Linux操作系统中的防火墙技术及其应用（1） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022_Linux_E6_93_8D_E4_BD_c103_144534.htm 概述 在众多的网络防火墙产品中，Linux操作系统上的防火墙软件特点显著。它们和Linux一样，具有强大的功能，大多是开放软件，不仅可免费使用而且源代码公开。这些优势是其他防火墙产品不可比拟的。选用这类软件确实是最低硬件需求的可靠、高效的解决方案。但用户最关心的还是安全系统的性能，有关部门根据网络安全调查和分析曾得出结论：网络上的安全漏洞和隐患绝大部分是因网络设置不当引起的。使用Linux平台上的这些优秀软件同样也存在这样的问题。要使系统安全高效地运行，安装人员和管理人员必须能够理解该软件产品的运行机制并能深入分析所采用的防火墙设置策略会不会被人利用。本文仅对Linux平台上的IP包过滤防火墙软件Ipchains进行探讨。 防火墙的基本模型 基于TCP/IP协议簇的Internet网际互联完全依赖于网络层以上的协议栈（网络层的IP协议、传输控制协议TCP/UDP协议和应用层协议）。考虑到网络防火墙是为了保持网络连通性而设立的安全机制，因此防火墙技术就是通过分析、控制网络以上层协议特征，实现被保护网络所需安全策略的技术。构建防火墙有三类基本模型：即应用代理网关、电路级网关(Circuit Level Gateway)和网络层防火墙。它们涉及的技术有应用代理技术和包过滤技术等。 应用代理网关允许内部网络上的用户通过防火墙非直接地访问Internet。它根据用户的请求代替用户与目的地进行连接。由于应用代理网关在应用层进行代理，所以它可以对应用协议进行控制，

而且还可以在应用级进行记录。它比网络级防火墙的安全措施更加严格，因为它能提供更详细的审计报告、跟踪用户和应用进程以及IP包的参数。然而，采用应用层防火墙对网络性能有较大影响。由于对任何用户的请求都要求应用代理进程为其提供应用服务，所以速度较慢，并且不如网络层防火墙那样透明以及维护不便等。在Linux上实现这种防火墙模型的软件有squid等。 电路级网关与应用代理网关类似，但进行的代理通常与应用无关。这样就失去了详尽记录和精确定义规则的能力。电路级网关是一台运行网关应用程序的设备，它只支持TCP/IP应用，使用TCP端口实现网络资源和用户应用程序之间的通信。它还要求客户端使用特殊软件才能为应用到应用的通信服务。SOCKS是Linux上实现这类防火墙模型的软件。 网络层的IP包过滤防火墙在IP包水平上工作。它根据在每个包中的源地址、目的地址和包类型等信息控制包的流动。更彻底的过滤过程是检查包中的源、目的端口号以及连接状态等信息。这种防火墙比较安全，但缺少足够的记录信息。它可以阻止外部网络访问被保护的内部网络，但不能记录谁访问了公开的系统，以及谁从内部网络访问Internet。在Linux内核中支持IP包过滤，所以不需要增加其他软件就可以构建包过滤防火墙，Ipchains软件包是Linux平台上一个功能强大的包过滤策略管理软件，用于设置可靠的防火墙系统。