Iptables防火墙

关闭两项功能：

1、selinux（生产中也是关闭的）,ids入侵检测,md5指纹。

2、iptables（生产中看情况，内网关闭，外网打开）

大并发的情况，不能开iptables，影响性能，要使用硬件防火墙。

安全优化：

1、尽可能不给服务器配置外网IP。可以通过代理转发。

2、并发不是特别大情况再外网IP的环境，开启防火墙。

其他<http://edu.51cto.com/course/course_id-772.html>

学好iptables的基础：

1、OSI7层模型以及不同层对应哪些协议?

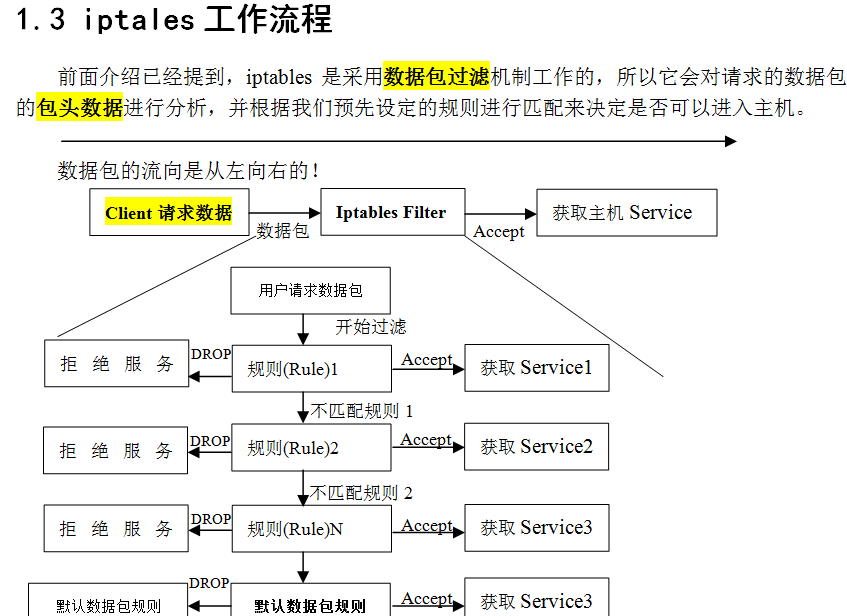
2、TCP/IP三次握手，四次断开的过程，TCP HEADER。

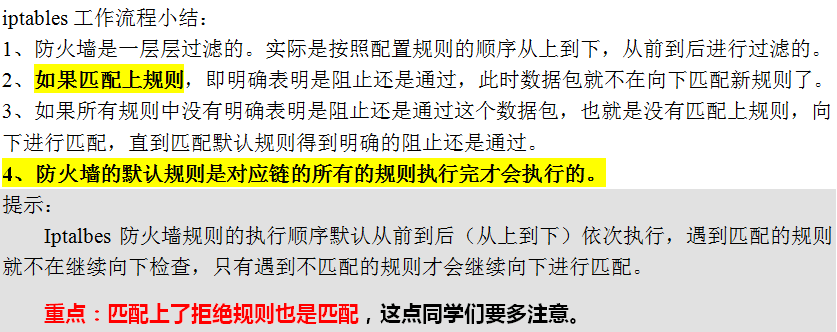
3、常用的服务端口要了如指掌。

iptables是基于包过滤的防火墙。

iptables+zebra+squid做网关服务器

iptables主要做osi七层模型的2、3、4层。





容器   包含和被包含的关系

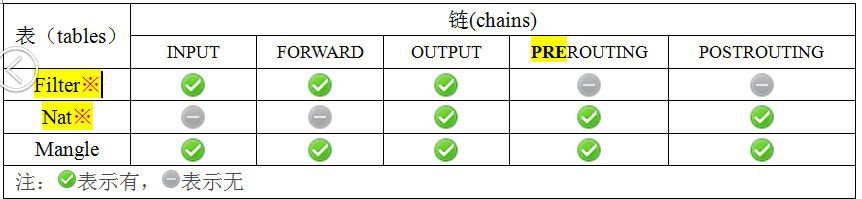
iptables是表的容器，iptables包含4张表，表示链的容器，每个表当中都包含若干个链。

链是规则的容器，真正的过滤规则是属于链里面的

四表：filter,nat,mangle，RAW

表 table、链 chain、规则 policy

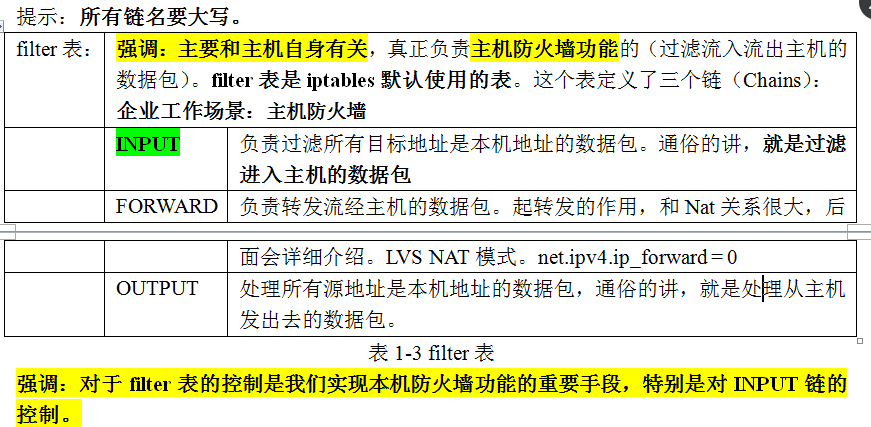
五链：

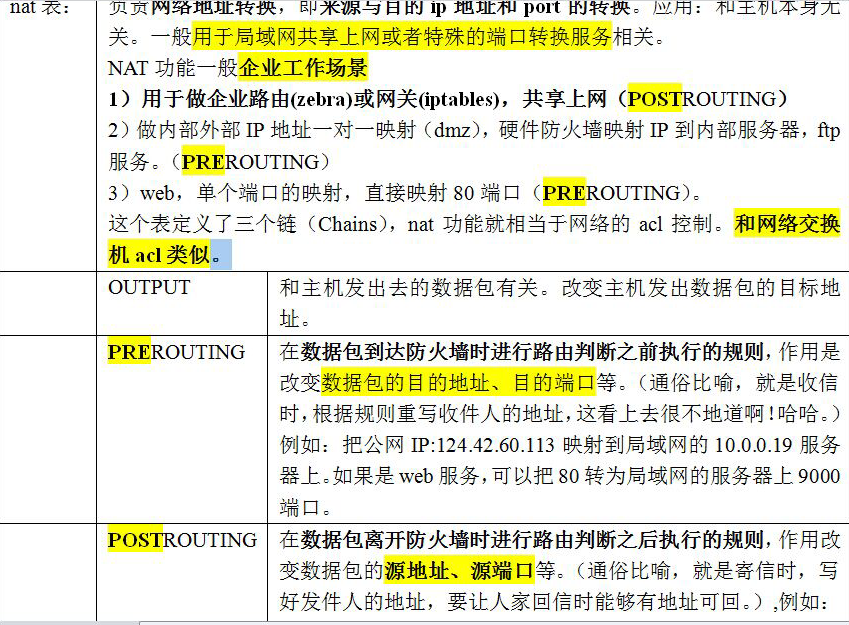


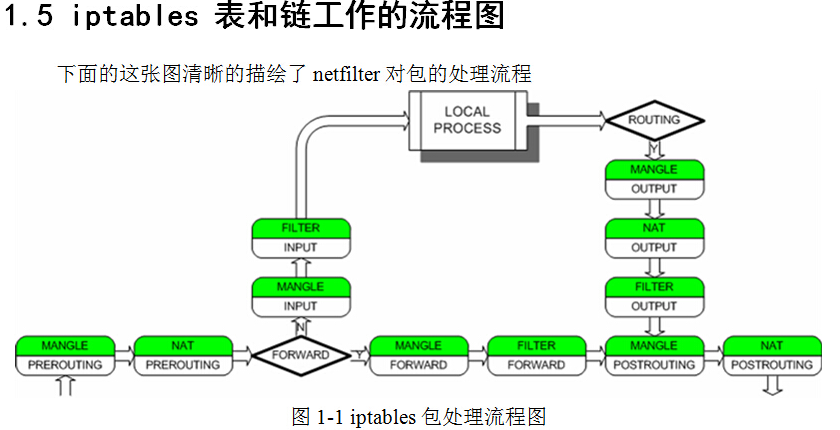
filter表：强调：主要和主机自身有关，真正负责主机防火墙功能的。filter是iptables的默认表。

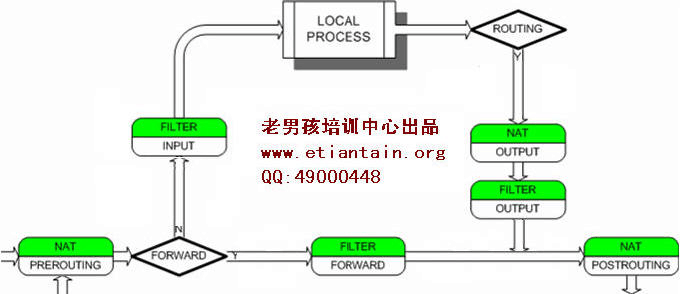
Filter表 真正的防火墙功能

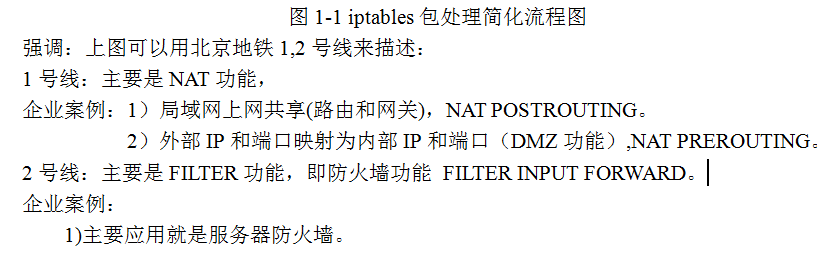
NAT表 负责数据包改写，主要功能：网关、共享上网、IP和端口映射。









****

modprobe ip\_tables  
modprobe iptable\_filter  
modprobe iptable\_nat  
modprobe ip\_conntrack  
modprobe ip\_conntrack\_ftp  
modprobe ip\_nat\_ftp  
modprobe ipt\_state

[root@db02 ~]# lsmod |egrep "nat|filter"  
nf\_nat\_ftp              3443  0   
nf\_conntrack\_ftp       11953  1 nf\_nat\_ftp  
iptable\_nat             5923  0   
nf\_nat                 22676  2 nf\_nat\_ftp,iptable\_nat  
nf\_conntrack\_ipv4       9154  5 iptable\_nat,nf\_nat  
nf\_conntrack           79206  6 nf\_nat\_ftp,nf\_conntrack\_ftp,iptable\_nat,nf\_nat,nf\_conntrack\_ipv4,xt\_state  
iptable\_filter          2793  1   
ip\_tables              17831  2 iptable\_nat,iptable\_filter

默认规则都是允许的。

[root@amoeba ~]# iptables -F

[root@amoeba ~]# iptables -nL

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

[root@amoeba ~]#

[root@db02 ~]# iptables -F   
[root@db02 ~]# iptables -X  
[root@db02 ~]# iptables -Z

iptables -A INPUT -p tcp --dport 52113 -j DROP

等价于

iptables -t filter -A INPUT -p tcp --dport 52113 -j DROP

3. --jump        -j target  
   target for rule (may load target extension)  
基本的处理行为：ACCEPT（接受）、DROP（丢弃）、REJECT（拒绝,一般不使用此项）

拒绝一般使用-I插入到第一个。-A向后插入。

使用-I和-A的顺序，防火墙的过滤根据规则顺序的。

-A是添加规则到指定链的结尾，最后一条。

-I是添加规则到指定链的开头，第一条。

查看规则列表及排序。

iptables -nL --line-number

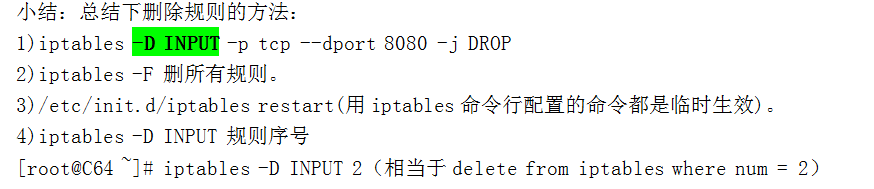
iptables -t filter -I INPUT 2 -p tcp --dport 800 -j DROP

删除单个规则：

iptables -t filter -D INPUT -p tcp --dport 800 -j DROP

删除单个规则：

iptables -t filter -D INPUT 2



封单个ip：

[root@db02 ~]# iptables -I INPUT -s 10.0.0.8 -p all  -j DROP 

封整个网段：

[root@db02 ~]# iptables -I INPUT -s 10.0.0.0/24 -p all  -j DROP

还可以用非(!)

iptables 参数：

-F 清空所有规则

-X 清空自定义规则

-Z 清空计数器

-P 清空默认规则

-A指定链添加规则到结尾

-I 指定链插入规则到开头

-D 指定链删除规则

-j 行为 ACCEPT（接受）、DROP（丢弃）、REJECT（拒绝,一般不使用此项）

-t 指定表

-line-number 查看规则序号

-n数字显示

-L 列表

-p 指定协议

--dport目的端口

可以匹配端口范围：--dport 20:80（端口20到端口80）

-m multiport --dport 21,22,23,24 匹配目标端口范围

-sport 源端口

-s 源地址或网段

-d 目的地址或网段

! 非

-I eth0 进入端口（input）

-o eth0 外出端口 （output）

iptables -A INPUT -p icmp --icmp-type 8 -j DROP

iptables -A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT

匹配网络状态  
-m state --state  
    NEW：已经或将启动新的连接  
    ESTABLISHED：已建立的连接  
    RELATED：正在启动的新连接  
INVALID：非法或无法识别的

●7.允许关联的状态包通过(web服务不要使用FTP服务)

#others RELATED ftp协议

#允许关联的状态包

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

限制指定时间包的允许通过数量及并发数  
-m limit --limit n/{second/minute/hour}:

--limit-burst [n]：

在同一时间内允许通过的请求"n"为数字,不指定默认为5

老师记录：

-F 清空所有规则

-X 清空自定义规则

-Z 清空计数器

-A 指定链上添加规则，结尾

-I 指定链上插入规则，开头

-D 指定链上删除规则

-j 行为ACCEPT（接受）、DROP（丢弃）、REJECT（拒绝）

-t 指定表

--line-number 查看规则行号

-n 数字显示

-L list列表查看

-p 指定协议-p (all,tcp,udp,icmp)。默认all

--dport 80 目的端口

--dport 20:80 匹配目标端口范围

-m multiport --dport 21,22,23,24 匹配目标端口范围

--sport 53 源端口

--sport 20:80 匹配源端口范围

-s 源ip地址或网段

-d 目的地址或网段

! 非，例如 ! -s

-i eth0 进入端口(INPUT)

-o eth0 外出端口(OUTPUT)

匹配ICMP类型

-p icmp --icmp-type 8 -j DROP

-p icmp -m icmp --icmp-type any -j ACCEPT

匹配网络状态

-m state --state

NEW：已经或将启动新的连接

ESTABLISHED：已建立的连接

RELATED：正在启动的新连接

INVALID：非法或无法识别的

●7.允许关联的状态包通过(web服务不要使用FTP服务)

#ftp协议

#允许关联的状态包

-m state --state ESTABLISHED,RELATED -j ACCEPT

-m state --state ESTABLISHED,RELATED -j ACCEPT

手动执行iptables命令配置企业生产环境下的防火墙

[root@db02 ~]# iptables -A INPUT -p tcp -s 10.0.0.0/24 -j ACCEPT

[root@db02 ~]# iptables -A OUTPUT -o lo -j ACCEPT

[root@db02 ~]# iptables -P OUTPUT ACCEPT   
[root@db02 ~]# iptables -P INPUT DROP  
[root@db02 ~]# iptables -P FORWARD DROP

[root@db02 ~]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

[root@db02 ~]# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

[root@db02 ~]# iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

[root@db02 ~]# iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT

iptables -A INPUT -s 124.43.62.96/27 -p all -j ACCEPT  ç办公室固定IP段。  
iptables -A INPUT -s 192.168.1.0/24 -p all -j ACCEPT   çIDC机房的内网网段。  
iptables -A INPUT -s 10.0.0.0/24 -p all -j ACCEPT      ß其他机房的内网网段。  
iptables -A INPUT -s 203.83.24.0/24 -p all -j ACCEPT   ßIDC机房的外网网段  
iptables -A INPUT -s 201.82.34.0/24 -p all -j ACCEPT   ß其它IDC机房的外网网段

防火墙规则保存方法：

第一种：

[root@db02 ~]# /etc/init.d/iptables save  
iptables：将防火墙规则保存到 /etc/sysconfig/iptables：     [确定]

第二种：  
[root@db02 ~]# iptables-save >/etc/sysconfig/iptables

平滑生效：

[root@db02 ~]# /etc/init.d/iptables reload  
iptables: Trying to reload firewall rules:                 [确定]

方法1：适合于有固定外网地址的：

iptables -t nat -A POSTROUTING -s 1172.161.0/24 -o eth1 -j SNAT --to-source 10.0.0.21

方法2：适合变化外网地址（ADSL）：  
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE

网关Ip:eth0:124.42.60.109 eth1:10.0.0.254

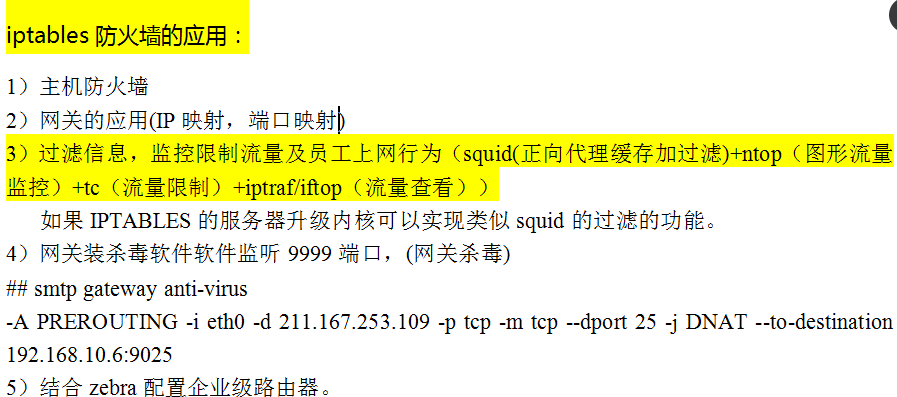
首先在路由网关上绑定124.42.34.112，可以是别名的方式。

-A PREROUTING -d 124.42.34.112 -j DNAT --to-destination 10.0.0.8

-A POSTROUTING -s 10.0.0.8 -o eth0 -j SNAT --to-source 124.42.34.112

-A POSTROUTING -s 10.0.0.0/255.255.240.0 -d 124.42.34.112 -j SNAT --to-source 10.0.0.254

4.5 跨不同网段IP服务器通信问题  
(1)生产环境大于254台机器网段划分及路由解决方案详解01   
C:\Users\ADMINI~1\AppData\Local\Temp\8LDO48C$8@[GWU0353$FOVS.pnghttp://v.youku.com/v\_show/id\_XNTAyMjAwMzI0.html   
  
(2) linux route命令深入浅出与实战案例精讲  
C:\Users\Administrator\AppData\Roaming\Tencent\QQ\Temp\%W@GJ$ACOF(TYDYECOKVDYB.pnghttp://oldboy.blog.51cto.com/2561410/1119453  
必看3遍以上。



映射多个外网IP上网

iptables -t nat -A POSTROUTING -s 10.0.1.0/255.255.240.0 -o eth0 -j SNAT --to-source 124.42.60.11-124.42.60.16

C64：

net.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 180

net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120

net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60

net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120

#5、dmesg里面显示 ip\_conntrack: table full, dropping packet.的错误提示.如何解决

Linux上配置zebra路由:  
client(config)#int eth0  
client(config-if)#ip add 10.1.34.81 255.255.255.0  
client(config-if)#int eth1  
client(config-if)#ip add 110.233.24.96 255.255.255.224  
client(config)#ip route 0.0.0.0 0.0.0.0 10.1.32.1  
client(config)#ip route 110.233.24.96/27 eth1

映射多个外网IP上网  
iptables -t nat -A POSTROUTING -s 10.0.1.0/255.255.240.0 -o eth0 -j SNAT --to-source 124.42.60.11-124.42.60.16

例：企业级路由器的配置  
路由连接地址为10.1.34.81/24  
默认路由：10.1.34.1  
分配的公网ip地址：110.233.24.96/27 255.255.255.224  
购买企业级路由器：

iptables -F 清除所有规则，不会处理默认的规则

iptables -X 删除用户自定义的链

iptables -Z 链的计数器清零。

iptables -t 指定表

iptables -A 添加规则

iptables -p 协议

iptables -dport 目的端口

iptables -j jump 处理的行为（ACCEPT（接受）、DROP（丢弃）、REJECT（拒绝） ）

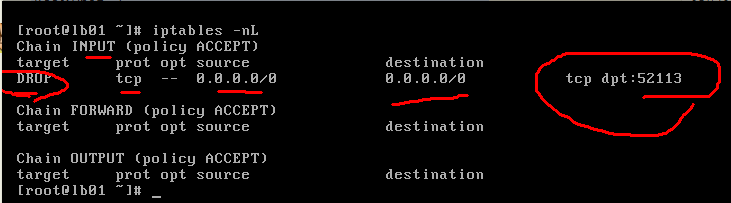
禁止Windows连接虚拟机的命令：

netstat -lntup|grep ssh

0 0.0.0.0:22 0.0.0.0:\* LISTEN 1557/sshd

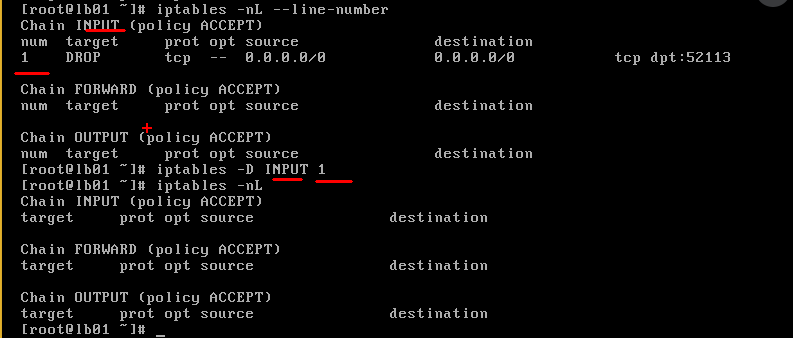
0 :::22 :::\* LISTEN 1557/sshd

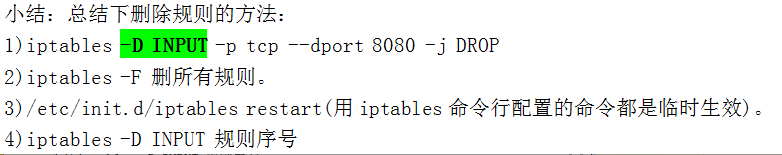
iptables -t filter -A INPUT -p tcp --dport 22 -j DROP



解决方法：

1、 iptables -F

2、 



centos5.8版本：  
iptables -t filter -A INPUT -i eth0 -s ! 10.0.0.115 -j DROP  
iptables -t filter -A INPUT -i eth0 -s ! 10.0.0.115 -j ACCEPT  
centos6.4高版本：  
[root@C64-GW ~]# iptables -t filter -A INPUT -i eth0 -s ! 10.0.0.115 -j DROP  
Using intrapositioned negation (`--option ! this`) is deprecated in favor of extrapositioned (`! --option this`).  
解决方案：iptables -t filter -A INPUT -i eth0 ! -s 10.0.0.115 -j DROP

多条件命令：

[root@lb01 ~]# iptables -A INPUT -p tcp --dport 52113 -i eth0 ! -s 10.0.0.0/24 -j DROP

封端口的命令：

iptables -A INPUT -p tcp  --dport 3306 -j DROP

匹配指定协议：

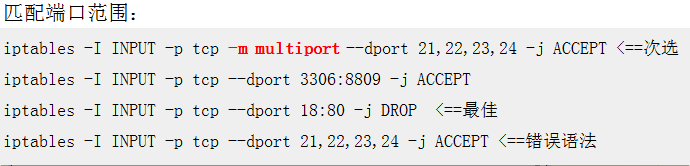
iptables -A INPUT -p tcp  
iptables -A INPUT -p udp

匹配主机源IP，目的IP

匹配单一端口  
iptables -A INPUT -p tcp --sport 53 #源端口  
iptables -A INPUT -p udp --dport 53 #目的端口

匹配端口范围：

iptables -I INPUT -p tcp --dport 18:80 -j DROP



匹配指定的网络接口

iptables -A INPUT -i eth0

iptables -A FORWARD -o eth0

匹配ICMP类型

iptables -A INPUT -p icmp --icmp-type 8  
例：iptables -A INPUT -p icmp --icmp-type 8 -j DROP  
iptables -A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT  
iptables -A FORWARD -s 192.168.1.0/24 -p icmp -m icmp --icmp-type any -j ACCEPT

匹配网路状态

-m state --state

NEW：已经或将启动新的连接

ESTABLISHED：已建立的连接

RELATED：正在启动的新连接

INVALID：非法或无法识别的

允许关联的状态包通过(web服务不要使用FTP服务)

#others RELATED ftp协议  
#允许关联的状态包  
iptables -A INPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT  
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

限制指定时间包的允许通过数量及并发数

-m limit --limit n/{second/minute/hour}:

防火墙案例：

生产环境配置主机防火墙的两种模式

逛公园及看电影两种模式

逛公园：默认随便进出，对非法的分子进行拒绝，企业应用：企业配置上网网关路由。

看电影：默认没票进不去。花钱买票才能看电影，企业应用：服务器主机防火墙。

很显然：第三种更严格，更安全。

逛公园及看电影两种模式本质是就是防火墙的默认规则是允许还是拒绝。

我们就以电影院看电影模式来和大家一起手动部署一个安全的防火墙。

iptables –F

iptables -X

iptables -Z

iptables -A INPUT -p tcp -s 10.1.0.0/24 -j ACCEPT

iptables -A INPUT -i lo -j ACCEPT ##输入接口

iptables -A OUTPUT -o lo -j ACCEPT

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

iptables -A INPUT -s 124.43.62.96/27 -p all -j ACCEPT

iptables -A INPUT -s 192.168.1.0/27 -p all -j ACCEPT

iptables -A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT

iptables -A INPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT  
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

保存配置文件：

法1：

[root@lb01 ~]# /etc/init.d/iptables save  
iptables：将防火墙规则保存到 /etc/sysconfig/iptables：     [确定]  
[root@lb01 ~]# cat  /etc/sysconfig/iptables  
# Generated by iptables-save v1.4.7 on Fri Feb 26 15:16:18 2016  
\*nat  
:PREROUTING ACCEPT [80:11494]  
:POSTROUTING ACCEPT [3048:184386]  
:OUTPUT ACCEPT [3048:184386]  
COMMIT  
# Completed on Fri Feb 26 15:16:18 2016  
# Generated by iptables-save v1.4.7 on Fri Feb 26 15:16:18 2016  
\*filter  
:INPUT DROP [0:0]  
:FORWARD DROP [0:0]  
:OUTPUT ACCEPT [168:7524]  
-A INPUT -s 10.0.0.0/24 -p tcp -j ACCEPT   
-A INPUT -p tcp -m tcp --dport 52113 -j ACCEPT   
-A INPUT -i lo -j ACCEPT   
-A INPUT -s 124.43.62.96/27 -j ACCEPT   
-A INPUT -s 192.168.1.0/24 -j ACCEPT   
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT   
-A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT   
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT   
-A OUTPUT -o lo -j ACCEPT   
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT   
COMMIT  
# Completed on Fri Feb 26 15:16:18 2016

法2：

iptables-save >/etc/sysconfig/iptables

实际操作：

[root@lb01 ~]# iptables -F  
[root@lb01 ~]# iptables -X  
[root@lb01 ~]# iptables -Z  
[root@lb01 ~]# iptables -nL  
Chain INPUT (policy ACCEPT)  
target     prot opt source               destination           
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source               destination           
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source               destination           
[root@lb01 ~]# iptables -A INPUT -p tcp -s 10.0.0.0/24 -j ACCEPT  
[root@lb01 ~]# iptables -A INPUT -p tcp --dport 52113 -j ACCEPT           
[root@lb01 ~]# iptables -nL  
Chain INPUT (policy ACCEPT)  
target     prot opt source               destination           
ACCEPT     tcp  --  10.0.0.0/24          0.0.0.0/0             
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:52113   
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source               destination           
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source               destination

如何在工作中维护防火墙：

配置内部服务器上网  
环境准备：  
B  
两个网卡  
Eth0 10.0.0.7  
Eth2 172.16.1.7  
C  
一块内网卡  
172.16.1.8  
  
B操作   
1. 清除所有规则  
2. 设置内网转发，生效   
3. 添加模块  
modprobe ip\_tables  
modprobe iptable\_filter  
modprobe iptable\_nat  
modprobe ip\_conntrack  
modprobe ip\_conntrack\_ftp  
modprobe ip\_nat\_ftp  
modprobe ipt\_state  
  
  
C操作  
1. route –n  
2. route –n del default gw 172.16.1.\*  \*代表存在的IP  
3. 添加 route –n add fefault gw 172.16.1.7  
4. 再route –n   
5. 关闭外网  
A远程连接C  
A执行iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j SNAT --to 10.0.0.7  
B ping 10.0.0.2

iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -o eth2 -j MASQUERADE 适用于外网IP不固定情况。

iptables -t nat -F 清除nat规则

iptable -t nat -nL 查看nat规则

为什么用POSTROUTING？

企业共享上网：

1、 办公网共享上网（网关要有外网IP，否则需要用路由（zebra））。

2、 IDC内网机器上网。

企业上网到底需要不需要Linux网关？

解答：

1） 如果有企业里有企业级路由器的情况下，可以不需要上网网关。使用网关只是解决路由器无法解决的需求（例如：上网行为，IP及端口的映射，网关杀毒）。

2） IDC机房，大厦有固定外网IP的宽带，直接用网关解决上网及控制问题。

iptables常用企业案例：

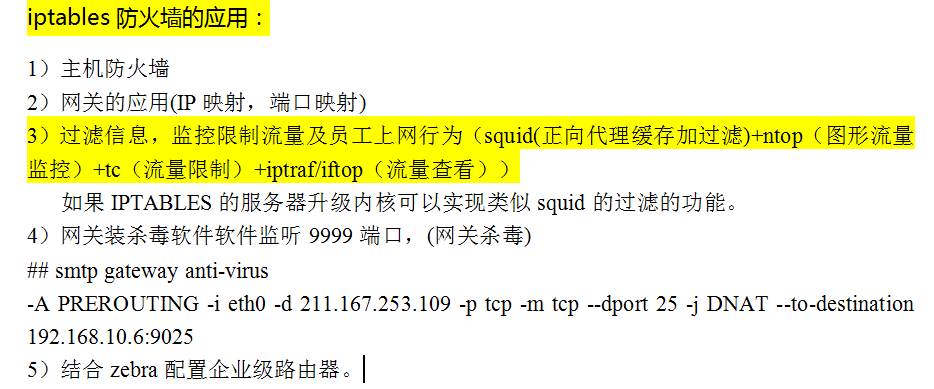
1、 Linux主机防火墙（表：FILTET 链：INPUT）

2、 局域网机器共享上网（表：NAT 链：POSTROUTING）

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j SNAT --to-source 10.0.0.7

3、 外部地址和端口，映射为内部地址和端口（表：NAT 链：PREROUTING）





映射多个外网IP上网  
iptables -t nat -A POSTROUTING -s 10.0.1.0/255.255.240.0 -o eth0 -j SNAT --to-source 124.42.60.11-124.42.60.16

#5、dmesg里面显示 ip\_conntrack: table full, dropping packet.的错误提示.如何解决。

cat /proc/sys/net/ipv4/netfilter/ip\_conntrack\_tcp\_timeout\_close\_wait

#5、dmesg里面显示 ip\_conntrack: table full, dropping packet.的错误提示.如何解决。  
#以下参数是对iptables防火墙的优化，防火墙不开会提示，可以忽略不理。  
c58:  
net.ipv4.ip\_conntrack\_max = 25000000  
net.ipv4.netfilter.ip\_conntrack\_max=25000000  
net.ipv4.netfilter.ip\_conntrack\_tcp\_timeout\_established=180  
net.ipv4.netfilter.ip\_conntrack\_tcp\_timeout\_time\_wait=120  
net.ipv4.netfilter.ip\_conntrack\_tcp\_timeout\_close\_wait=60  
net.ipv4.netfilter.ip\_conntrack\_tcp\_timeout\_fin\_wait=120  
################################################################  
C64：  
net.nf\_conntrack\_max = 25000000  
net.netfilter.nf\_conntrack\_max = 25000000  
net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 180  
net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120  
net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60  
net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120

本系列博文完整内容共5篇：  
第一篇：详解linux netstat输出的网络连接状态信息  
http://oldboy.blog.51cto.com/2561410/1184139  
第二篇：庖丁解牛获取连接状态数的awk数组命令  
http://oldboy.blog.51cto.com/blog/2561410/1184165  
第三篇：awk数组命令经典生产实战应用拓展  
http://oldboy.blog.51cto.com/blog/2561410/1184177  
第四篇：老男孩培训第八节课前awk考试题案例(门户面试题解答)   
http://oldboy.blog.51cto.com/2561410/1184206  
第五篇：linux生产服务器有关网络状态的优化措施（告一段落）   
http://oldboy.blog.51cto.com/2561410/1184228

4.5 跨不同网段IP服务器通信问题  
(1)生产环境大于254台机器网段划分及路由解决方案详解01   
http://v.youku.com/v\_show/id\_XNTAyMjAwMzI0.html   
  
  
(2) linux route命令深入浅出与实战案例精讲  
http://oldboy.blog.51cto.com/2561410/1119453  
http://oldboy.blog.51cto.com/2561410/974194  
必看3遍以上。