**iptables防火墙**

防火墙概述

什么是防火墙（一道保护性屏障保护、隔离）

Linux包过滤防火墙

RHEL默认使用firewalld作为防火墙，但firewalld底层还是调用包过滤防火墙iptables

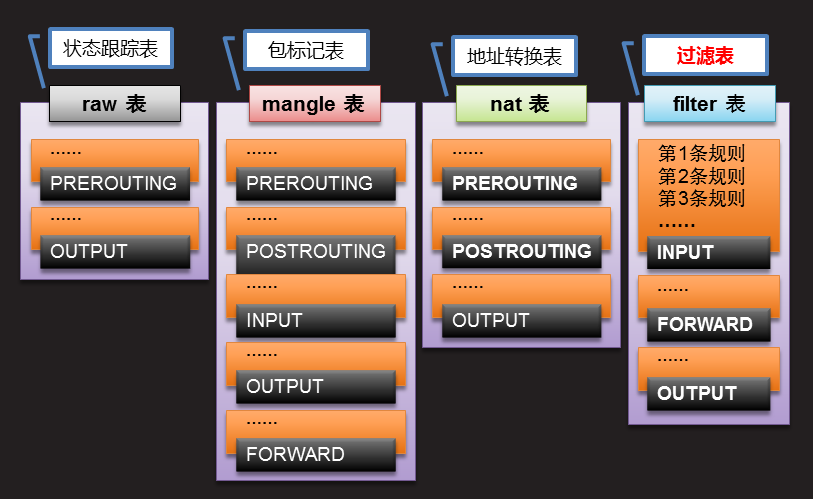
systemctl stop firewalld

systemctl disable firewalld

yum -y install iptables

systemctl start iptables

iptables的表、链结构（四表五链：四表：filter（过滤信息）、nat（地址转换）、mangle（对进来的数据包修改）、raw（跟踪数据包），五链：OUTPUT出站规则、INPUT入站规则、FORWORD转发规则、PREROUTING路由前规则、POSTROUTING路由后规则 地址转换时用到）



包过滤匹配规则

规则链内匹配顺序

顺序比对，匹配即停止（LOG除外）

若无任何匹配，则按该链的默认策略处理

iptables用法解析

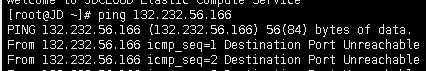
iptables基本用法

管理程序位置：/sbin/iptables

指令组成：iptables [-t 表名] 选项（增删改查） [链名] [条件] [-j 目标操作（怎么处理）]

iptables -t filter -l INPUT -p icmp -j REJECT





注意事项/整体规律

可以不指定表，默认为filter表

可以不指定链，默认为对应表的所有链

除非设置默认策略，否则必须指定匹配条件

选项/链名/目标操作用大写字母，其余都用小写

基本的目标操作

ACCEPT：允许通过/放行

DROP：直接丢弃

REJECT：拒绝通过，必要时会给出提示

LOG：记录日志，然后传给下一条规则（匹配即停止规律的唯一例外，会记录在/var/log/message）

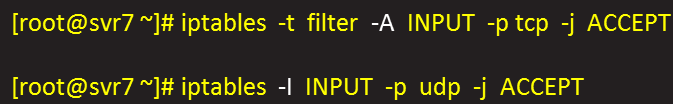
常用的管理选项

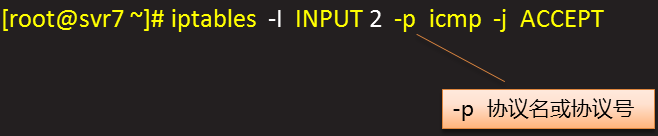
|  |  |  |
| --- | --- | --- |
| 类别 | 选项 | 用途 |
| 添加规则 | -A | 在链的末尾追加一条规则 |
| -I | 在链的开头（或指定序号）插入一条规则 |
| 查看规则 | -L | 列出所有的规则条目 |
| -n | 以数字形式显示地址、端口等信息 |
| --line-numbers | 查看规则时，显示规则的序号 |
| 删除规则 | -D | 删除链内指定序号（或内容）的一条规则 |
| -F | 清空所有规则 |
| 默认策略 | -P | 为指定的链设置默认规则 |

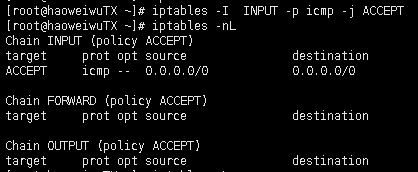
规则管理示例

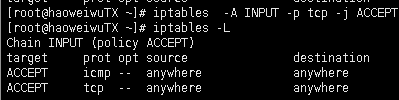
添加新规则

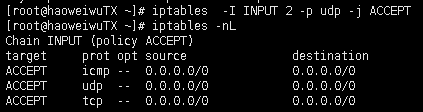
-A追加、-I插入





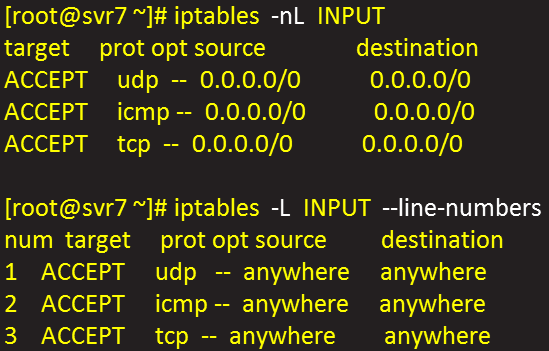


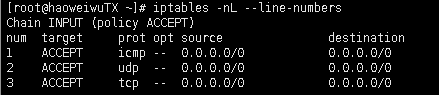




查看规则列表

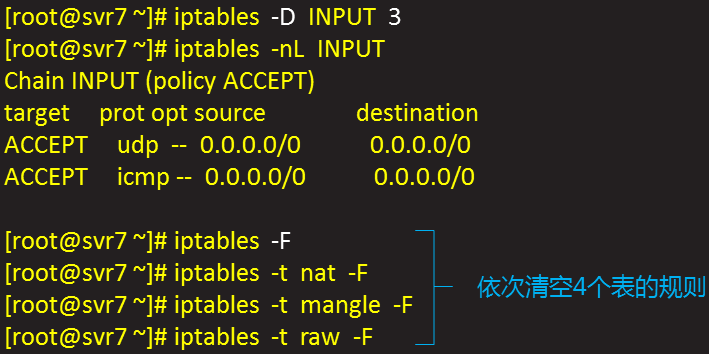
-L查看

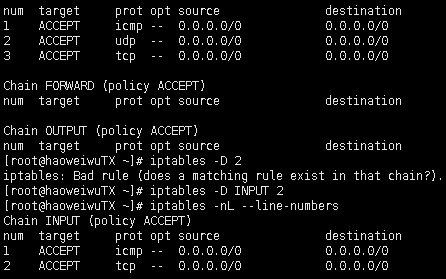


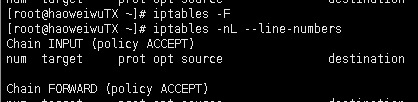


删除清空规则

-D删除、-F清空





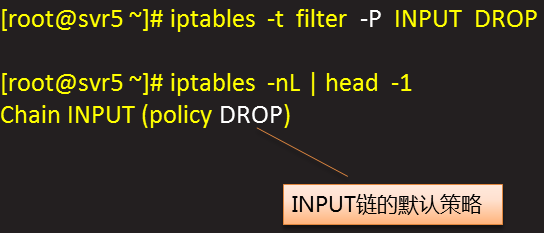


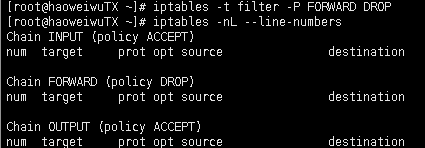
设置默认规则（只能写两个，分别是ACCEPT或DROP）

所有链的初始默认规则均视为ACCECPT

通过-P选项可重置默认规则

ACCEPT或DROP



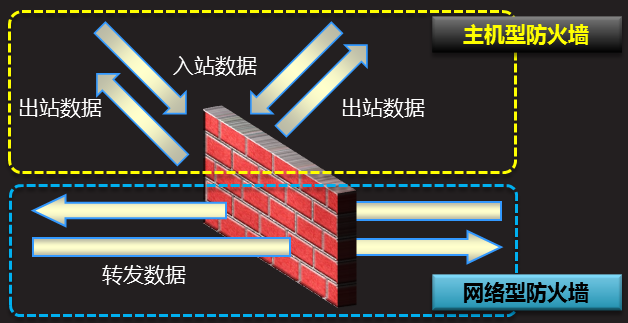


**filter表控制**

防护类型及条件

主机/网络型防护

根据保护对象（本机、其他主机）区分



开启内核的IP转发

作为网关、路由的必要条件

echo ‘net.ipv4.ip\_forward=1’ >> /etc/sysctl.conf（永久）

或者

echo 1 >/ proc/sys/net/ipv4/ip\_forward（临时）

基本的匹配条件

通用匹配

可直接使用，不依赖与其他条件或扩展

包括网络协议、IP地址、网络接口等条件

隐含匹配

要求以特定的协议匹配作为前提

包括端口、TCP标记、ICMP类型等条件

|  |  |  |
| --- | --- | --- |
| 类别 | 选项 | 用法 |
| 通用匹配 | 协议匹配 | -p 协议名 |
| 地址匹配 | -s 源地址、-d目的地址 |
| 接口匹配 | -i收数据的入站网卡、-o 发数据的出站网卡 |
| 隐含匹配 | 端口匹配 | --sport 源端口、--dport 目标端口 |
| ICMP类型匹配 | --icmp-type ICMP类型 |

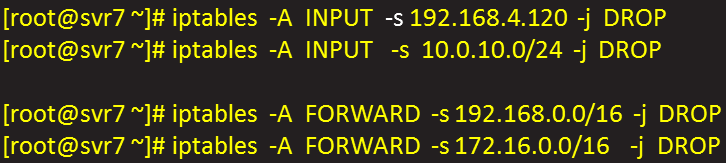
需要取反时，用!感叹号

过滤规则示例

封禁IP地址/网段

主机防护，针对入站访问的源地址

网络防护，针对准发访问的源地址



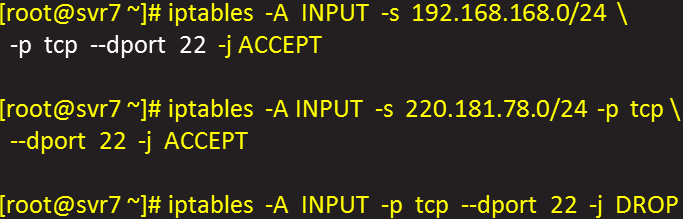
禁止223.11.26.106的一切访问

限制一个网段

网络防火墙

保护特定的网络服务

限制对指定服务端口的访问



设定入站规则，禁用tcp 80端口

禁止指定网卡访问80端口

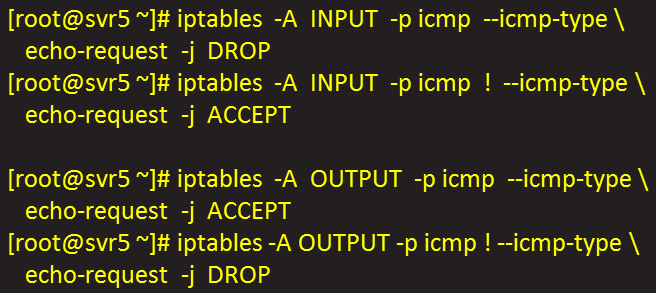
禁止访问172.27.0.4的80端口

禁止114.212.33.12远程登录

禁ping相关策略处理

允许本机ping其他主机

但是，禁止其他主机ping本机



禁止外网Ping自己，可以自己ping别人

**扩展匹配**

**Iptables 选项 链名称 -m 扩展模块 --具体扩展模块 -j 动作**

扩展条件的方法

前提条件：有对应的防火墙模块支持

基本用法：

-m 扩展模块 --扩展条件 条件值



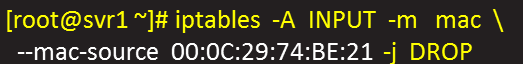
常见的扩展条件类型

|  |  |  |
| --- | --- | --- |
| 类别 | 选项 | 用法 |
| 扩展匹配 | 状态匹配 | -m stat --state 状态值 |
| MAC地址匹配 | -m mac --mac-source MAC地址 |
| 多端口匹配 | -m multiport --sports 源端口列表 |
| -m multiport --dports 目标端口列表 |
| IP范围匹配 | -m iprange --src-range IP1-IP2 |
| -m iprange --dst-range IP1-IP2 |

扩展案例

根据MAC地址封锁主机

适用于交换网络，针对源MAC地址，不管IP地址变成多少





多端口案例

一条规则开放多个端口

比如Web、FTP、SSH等





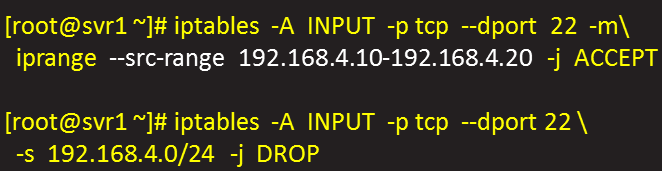
允许开放端口，连续的端口用冒号隔开，不连续的用逗号隔开

根据IP地址封锁主机

SSH登录的IP范围控制

允许从192.168.4.10-192.168.4.20登录

禁止从192.168.4.0/24网段其他的主机登录





**nat表典型应用**

NAT转换原理

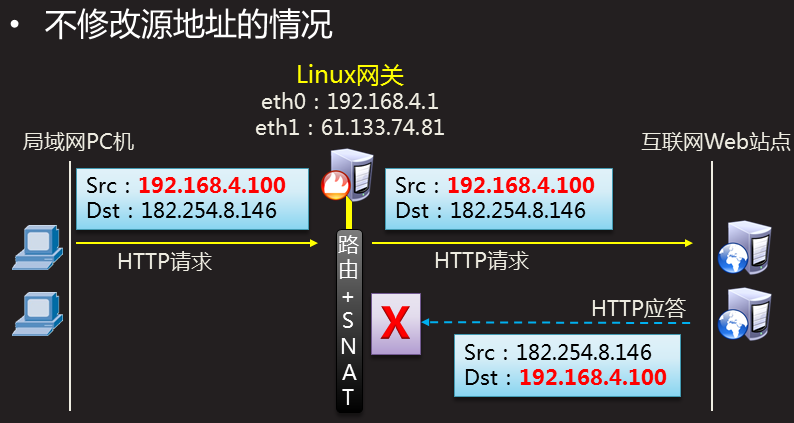
私有地址的局限性

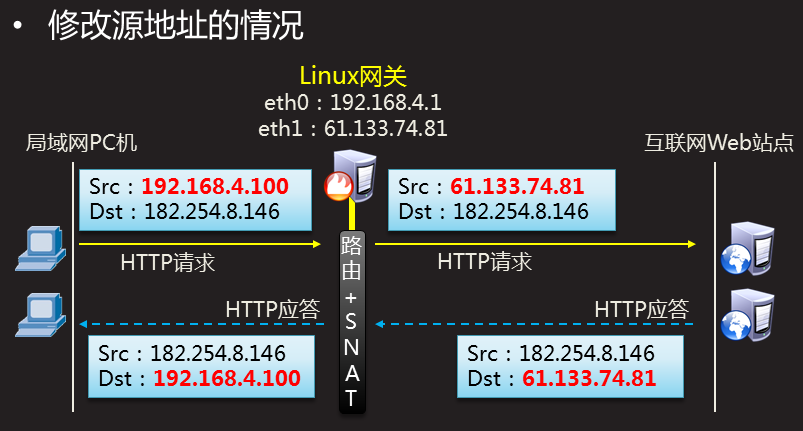
比如看网页、收邮件、....源地址为私有地址，服务器如何正确给出回应

SNAT源地址转换

修改数据包的源地址

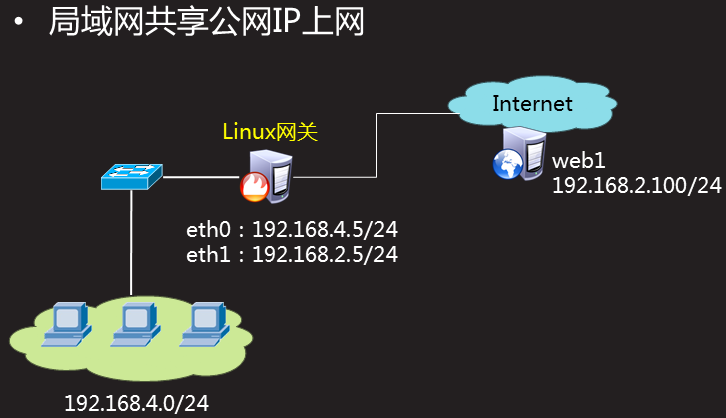
仅用于nat表的POSTROUTING链





SNAT策略应用

案例环境：局域网共享IP上网



前期准备：

局域网PC机正确设置IP地址/子网掩码

局域网PC机正确设置默认网关

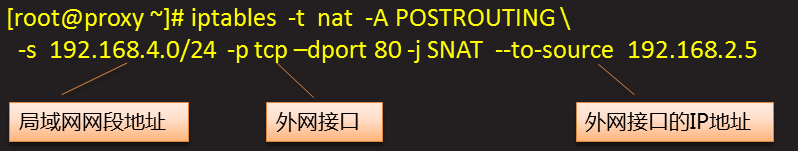
linux网关服务器开启IP路由转发

本实验中，不要为web服务器设置默认网关

配置SNAT共享上网

配置的关键策略

选择路由之后，针对来自局域网、即将从外网接口发出去的包，将源IP地址修改为网关的公网IP地址





验证访问结果

客户机上：PC机192.168.4.100能够访问外网的web服务器174.16.16.120

服务器上：查看web主机192.168.2.100的访问日志，来访者是linux的网关的外网IP地址192.168.2.5

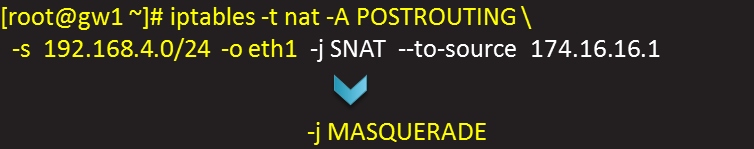
地址伪装策略

共享动态公网IP地址实现上网

主要针对外网接口的IP地址不固定的情况

将SNAT改为MASQUERADE（自动识别）即可

对于ADSL宽带拨号连接，网路接口可写ppp+



**service iptables save（保存规则，不保存重启就会丢掉）**