公告

昵称：valiente
园龄：1年1个月
粉丝：8
关注：9
+加关注

< 2017年7月 >

日	一	二	三	四	五	六
25	26	27	28	29	30	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	29
30	31	1	2	3	4	5

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

最新随笔

1. day25 CMDB(1)
2. day20 BBS前奏
3. day19 django继续
4. day18 jQuery，JavaScript高级&Django
5. day17 jQuery
6. day16 web前端之JavaScript
7. day15 web前端之css
8. day14 paramiko堡垒机
9. saltstack快速入门
10. day13 SQLAlchemy

随笔分类

linux学习(2)
mysql学习
python其他资料(1)

随笔-30 文章-0 评论-0

iptables的实战整理

一、iptables使用场景：

内网情况下使用；在大并发的情况下不要开iptables否则影响性能

二、iptables出现下面的问题：

在yewufangwenbijiaoman/var/log/message中出现 ip(nf)_conntrack: table full 使得企业访问较慢的解决方法：

```
vim /etc/sysctl.conf
#加大 ip_conntrack_max 值
net.ipv4.ip_conntrack_max =393216
net.ipv4.netfilter.ip_conntrack_max =393216#降低 ip_conntrack timeout时间
net.ipv4.netfilter.ip_conntrack_tcp_timeout_established =300
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
```

三、安全优化

尽可能不给服务器分配外网IP，可以通过代理转发；并发布不是特别大的外网ip环境，尽量开启防火墙

四、iptables简介

基于数据包过滤的防火墙工具，主要工作在osi模型的二三四层（经过内核编译可以实现七层控制）

五、基本名词介绍

四表：filter（INPUT，FORWARD，OUTPUT），NAT（OUTPUT，PREROUTING，POSTROUTING），MANGLE（五链），RAW

五链（要大写）：INPUT，OUTPUT，FORWARD，PREROUTING，POSTROUTING

链（chain）是规则（policy）的容器

六、详细介绍

filter表：主要和主机自身相关，真正负责防火墙功能的（过滤流入流出主机的数据包）。

INPUT：负责过滤所有进入主机的数据包(最主要)

FORWARD：负责流经主机的数据包

OUTPUT：处理所有源地址都是本机地址的数据包（也就

python学习(13)
网络及其他(1)

随笔档案

2017年5月 (1)
2017年4月 (1)
2017年3月 (2)
2017年2月 (4)
2017年1月 (5)
2016年12月 (3)
2016年11月 (1)
2016年10月 (1)
2016年9月 (4)
2016年8月 (4)
2016年7月 (2)
2016年6月 (2)

友情链接

CSDN大神
金角大王
连志雷
我当道士那些年
学习链接
银角大王

积分与排名

积分 - 7015
排名 - 33831

阅读排行榜

1. 【python自动化第一篇：python介绍与入门】(3675)
2. 【python自动化第二篇：python入门】(729)
3. 【python自动化第三篇：python入门进阶】(459)
4. iptables的实战整理(360)
5. 【python自动化第四篇：python入门进阶】(343)

推荐排行榜

1. 【python自动化第一篇：python介绍与入门】(1)

是主机发出去的数据包）

nat表：主要负责网络地址之间的转换,包括来源和目的端口以及ip（PREROUTING），可以共享上网（POSTROUTING），端口转换，企业路由和网关

OUTPUT：和从主机发出去的数据包有关，改变数据包的目的地址

PREROUTING：在数据包到达防火墙时进行路由判断之前的的规则，作用是改变数据包的目的地址，目的端口等

POSTROUTING：离开防火墙时进行路由判断之后执行的规则，作用是改变数据包的源地址和源端口

mangle：路由标记（TTL，TOS，mark）。。。。

七、iptables的工作流程

采用的是数据包过滤的机制，会对请求的数据包的包头数据进行分析，按照规则从上到下匹配

小结：防火墙是层层过滤的，通过匹配上规则来允许或者组织数据包的走向，默认规则是最后处理的。

八、iptables 表和链的工作流程图

总结：在使用nat表的时候要注意和nat的PREROUTING，filter的FORWARD和nat的POSTROUTING一起使用

在使用filter的时候只是在INPUT链加以控制即可

九、实战演练

（0）、查看防火墙：

```
iptables -L -n (-v -x)
iptables -L -n --line-numbers  带序号显示配合删除
```

无法启动iptables的解决（setup）

```
lsmod | egrep "nat | filter"    查看加载的内核文件
modprobe +内核加载文件          可以添加内核加载文件
```

（1）、清理参数

```
iptables -F :清除所有的防火墙规则
iptables -X [chain] :删除自定义的链        iptables -N chain    新建自定义的链
iptables -Z:  对链计数器的清零
```

（2）、禁止规则

iptables -t filter -A INPUT -p tcp --dport 22 -j DROP 禁止ssh远程登录

-t 指定表 -A 追加 -p 指定协议 --dport 指定目的端口 -j 采取的方式

掉ssh的处理方法：下机房，管理卡，计划任务关防火墙，

iptables -t filter -A INPUT -p tcp --dport 80 -j DROP 会造成找不到网页不会造成404

（3）、添加规则

封IP实战演练：

首先要分析日志中的ip连接数：

```
awk '{print $1}' /opt/nginx/access.log | sort |uniq -c | sort -rn -k1
```

然后再封ip

```
iptables -I INPUT -p tcp -s IP --dport 80 -j DROP
```

将此规则置顶

```
iptables -I INPUT 2 -p tcp -s IP --dport 8080 -j DROP
```

将此规则放到第二位

```
iptables -t filter -A INPUT -i eth0 -s 172.1.1.2 -j DROP
```

封ip

禁止某个网段连入:不管什么服务都连不进来

```
iptables -A INPUT -i eth0 -s 172.1.1.0/24 -j DROP
```

取消该网段连入

```
iptables -A INPUT -i eth0 ！-s 172.1.1.0/24 -j DROP
```

封一下ICMP协议(不让ping)，其他服务可以使用：

```
iptables -A INPUT -p icmp-type 8(any) -i eth0 ！-s 172.1.1.2 -j DROP
```

更改ssh和rootuankouzhihoude防火墙操作

```
iptables -A INPUT -p tcp --dport 65535！-s 172.1.1.0/24 -j DROP
```

封掉3306端口

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

匹配DNS端口：tcp&udp

```
iptables -A INPUT -p tcp --sport 53
iptables -A INPUT -p udp --sport 53
```

匹配指定端口以外的端口：

```
iptables -A INPUT -p tcp --dport！22
iptables -A INPUT -p tcp！--doprt 22 -s 172.1.1.0/24 -j DROP
```

端口匹配范围：

```
iptables -A INPUT -p tcp --sport 22:80
iptables -A INPUT -p tcp -m mulport --dport 21,25,24,80 -j ACCEPT
```

匹配网络状态

-m state --state

NEW:建立的或者将启动新的连接

ESTABLISHED：已经建立的连接

RELATED：正在启动新连接

INVALID：非法连接

FTP

允许关联的状态包：

```
iptables -A INPUT -m state --state ESTABLISHE,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHE,RELATED -j ACCEPT
```

-m limit

--limit n/{second/minute/hour}:指定时间内的请求速度“n”为

速率，后面的时间分别是秒分时

--limit-burst [n]:在同一时间允许通过的请求"n"位数字，不能指定为默认的5

限制每分钟请求和并发不超过6个

iptables -A INPUT -s 172.1.1.0/24 -d 172.1.1.2 -p icmp --icmp-type 8 -m limit --limit 20/min --limit-burst 6 -j ACCEPT

iptables -A OUTPUT -s 172.1.1.2 -d 172.1.1.0/24 -p icmp --icmp-type 0 -j ACCEPT

企业实战

企业及防火前实战模式：逛公园模式和看电影模式

看电影模式：

（1）清理所有的防火墙规则

iptables -F

iptables -X

iptables -Z

（2）设置ssh登录

iptables -A INPUT -p tcp --dport 65535 -s 172.1.1.0/24 -j ACCEPT

（3）允许本机lo通信机制

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

（4）设置默认的防火墙允许和禁止规则

iptables -P OUTPUT ACCEPT

iptables --policy FORWARD DROP

iptables --policy INPUT DROP

（5）开启信任的网段

iptables -A INPUT -s 172.1.1.1/24 -p all -j ACCEPT

iptables -A INPUT -s 172.168.1.2/24 -p all -j ACCEPT

这边开启的信任包括：办公室指定ip，idc内网ip，其他机房的ip

（6）允许业务访问的端口开启

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p icmp --icmp-type any -j ACCEPT(可以聚聚ping的)

（7）允许关联的状态包通过（web服务不要使用FTP服务）

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

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

使用nmap测试开启的端口

nmap IP -p 1-65535

（8）永久保存配置

```
/etc/init.d/iptables save
```

（9）企业面试规则

自定义链，处理syn攻击

```
iptables -N syn-flood
iptables -A INPUT -i eth0 -syn -j syn-flood
iptabls -A syn-flood -m limit --limit 5000/s --limit-
burst 200 -j RETURN
iptables -A syn-flood DROP
```

自动封IP脚本(计划任务结合执行)

```
#!/bin/sh
/bin/netstat -
na | grep ESTABLISHED | awk {print $5} |awk -
F: '{print $1}' |sort |uniq -c |sort -rn | head -10| grep -v -
E '192.168|127.0' |awk '{if ($2!=null && $1>4) {print $2}
}' > /home/shell/dropip
for i in $(cat /home/shell/dropip)
do
    /sbin/iptables -I INPUT -s $i -j DROP
    echo "$i kill at `date`" >> /var/log/ddos.txt
done
```

常用服务的iptables设置

```
##nagios监控
iptables -A INPUT -s 172.1.1.0/24 -p tcp --dport 5666 -
j ACCEPT
##mysql
iptables -A INPUT -s 172.1.1.0/24 -p tcp --dport 3306 -
j ACCEPT
iptables -A INPUT -s 172.1.1.0/24 -p tcp --dport 3307 -
j ACCEPT
###snmp
iptables -A INPUT -s 172.1.1.0/24 -p UDP --dport 161 -
j ACCEPT
##rsync
iptables -A INPUT -s 171.0.0.1/24 -p tcp -m tcp --
dport 873 -j ACCEPT
##nfs2049,portmap 111
iptables -A INPUT -s 172.1.1.0/24 -p udp -m multiport --
dport 111,892,2049 -j ACCEPT
iptables -A INPUT -s 172.1.1.0/24 -p tcp -m multiport --
dport 111,892,2049 -j ACCEPT
##icmp
iptables -A INPUT -s 172.1.1.0/24 -p icmp -m icmp --icmp-
type any -j ACCEPT
```

网关服务器配置：

需要具备的条件

（1）、物理条件是具备双网卡（eth0和外网的网关要有，eth1是内网且不具备网关）

（2）、网关服务器要能上网

（3）、开启转发功能。修改/etc/sysctl.conf下的net.ipv4.ip_forward = 1，之后再sysctrl -p使得配置生效

（4）、iptables的forward链允许转发[iptables -P INPUT ACCEPT]

（5）、清空防火墙规则iptables -F；iptables -P FORWARD ACCEPT

（6）、载入模块

先查看lsmod |egrep ^ip

在导入

modprobe ip_contrack

modprobe ip_nat_ftp

modprobe ipt_state

modprobe ip_contrack_ftp

modprobe iptable_filter

（7）、然后再网关服务器上执行

iptables -t nat -A POSTROUTING -s 172.1.1.0/24 -o eth0 -j SNAT --to-source 外网IP（路由器内网ip）

iptables -t nat -A POSTROUTING -s 172.1.1.0/24 -j MASQUERADE

（8）、访问外网映射到内网的服务器上

iptables -t nat -A PREROUTING -d 服务器内网IP -p tcp --dport 80 -j DNAT --to-destination 内网IP：端口

iptables的企业案例：

（1）、linux主机防火墙（filter）

（2）、共享上网（nat postrouting）

（3）、web地址和端口映射

（4）、ip的一对一映射

企业应用：实现外网ip（124.42.34.112）一对一映射到内网的server(10.0.0.8)上

网关ipeth0：124.42.60.109 eth1:10.0.0.254

首先在路由网关上绑定124.42.34.112，可以用别名的方式：

iptables -t nat -A PREROUTING -d 124.42.34.112 -j DNAT --to-destination 10.0.0.8

```
iptables -t nat -A POSTROUTING -s 10.0.0.8 -o eth0 -
j SNAT --to-source 124.42.34.112
iptables -t nat -A POSTROUTING -
s 10.0.0.0/255.255.255.0 -d 124.24.34.112 -j SNAT --to-
source 10.0.0.254
```

映射多个外网ip上网：

```
iptables -t nat -A POSTROUTING -
s 10.0.0.0/255.255.255.0 -o eth0 -
j SNAT 124.42.60.11 -124.42.60.16
iptables -t NAT -A POSTROUTING -
s 172.0.0.0/255.255.255.0 -o eth0 -
j SNAT 124.42.60.103-124.42.60.106
```

大于254台机器的网段划分，route命令讲解

oldboy.blog.51cto.com下搜索route

分类: linux学习

最新IT新闻：
- Linus Torvalds：Linux之旅既有趣又幸运，不敢奢望精通内核
- 八年iOS老开发的五点心得
- SpaceX成功发射Intelsat 35e卫星
- 300家平台倒闭，BAT纷纷离场，众筹平台为什么全军覆没？
- 再谈摩拜ofo之争，背后其实是两家公司对物联网技术的理解偏差

» 更多新闻...

最新知识库文章：
- 小printf的故事：什么是真正的程序员？
- 程序员的工作、学习与绩效
- 软件开发为什么很难
- 唱吧DevOps的落地，微服务CI/CD的范本技术解读
- 程序员，如何从平庸走向理想？

» 更多知识库文章...