iptables 添加，删除，查看，修改

张映 发表于 2012-05-10

分类目录： linux, 系统安全

标签：iptables, 修改, 删除, 查看, 添加

iptables是linux系统自带的防火墙，功能强大，学习起来需要一段时间，下面是一些习iptables的时候的记录。如果iptables不熟悉的话可以用apf，是一款基于iptables的防火墙，挺好用的。请参考：**linux apf 防火墙 安装 配置**

一,安装并启动防火墙

```
01. [root@linux ~]# /etc/init.d/iptables start
```

当我们用iptables添加规则，保存后，这些规则以文件的形势存在磁盘上的，以centos为例，文件地址是/etc/sysconfig/iptables，我们可以通过命令的方式去添加，修改，删除规则，也可以直接修改/etc/sysconfig/iptables这个文件就行了。

二,添加防火墙规则

1,添加filter表

```
查看 复制 打印 ?
01. [root@linux ~]# iptables -A INPUT -p tcp -m tcp --dport 21 -j ACCEPT  //开放21端口
```

出口我都是开放的**iptables -P OUTPUT ACCEPT**，所以出口就没必要在去开放端口了。

2,添加nat表

```
01. [root@linux ~]# iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -j MASQUERADE
```

将源地址是 192.168.10.0/24 的数据包进行地址伪装

3,-A默认是插入到尾部的，可以-I来插入到指定位置

```
查看 复制 打印 ?
01. [root@linux ~]# iptables -I INPUT 3 -p tcp -m tcp --dport 20 -j ACCEPT
02.
03. [root@linux ~]# iptables -L -n --line-number
04. Chain INPUT (policy DROP)
05. num  target     prot opt source               destination
06. 1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
07. 2    DROP       icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 8
08. 3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:20                //-I指定位置插的
09. 4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
10. 5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
11. 6    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
12. 7    DROP       all  --  0.0.0.0/0            0.0.0.0/0           state INVALID,NEW
13. 8    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21                //-A默认插到最后
14.
15. Chain FORWARD (policy ACCEPT)
16. num  target     prot opt source               destination
17.
18. Chain OUTPUT (policy ACCEPT)
19. num  target     prot opt source               destination
```

三,查下iptable规则

1,查看filter表

```
查看 复制 打印 ?
01. [root@linux ~]# iptables -L -n --line-number |grep 21 //--line-number可以显示规则序号，在删除的时候比较方便
02. 5    ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:21
```

如果不加-t的话，默认就是filter表，查看，添加，删除都是的

2,查看nat表

```
[root@linux ~]# iptables -t nat -vnL POSTROUTING --line-number
Chain POSTROUTING (policy ACCEPT 38 packets, 2297 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 MASQUERADE  all  --  *      *       192.168.10.0/24      0.0.0.0/0
```

四，修改规则

```
查看  复制  打印  ?
[root@linux ~]# iptables -R INPUT 3 -j DROP    //将规则3改成DROP
```

五,删除iptables规则

```
查看  复制  打印  ?
[root@linux ~]# iptables -D INPUT 3  //删除input的第3条规则

[root@linux ~]# iptables -t nat -D POSTROUTING 1  //删除nat表中postrouting的第一条规则

[root@linux ~]# iptables -F INPUT   //清空 filter表INPUT所有规则

[root@linux ~]# iptables -F    //清空所有规则

[root@linux ~]# iptables -t nat -F POSTROUTING   //清空nat表POSTROUTING所有规则
```

六，设置默认规则

```
查看  复制  打印  ?
[root@linux ~]# iptables -P INPUT DROP  //设置filter表INPUT默认规则是 DROP
```

所有添加，删除，修改后都要保存起来，/etc/init.d/iptables save.上面只是一些最基本的操作，要想灵活运用，还要一定时间的实际操作。

<< iptables snat和dnat
centos5.5 vpn 安装配置详解 >>

相关文章

- git 命令行下 添加 修改 删除 冲突解决
- elasticsearch 数据 添加，更新，删除，查询
- elasticsearch mapping 添加 编辑 删除字段
- redis cluster 添加 删除 重分配 节点
- json 数据 添加 删除 排序
- mongodb replica set 添加 删除 节点 2种方法
- kafka 删除 topic 及数据
- linux lvm 安全 删除 硬盘或分区
- vi vim 行尾 ^M 删除
- mongodb 数据库创建,切换,删除

1 条评论

1. *canon* 留言 (2018年1月17日 15:16):

   `iptables -t nat -vnL POSTROUTING --line-number `
   这条命令去了POSTROUTING 我执行成功了

留下评论

抱歉，发表回复评论您必须登录。

- **分类目录**
  - apache/nginx (36)
  - cache (21)
  - clickhouse (14)
  - drupal (7)
  - eclipse (8)
  - elasticsearch (18)
  - google (3)
  - hadoop/spark/scala (96)
  - html/css (12)
  - java/android (14)
  - linux (87)
  - mariadb (2)
  - mysql (74)
  - nodejs/vue/js/jquery (72)

- nosql (39)
- oracle (9)
- pgsql (8)
- php (107)
- seo (16)
- shell (11)
- smarty (5)
- tidb (21)
- wordpress (13)
- 云计算 (22)
- 双眼看社会 (13)
- 技术其他 (41)
- 服务器相关 (136)
- 系统安全 (7)

- **最近文章**

  - tidb 误删库，表，数据恢复
  - ticdc 同步有规律的数据库
  - canal 同步mysql数据到clickhouse 支持update delete truncate
  - canal 同步mysql数据到clickhouse 忽略delete update
  - tidb 扩容和缩容
  - clickhouse,tidb,mysql 读取速度对比
  - clickhouse right join 问题
  - canal 同步mysql数据到clickhouse
  - nginx clickhouse 反向代理
  - clickhouse MaterializeMySQL 同步 mysql 数据

- **最近评论和留言**

  - banner 在 awk是命令还是编程语言 上的评论
  - lin 在 hadoop 查看 mr日志报错 上的评论
  - ccc 在 cdh hive 2.1.1 升级到 2.3.4 上的评论
  - 简简单单 在 关于我 上的评论
  - www 在 clickhouse,tidb,mysql 读取速度对比 上的评论
  - zzq 在 mysql分表，分区的区别和联系 上的评论
  - Bill 在 怎么在网上找到你要的信息 上的评论
  - 11 在 留言板 留言了
  - Michael 在 canal 同步mysql数据到clickhouse 支持update delete truncate 上的评论
  - 我兜里有糖 在 linux postgresql 安装配置详解 上的评论

- **登录**

  - 登录