详解用Linux Iptables构建防火墙实例 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/240/2021_2022__E8_AF_A6_E8_A7_A3_E7_94_A8L_c103_240639.htm 前言 用Linux iptables做防火墙具有很高的灵活性和稳定性(老兄我的防火墙自从做了之后还一直没有重启过)，但安装和设定起来比较麻烦，而且容易出错，本文旨在用为公司做防火墙的实例，让大家对Linux iptables做防火墙的安装和配置有一个大致的了解，希望能起到抛砖引玉的作用。 系统环境与网络规化 先了解一下公司的环境，公司利用2M ADSL专线上网，电信分配公用IP为218.4.62.12/29,网关为218.4.62.13 ,公司有电脑五十多台，使用DHCP，IP是192.168.2.XXX，DHCP Server建在iptables Server上；另公司有一电脑培训中心，使用指定固定IP，IP为192.168.20.XXX，为了更加快速的浏览网页，我们架了一台Squid Server，所有电脑通过Squid Server浏览网页，公司还另有一台WEB Server Mail Server Ftp Server。其IP为218.4.62.18。以上电脑和服务器要求全架在防火墙内。我们规化如下：Iptables Server上有三块网卡,eth0上加有二个IP，218.4.62.14和218.4.62.18。 其中218.4.62.14为共享上网，218.4.62.18为WEB Server专用，Eth1的IP为192……168.2.9；为了使培训中心PC与公司PC之间互不访问，所以直接从Iptables Server接到Switch-B,eth2接至Switch-A，连接培训中心PC和Squid Server, Web Server。 网络规化好了后，就开始装服务器了，Iptables Server 用的系统为Redhat Linux V7.3。在装服务器时要注意选上防火墙的安装包。 IPTABLES基础 Iptables语法： Iptables [-t TABLE] ACTION [PATTERN] [-j TARGET] TABLE:

有filter,nat,mangle；若无指定，预设为filter table. ACTION(对Chains执行的动作): ACTION 说明 -L Chain 显示Chain中的所有规则 -A Chain 对Chain新增一条规则 -D Chain 删除Chain中的一条规则 -I Chain 在Chain中插入一条规则 -R Chain 替换Chain中的某一条规则 -P Chain 对Chain设定的预设的Policy -F Chain 清除Chain中的所有规则 -N Chain 自订一个Chain -X 清除所有的自订Chain CHAINS: Iptables 有五条默认的Chains(规则链)，如下表： Chains 发生的时机 PREROUTING 数据包进入本机后，进入Route Table前 INPUT 数据包通过Route Table后，目地为本机 OUTPUT 由本机发出，进入Route Table前 FORWARD 通过Route Table后，目地不是本机时 POSTROUTING 通过Route Table后，送到网卡前 PATTERN(设定条件部份): 参数 内容 说明 -p Protocol 通讯协议，如tcp,udp,icmp,all等…… -s Address 指定的Source Address为Address -d Address 指定的Destination Address为Address -I Interface 指定数据包进入的网卡 -o Interface 指定数据包输出的网卡 -m Match 指定高级选项，如mac,state,multiport等…… TARGET(常用的动作)： TARGET 说明 ACCEPT 让这个数据包通过 DROP 丢弃数据包 RETURN 不作对比直接返回 QUEUE 传给User-Space的应用软件处理这个数据包 SNAT nat专用：转译来源地址 DNAT nat专用：转译目地地址 MASQUERADE nat专用：转译来源地址成为NIC的MAC REDIRECT nat专用：转送到本机的某个PORT 