Linux操作系统中的防火墙技术及其应用（2） 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_144531.htm Ipchains及IP伪装原理 在Linux系统上，支持包过滤的核心中有三个规则列表，这些列表称为防火墙链。三个链分别称为输入链、输出链和转发链。当一个包从Internet进入配置了防火墙的Linux主机，内核使用输入链决定该包的取舍。如果该包没有被丢弃，则内核继而调用转发链决定是否将包发送到某个出口，最后包要被发出前，内核通过输出链来做决定。 图1 Ipchains 流程图 一个链是一系列规则的列表。每个规则规定：如果包的包头与规则相匹配，那么对包进行相应的处理。如果该规则与包不匹配，则引入链中的下一条规则。最后，如果没有要引入的规则，内核根据内置策略决定如何做。在一个有安全意识的系统中，该规则通常告诉内核将包拒绝或丢弃。 通过适当配置IP过滤规则，即三条链的过滤策略，该防火墙可以控制输入的包来自信任的IP网段，也可配置为只对外开放指定的TCP/UDP端口号。这些策略可分别指定到防火墙主机的某固定接口设备如以太网卡、PPP连接等。除这三条链外，我们还可以配置用户自定义的规则链。在三条链的执行中可随时跳转到自定义链执行，完成后再回到主链，这使过滤规则可以相当灵活。 在防火墙链中有一些特殊的跳转目标值如下表所示： 在防火墙链中的IP伪装是一个比包过滤策略更加安全的解决方案，它同时解决了Internet中IP地址资源不足的问题。IP伪装是指当一台计算机访问Internet时能够将其IP地址伪装成其他地址的机制。如果连接到Internet上的一个Linux主机具有IP伪装功能

，那么与该Linux计算机无论是在同一个局域网上还是通过PPP连接的，尽管它们没有正式的IP地址，都可与Internet连接。这意味着可将一系列主机藏在一个网关系统之后来访问Internet，它们的访问在外界看来是不可见的。