Linux2.4内核中新增功能指南 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/143/2021_2022_Linux24_E5_86_c103_143975.htm 一 本文目的 本文主要是探讨 Linux 2.4 内核中的iptables 的各种新增功能和使用方法，如何有效地使用这些新增的功能设置企业的防火墙规则，举例说明了新增功能在企业中的应用。 二 操作环境 Redhat Linux 7.1自带的模块化内核，专线连接互联网，两块网卡的防火墙，内部网段为10.0.0.0/255.255.255.0, 防火墙外部网卡接口地址为1.2.3.4。 三 iptables与ipchains的不同之处 1. 内置规则的重新定义，简单化规则管理Linux 内核中内置的INPUT,OUTPUT,FORWARD规则在新的iptables中，任何一个包仅仅只在这三个规则中的任何一个上应用，或者被INPUT规则击中，或者被FORWARD规则或者OUTPUT规则击中，不象在ipchains中任何一个包如果是穿过这台防火墙总要同时击中三个规则。为了说明这种改变，请看下面的代码。 Incoming / Outgoing [Routing]-|FORWARD|----- [Decision] _____/ ^ | | v ____ ___ / / Linux防火墙 |OUTPUT| |INPUT| ____/ ___/ ^ | | -- Local Process ---- a. 首先，当一个包进来的时候，也就是从以太网卡进入防火墙，内核首先根据路由表决定包的目标。 b. 如果目标主机就是本机，则如上图直接进入INPUT链，再由本地正在等待该包的进程接收，结束。 c. 否则，如果从以太网卡进来的包目标不是本机，再看是否内核允许转发包(可用echo 1> /proc/sys/net/ipv4/ip_forward 打开转发功能)如果不允许转发，则包被DROP掉，如果允许转发，则送出本机，结束。这当中决不经过INPUT或者OUTPUT链，因为路由后的目标

不是本机，只被转发规则应用 d. 最后，该linux防火墙主机本身能够产生包，这种包只经过OUTPUT链出去。 注意： echo 1 > /proc/sys/net/ipv4/ip_forward 和 FORWARD 链的区别 前者的意思是是否打开内核的转发功能，后者是转发链规则只有内核打开转发功能，一个包才可能被送到转发链上去逐项检查规则。 如果一台防火墙没有打开前者的IP转发功能，则根防火墙相连的两边的网络是完全隔离的，如果是一端连到internet上，则只能通过代理防问internet,不可能通过IP伪装的方式防问。 这样，任何一个包只可能应用INPUT/OUTPUT/FORWARD中的一个规则，这种巨大的改进同时也简单化了防火墙规则管理。 2. iptables 是有状态的(stateful)。 有状态的意思是指如果一个包是对从防火墙原先发出去的包的回复，则自动不用检查任何规则就立即允许回复包进入并返回给请求者，这样我们不用设置许多规则定义就可实现应有的功能，在新的内核中使用这种有状态的能力是强烈地被推荐的，那么如何打开并使用这种功能呢？ 我们假定某公司有如下图所示的典型的internet连接方案：