网络数据包（如果是以太网那就是以太帧）。NDIS中间层驱动的应用很广泛，不仅仅是个人防火墙，还可以用来实现VPN，NAT，PPPOverEthernet以及VLan。中间层驱动的概念是在Window NT SP4之后才有的，因此对于Windows9x来说无法直接利用中间层驱动的功能。Windows DDK提供了两个着名的中间层驱动例子：Passthru以及Mux。开发人员可以在Passthru的基础上进行开发，Mux则实现了VLan功能。目前个人防火墙的产品还很少用到这种技术，主要的原因在于中间层驱动的安装过于复杂，尤其是在Windows NT下。Windows 2000下可以通过程序实现自动安装，但是如果驱动没有经过数字签名的话，系统会提示用户是否继续安装。中层层驱动功能强大，应该是今后个人防火墙技术的趋势所在，特别是一些附加功能的实现。图1.NDIS驱动程序模型 