三毛仔

昵称：三毛仔
园龄：2年5个月
粉丝：7
关注：3
+加关注

< 2019年2月 >

日	一	二	三	四	五	六
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

搜索
找找看
谷歌搜索

常用链接
我的随笔
我的评论
我的参与
最新评论
我的标签
更多链接

我的标签
supervisor 配置(1)

随笔档案
2016年9月 (3)

最新评论
1. Re:linux下IPTABLES配置详解
学习了
--陈其苗
2. Re:linux下IPTABLES配置详解
mark
--陈其苗
3. Re:linux下IPTABLES配置详解
谢谢楼主 很nice 希望以后多出精品
--hero314
4. Re:linux下IPTABLES配置详解
楼主文章写得很详细，超赞，美中不足就是保存iptables文件的命令好像不太对，我用的service iptables save才成功保存的，还有NAT表里似乎不能添加drop规则，添加drop规则的.....
--climber1605
5. Re:linux下IPTABLES配置详解
很有帮助，谢谢楼主
--长平

阅读排行榜
1. linux下IPTABLES配置详解(153811)
2. Supervisor 配置过程(3479)
3. openssl 非对称加密DSA,RSA区别与使用介绍（转）(267)

评论排行榜
1. linux下IPTABLES配置详解(8)

推荐排行榜

linux下IPTABLES配置详解

linux下IPTABLES配置详解

-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 24000 -j ACCEPT
-A RH-Firewall-1-INPUT -s 121.10.120.24 -p tcp -m tcp --dport 18612 -j ACCEPT

如果你的IPTABLES基础知识还不了解,建议先去看看.
开始配置
我们来配置一个filter表的防火墙.
(1)查看本机关于IPTABLES的设置情况

```
[root@tp ~]# iptables -L -n
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
Chain RH-Firewall-1-INPUT (0 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:25
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

可以看出我在安装linux时,选择了有防火墙,并且开放了22,80,25端口.
如果你在安装linux时没有选择启动防火墙,是这样的

```
[root@tp ~]# iptables -L -n
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
```

什么规则都没有.
(2)清除原有规则.
不管你在安装linux时是否启动了防火墙,如果你想配置属于自己的防火墙,那就清除现在filter的所有规则.

```
[root@tp ~]# iptables -F      清除预设表filter中的所有规则链的规则
[root@tp ~]# iptables -X      清除预设表filter中使用者自定链中的规则
```

我们在来看一下

```
[root@tp ~]# iptables -L -n
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
```

什么都没有了吧,和我们在安装linux时没有启动防火墙是一样的.(提前说一句,这些配置就像用命令配置IP一样,重起就会失去作用),怎么保存.

```
[root@tp ~]# /etc/rc.d/init.d/iptables save
```

这样就可以写到/etc/sysconfig/iptables文件里了.写入后记得把防火墙重起一下,才能起作用.
[root@tp ~]# service iptables restart

现在IPTABLES配置表里什么配置都没有了,那我们开始我们的配置吧
(3)设定预设规则
[root@tp ~]# iptables -P INPUT DROP
[root@tp ~]# iptables -P OUTPUT ACCEPT
[root@tp ~]# iptables -P FORWARD DROP
上面的意思是,当超出了IPTABLES里filter表里的两个链规则(INPUT,FORWARD)时,不在这两个规则里的数据包怎么处理呢,那就是DROP(放弃).应该说这样配置是很安全的.我们要控制流入数据包
而对于OUTPUT链,也就是流出的包我们不用做太多限制,而是采取ACCEPT,也就是说,不在着个规则里的包怎么办呢,那就是通过.
可以看出INPUT,FORWARD两个链采用的是允许什么包通过,而OUTPUT链采用的是不允许什么包通过.
这样设置还是挺合理的,当然你也可以三个链都DROP,但这样做我认为是没有必要的,而且要写的规则就会增加.但如果你只想要有限的几个规则是,如只做WEB服务器.还是推荐三个链都是DROP.
注:如果你是远程SSH登陆的话,当你输入第一个命令回车的时候就应该掉了.因为你没有设置任何规则.
怎么办,去本机操作呗!
(4)添加规则.
首先添加INPUT链,INPUT链的默认规则是DROP,所以我们就写需要ACCETP(通过)的链
为了能采用远程SSH登陆,我们要开启22端口.
[root@tp ~]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
[root@tp ~]# iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT **(注:这个规则,如果你把OUTPUT 设置成DROP的就要写上这一部,好多人都是望了写这一部规则导致,始终无法SSH.在远程一下,是不是好了.**
其他的端口也一样,如果开启了web服务器,OUTPUT设置成DROP的话,同样也要添加一条链:
[root@tp ~]# iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT ,其他同理.)
如果做了WEB服务器,开启80端口.
[root@tp ~]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
如果做了邮件服务器,开启25,110端口.
[root@tp ~]# iptables -A INPUT -p tcp --dport 110 -j ACCEPT
[root@tp ~]# iptables -A INPUT -p tcp --dport 25 -j ACCEPT
如果做了FTP服务器,开启21端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
[root@tp ~]# iptables -A INPUT -p tcp --dport 20 -j ACCEPT
如果做了DNS服务器,开启53端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 53 -j ACCEPT
如果你还做了其他的服务器,需要开启哪个端口,照写就行了.
上面主要写的都是INPUT链,凡是不在上面的规则里的,都DROP
允许icmp包通过,也就是允许ping,
[root@tp ~]# iptables -A OUTPUT -p icmp -j ACCEPT (OUTPUT设置成DROP的话)
[root@tp ~]# iptables -A INPUT -p icmp -j ACCEPT (INPUT设置成DROP的话)
允许loopback!(不然会导致DNS无法正常关闭等问题)
IPTABLES -A INPUT -i lo -p all -j ACCEPT (如果是INPUT DROP)
IPTABLES -A OUTPUT -o lo -p all -j ACCEPT(如果是OUTPUT DROP)
下面写OUTPUT链,OUTPUT链默认规则是ACCEPT,所以我们就写需要DROP(放弃)的链.
减少不安全的端口连接
[root@tp ~]# iptables -A OUTPUT -p tcp --sport 31337 -j DROP
[root@tp ~]# iptables -A OUTPUT -p tcp --dport 31337 -j DROP
有些些特洛伊木马会扫描端口31337到31340(即黑客语言中的 elite 端口)上的服务。既然合法服务都不使用这些非标准端口来通信,阻塞这些端口能够有效地减少你的网络上可能被感染的机器和它们的远程主服务器进行独立通信的机会
还有其他端口也一样,像:31335、27444、27665、20034 NetBus、9704、137-139（smb）,2049(NFS)端口也应被禁止,我在这写的也不全,有兴趣的朋友应该去查一下相关资料.

当然出入更安全的考虑你也可以包OUTPUT链设置成DROP,那你添加的规则就多一些,就像上边添加允许SSH登陆一样.照着写就行了.

下面写一下更加细致的规则,就是限制到某台机器
如:我们只允许192.168.0.3的机器进行SSH连接
[root@tp ~]# iptables -A INPUT -s 192.168.0.3 -p tcp --dport 22 -j ACCEPT
如果要允许,或限制一段IP地址可用 192.168.0.0/24 表示192.168.0.1-255端的所有IP.
24表示子网掩码数.但要记得把 /etc/sysconfig/iptables 里的这一行删了.
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT 因为它表示所有地址都可以登陆.
或采用命令方式:
[root@tp ~]# iptables -D INPUT -p tcp --dport 22 -j ACCEPT
然后保存,我再说一边,反是采用命令的方式,只在当时生效,如果想要重起后也起作用,那就要保存.写入到/etc/sysconfig/iptables文件里.

```
[root@tp ~]# /etc/rc.d/init.d/iptables save
```

这样写 !192.168.0.3 表示除了192.168.0.3的ip地址
其他的规则连接也一样这么设置.

在下面就是FORWARD链,FORWARD链的默认规则是DROP,所以我们就写需要ACCETP(通过)的链,对正在转发链的监控.
开启转发功能,(在做NAT时,FORWARD默认规则是DROP时,必须做)

```
[root@tp ~]# iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
[root@tp ~]# iptables -A FORWARD -i eth1 -o eh0 -j ACCEPT
```

丢弃坏的TCP包

```
[root@tp ~]#iptables -A FORWARD -p TCP ! --syn -m state --state NEW -j DROP
```

处理IP碎片数量,防止攻击,允许每秒100个

```
[root@tp ~]#iptables -A FORWARD -f -m limit --limit 100/s --limit-burst 100 -j ACCEPT
```

设置ICMP包过滤,允许每秒1个包,限制触发条件是10个包.

```
[root@tp ~]#iptables -A FORWARD -p icmp -m limit --limit 1/s --limit-burst 10 -j ACCEPT
```

我在前面只所以允许ICMP包通过,就是因为我在这里有限制.
二,配置一个NAT表放火墙
1,查看本机关于NAT的设置情况

```
[root@tp rc.d]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  192.168.0.0/24       anywhere            to:211.101.46.235
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

我的NAT已经配置好了的(只是提供最简单的代理上网功能,还没有添加防火墙规则).关于怎么配置NAT,参考我的另一篇文章
当然你如果还没有配置NAT的话,你也不用清除规则,因为NAT在默认情况下是什么都没有的
如果你想清除,命令是

```
[root@tp ~]# iptables -F -t nat
[root@tp ~]# iptables -X -t nat
[root@tp ~]# iptables -Z -t nat
```

2,添加规则
添加基本的NAT地址转换,(关于如何配置NAT可以看我的另一篇文章),
添加规则,我们只添加DROP链.因为默认链全是ACCEPT.
防止外网用内网IP欺骗

```
[root@tp sysconfig]# iptables -t nat -A PREROUTING -i eth0 -s 10.0.0.0/8 -j DROP
[root@tp sysconfig]# iptables -t nat -A PREROUTING -i eth0 -s 172.16.0.0/12 -j DROP
[root@tp sysconfig]# iptables -t nat -A PREROUTING -i eth0 -s 192.168.0.0/16 -j DROP
```

如果我们想,比如阻止MSN,QQ,BT等的话,需要找到它们所用的端口或者IP,(个人认为没有太大必要)
例:
禁止与211.101.46.253的所有连接

```
[root@tp ~]# iptables -t nat -A PREROUTING -d 211.101.46.253 -j DROP
```

禁用FTP(21)端口

```
[root@tp ~]# iptables -t nat -A PREROUTING -p tcp --dport 21 -j DROP
```

这样写范围太大了,我们可以更精确的定义.

```
[root@tp ~]# iptables -t nat -A PREROUTING -p tcp --dport 21 -d 211.101.46.253 -j DROP
```

这样只禁用211.101.46.253地址的FTP连接,其他连接还可以.如web(80端口)连接.
按照我写的,你只要找到QQ,MSN等其他软件的IP地址,和端口,以及基于什么协议,只要照着写就行了.

最后:
drop非法连接

```
[root@tp ~]# iptables -A INPUT   -m state --state INVALID -j DROP
[root@tp ~]# iptables -A OUTPUT  -m state --state INVALID -j DROP
[root@tp ~]# iptables-A FORWARD -m state --state INVALID -j DROP
```

允许所有已经建立的和相关的连接

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

[root@tp ~]# /etc/rc.d/init.d/iptables save
```

这样就可以写到/etc/sysconfig/iptables文件里了.写入后记得把防火墙重起一下,才能起作用.

```
[root@tp ~]# service iptables restart
```

别忘了保存，不行就写一部保存一次．你可以一边保存，一边做实验，看看是否达到你的要求，
上面的所有规则我都试过，没有问题．
写这篇文章，用了我将近１个月的时间．查找资料，自己做实验，希望对大家有所帮助．如有不全及不完善的地方还请提出.
因为本篇文章以配置为主.关于IPTABLES的基础知识及指令命令说明等我会尽快传上,当然你可以去网上搜索一下,还是很多的.

Linux防火墙iptables学习笔记

一、概要

1、防火墙分类

①包过滤防火墙(pack filtering)在网络层对数据包进行选择过滤，采用访问控制列表(Access control table－ACL)检查数据流的源地址，目的地址，源和目的端口，IP等信息。

②代理服务器型防火墙

2、iptables基础

①规则(rules)：网络管理员预定义的条件

②链(chains)：是数据包传播的路径

③表(tables)：内置3个表filter表，nat表，mangle表分别用于实现包过滤网络地址转换和包重构的功能

④filter表是系统默认的，INPUT表(进入的包)，FORWORD(转发的包)，OUTPUT(处理本地生成的包)，filter表只能对包进行授受和丢弃的操作。

⑤nat表(网络地址转换)，PREROUTING(修改即将到来的数据包)，OUTPUT(修改在路由之前本地生成的数据包)，POSTROUTING(修改即将出去的数据包)

⑥mangle表，PREROUTING，OUTPUT，FORWORD，POSTROUTING，INPUT

3、其它

iptables是按照顺序读取规则

防火墙规则的配置建议

Ⅰ 规则力求简单

Ⅱ 规则的顺序很重要

Ⅲ 尽量优化规则

Ⅳ 做好笔记

二、配置

1、iptables命令格式

iptables [-t 表] －命令 匹配 操作 （大小写敏感）

动作选项

ACCEPT 接收数据包

DROP 丢弃数据包

REDIRECT 将数据包重新转向到本机或另一台主机的某一个端口，通常功能实现透明代理或对外开放内网的某些服务

SNAT 源地址转换

DNAT 目的地址转换

MASQUERADE IP伪装

LOG 日志功能

2、定义规则

①先拒绝所有的数据包，然后再允许需要的数据包

iptalbes -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

②查看nat表所有链的规则列表

iptables -t nat -L

③增加，插入，删除和替换规则

iptables [-t 表名] <-A|I|D|R> 链名 [规则编号] [-i|o 网卡名称] [-p 协议类型] [-s 源ip|源子网] [--sport 源端口号] [-d 目的IP|目标子网] [--dport 目标端口号] [-j 动作]

参数：-A 增加

-I 插入

-D 删除

-R 替换

三、例子

①iptables -t filter -A INPUT -s 192.168.1.5 -i eth0 -j DROP

禁止IP为192.168.1.5的主机从eth0访问本机②iptables -t filter -I INPUT 2 -s 192.168.5.0/24 -p tcp --dport 80 -j DROP

禁止子网192.168.5.0访问web服务③iptables -t filter -I INPUT 2 -s 192.168.7.9 -p tcp --dport ftp -j DROP

禁止IP为192.168.7.9访问FTP服务

④iptables -t filter -L INPUT

查看filter表中INPUT链的规则

⑤iptables -t nat -F
删除nat表中的所有规则
⑥iptables -I FORWARD -d wwww.playboy.com -j DROP
禁止访问www.playboy.com网站
⑦iptables -I FORWARD -s 192.168.5.23 -j DROP
禁止192.168.5.23上网

三毛仔
关注 - 3
粉丝 - 7
+加关注

7 0

« 上一篇：openssl 非对称加密DSA,RSA区别与使用介绍（转）
» 下一篇：Supervisor 配置过程

posted @ 2016-09-07 10:14 三毛仔 阅读(153818) 评论(8) 编辑 收藏

发表评论

#1楼 2017-01-18 15:26 | 饥渴的青蛙5

这篇文章把我给害惨了，那么重要的注你都不强调一下，远程ssh登录的，现在完蛋了，还是重新编排下吧

支持(4) 反对

#2楼 2017-03-03 17:46 | 肖伯特

如何禁止访问外网某个ip地址：
iptables -A OUTPUT -d xx.xx.xx.xx -j REJECT

支持(0) 反对

#3楼 2017-07-21 08:53 | monster_ygs

@ 饥渴的青蛙5
这是一篇学习的文章，需要根据自己的时间情况进行操作
自己写入之前不注意自己的逻辑是否有问题
怪人家没有提醒，写文章最怕遇到这种人

支持(2) 反对

#4楼 2018-02-11 17:22 | 长平

很有帮助，谢谢楼主

支持(0) 反对

#5楼 2018-06-26 01:02 | climber1605

楼主文章写得很详细，超赞，美中不足就是保存iptables文件的命令好像不太对，我用的service iptables save才成功保存的，还有NAT表里似乎不能添加drop规则，添加drop规则的时候提示The "nat" table is not intended for filtering, the se of DROP is therefore inhibited.

支持(1) 反对

#6楼 2018-09-30 13:40 | hero314

谢谢楼主 很nice 希望以后多出精品

支持(0) 反对

#7楼 2018-11-23 18:08 | 陈其苗

mark

支持(0) 反对

#8楼 2018-11-23 18:08 | 陈其苗

学习了

支持(0) 反对

相关博文：
· Linux 下 iptables 配置详解
· linux中iptables配置文件及命令详解详解
· Linux服务器tomcat无法通过ip加端口访问
· linux中查看和开放端口
· Linux中如何开启8080端口供外界访问 和开启允许对外访问的端口8000

最新新闻：
· 消息称京东2019年将末位淘汰10%的高管
· 苹果聘请了一位做智能锁的失败创业者来拯救失败的智能家居业务
· Android 上的「三大金刚」快要只剩一个了
· Jolla的Sailfish OS在俄罗斯更名为Aurora OS
· 深度学习框架TensorFlow.NET 0.3.0，新增图片识别示例
» 更多新闻...