Linux iptables 学习

1. 课程介绍

iptables 主要用在Linux上的访问控制，网络行为管理

1. 场景演示

通过iptables控制并发访问场景

Client1 visit Server1

在server上启动一个HTTP服务

在client上使用ab -n 10000 -c 40 <http://ip:port/text.txt>

iptables -F 清除iptables的设置

在服务器上查看连接情况：

netstat -an | grep 80 | grep [client\_ip]|grep EST -c

使用w查看服务器的负载

添加iptables规则访问控制

iptables -I INPUT -p tcp --dport 80 -s [source\_ip] -m connlimit --connlimit-above 10 -j REJECT

这样客户端如果访问的数量超过限制，就会被禁止。

1. 学习课程的意义

使用iptables搭建一个企业应用的防火墙规则

使用iptables防止服务器被攻击

如何利用iptables进行数据包的转发

明白iptables的强大以及实际使用的意义。

1. iptables 原理及其组成
2. Netfilter

Netfilter 是Linux操作系统核心层内部的一个数据包处理模块

Hook Point：数据包在NetFilter中的挂在点（PRE\_ROUTING INPUT OUTPUT FORWARD POST\_ROUTING）在这五个挂在点进行数据包的处理

用户层：iptables 命令

内核层：iptables内核模块 TCP UDP 协议

Hook Point： 对应IP层，数据到达之后再HookPoint上进行操作处理

硬件层:数据链路层

1. iptables 的规则组成

四张表 +五条链 + 规则

四张表

Filter：

Nat：地址转发

Mangle表:修改数据包，改变包头内容（TTL TOS MARK）

Raw表： 不常用

1. 链:

INPUT

OUTPUT

FORWARD

PRE\_ROUTE

POST\_ROUTE

数据流

Data Stream IN Data stream out

PRE\_ROUTING (nat mangle raw) POST\_ROUTING(nat raw mangle)

Destination Localhost no => FOR\_WARD( filter mangle) =>

Input(filter mangle) => handle by localhost=> OUTPUT(filter nat mangle raw)

1. iptables 数据包访问控制

数据包访问控制：ACCEPT DROP REJECT

数据包改写: SNAT(修改源地址) DNAT（对于目标地址修改）

信息记录：LOG（写日志）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| iptables | table | command | Chain | Parameter&  XMatch | target |
|  | -t  filter  nat | -A last add  -D delete  -L -n view  -F flush  -P  -I first add | INPUT  FORWARD  OUTPUT  PRE\_ROUTING  POST\_TOUTING | -p tcp  -s  -d  --sport  --dport  --dports  -m tcp  state  multiport | -j ACCEPT  DROP  REJECT  DNAT  SNAT |

1. iptable实践场景

1. 测试iptables环境

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

iptables -I INPUT -p tcp --dport 22 -j ACCEPT

iptables -I INPUT -p tcp --dport 10:21 -j ACCEPT

iptables -I INPUT -p icmp -j ACCEPT

iptables -A INPUT -j REJECT

iptables -L #查看

使用namp进行端口扫描：

namp -sS -p 0-1000 [dest\_ip] 检测到 80http 和22 ssh

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

iptables -I INPUR -p tcp --dport 80 -j REJECT

namp -sS -p 1-1000 [dest\_ip] # 检测不到80服务

本机检测80端口是开放运行的

netstat -luntp | grep 80

2. iptables实验环境

本机无法访问本机

iptables -I INPUT -i lo -j ACCEPT

telnet 127.0.0.1 22 可以连接

本机无法访问其他主机

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

如果本地主动访问外面网络，允许数据过去，这样就可以连接到外面的网络。

curl -I <http://www.imooc.com>

1. 特殊例外

在上面的场景中，修改只允许10.103.188.233 访问本机的httpd服务

iptables -D INPUT -p tcp --dport 80 -j ACCEPT # 删除之前的规则

iptable -nL #查看

iptables -I INPUT -p tcp -s 10.10.188.233 --dport 80 -j ACCEPT

1. 场景二

FTP主动模式下的iptables的配置：客户端接收数据的端口是随机的，服务器发送数据的端口是固定的20

FTP被动模式下的iptables的配置：服务器端随机一个端口，并且通知给客户端，客户端再去服务器端获取数据。

1. FTP主动模式下

ftp默认采用的是被动模式，需要采取主动模式，则需要在vsftp中设置如下参数：

port\_enable=yes

connect\_from\_port\_20=yes

在iptables -I INPUT -p tcp --dport 21 -j ACCEPT #开放21端口

安装vsftp 配置参数之后，重新启动vsftp

iptables -F

iptables -I INPUT -p tcp --dport 21 -j ACCEPT

iptables -I INPUT -p tcp --dport 22 -j ACCEPT

iptables -I INPUT -p icmp -j ACCEPT

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

ftp 10.10.188.233

passive #关闭被动模式，启动主动模式，一般不建议主动模式连接。

1. FTP被动模式

客户端默认被动模式

被动模式，客户端主动向服务器随机开放的一个数据端口获取数据。

iptables -I INPUT -p tcp --dport 21 -j ACCEPT

vim /etc/vsftpd/vsftpd.conf

pasv\_min\_port=50000

pasv\_max\_port=60000

iptables -I INPUT -p tcp --dport 50000:60000 -j ACCEPT

1. FTP 被动模式的设置

方法一：

/etc/init.d/vsftpd restart

iptables -I INPUT -p tcp --dport 50000:60000 -j ACCEPT

方法二：使用连接追踪模块

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

iptables -I INPUT -p tcp --dport 21 -j ACCEPT

modprobe nf\_conntrack\_ftp # 临时

vim /etc/sysconfig/iptables-config # 开机自动加载

IPTABLES\_MODULES=”nf\_conntrack\_ftp”

1. 场景三

要求：

员工在公司内部能够访问服务器上的任何五福

员工在外出差，通过VPN连接服务器，VPN服务器可以访问内网FTP NFS SSH

公司有一个门户网站需要允许公网访问

公司内网是 10.10.155.0/24 10.10.188.0/24

常见端口

www http 80/tcp

https 443/tcp

Mail smtp 25/tcp

smtps 465/tcp

pop3 110/tcp

pop3s 995/tcp

imap 143/tcp

文件服务

NFS 123/udp

SAMBA 137 138 139/tcp 445/tcp

FTP 20/tcp 21/tcp

SSH 22/tcp

MYSQL 3306/tcp

ORACLE 1512/tcp

配置的基本思路

允许本地访问

允许已经监听数据包通过

允许规则中允许的数据包通过

拒绝规则

拒绝未允许的数据包

1. 具体实现

iptables -F

iptables -I INPUT -i lo -j ACCEPT

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

iptables -A INPUT -s 10.10.155.0/24 -j ACCEPT

iptables -A INPUT -s 10.10.188.0/24 -j ACCEPT

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

iptables -A INPUT -p tcp --dport 1723 -j ACCEPT #VPN port

iptables -I INPUT -p icmp -j ACCEPT

Ipatbles -A INPUT -j REJECT

/etc/init.d/iptables save

vim /etc/sysconfig/iptables

chkconfig iptables on

编写脚本文件

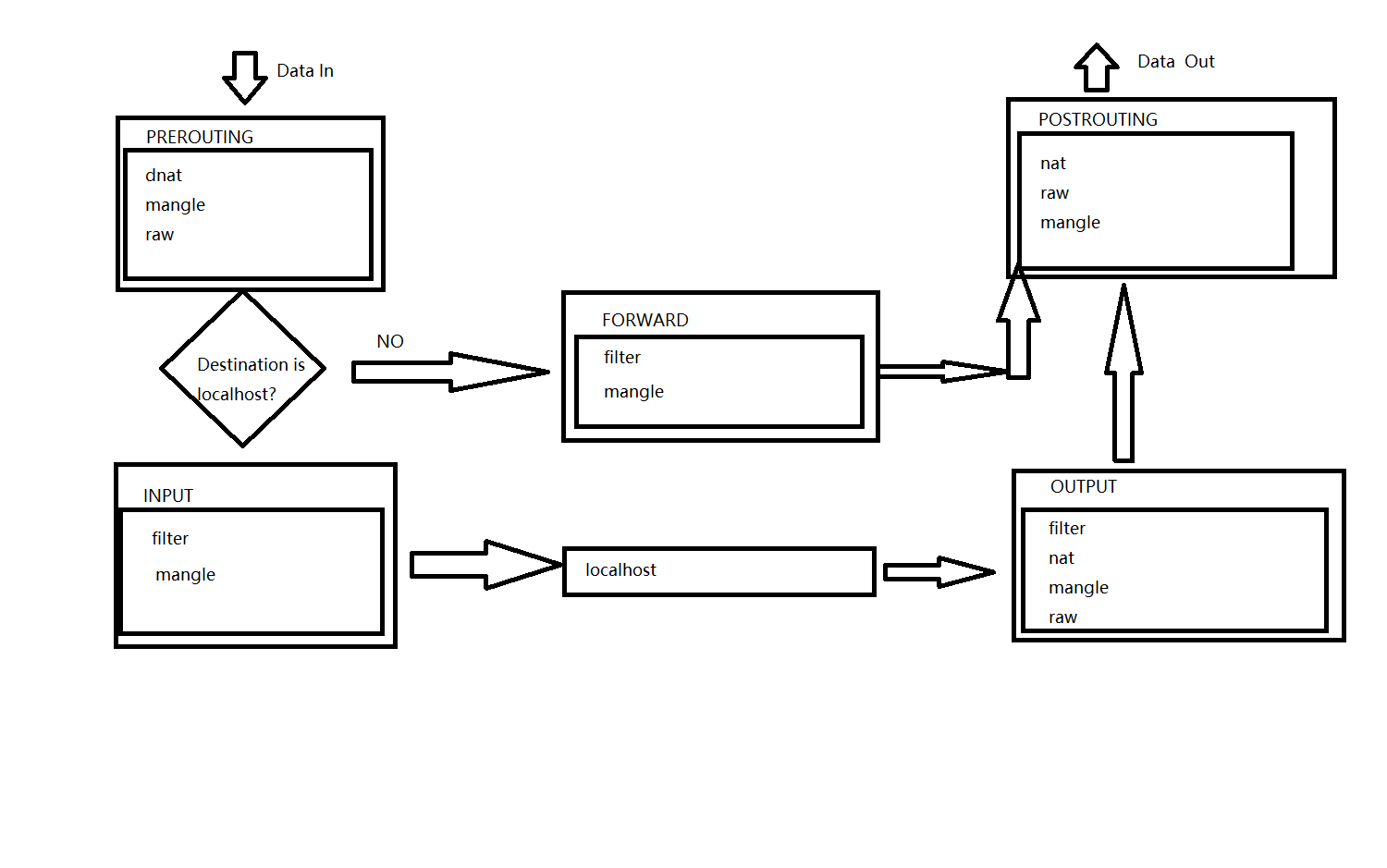
/bin/sh /opt/iptable\_ssh.sh

vim /etc/rc.local 运行该脚本。

1. iptables 中NAT的设置
2. iptables 防火墙NAT表的规则配置

SNAT 源地址转换 作用链：出口POSTROUTING

DNAT 目标地址转换 作用链：进口PREROUTING



Nat Server：双网卡

打开数据包转发的内核开关

/etc/sysctl.conf

Net.ipv4.ip\_forward=1

执行生效#sysctl -p

sysctl -a | grep ip\_forward

#iptables

iptables -t nat -A POSTROUTING -s 10.10.177.0/24 -j SNAT --to 10.10.188.232

iptables -t nat -L

HTTP SErver： 10.10.188.173

Client：添加默认网关 10.10.177.233/24 GW 10.10.177.232

/etc/sysconfig/network

GATEWAY=10.10.177.232

OR:

route add 0.0.0.0 gw 10.10.177.232

DNAT 模拟

Client： 10.10.188.173

NAT Server：

IP1：10.10.188.232:80

IP2：10.10.177.232

iptables -t nat -A PREROUTING -d 10.10.188.232 -p tcp --dport 80 -j DNAT --to 10.10.177.233:80 #改变数据包的目的地址

HTTP SErver：10.10.177.233:80

通过DNAT实现Client1 访问HTTP Server

iptables -t nat -A POSTROUTING -s 192.168.1.64 -p tcp -j SNAT --to-source 10.8.0.6 #改变数据包的源地址

1. iptables中的防攻击以及企业场景的应用
2. SYN 攻击 DDOS攻击

利用iptables防止CC攻击

connlimit 限制一个ip的客户端的并发连接数目

-connlimit-above n

iptables -I INPUT -p tcp --syn -dport 80 -m connlimit -connlimit-above 100 -j REJECT

Limit模块：限制控制流量

iptables -A INPUT -m limit --limit 3/hour

--limit-burst 默认值是5

# 只允许前10个通过，后面每分钟通过一个

iptables -A INPUT -p icmp -m limit --limit 1/m --limit-burst 10 -j ACCEPT

Iptables -A -p icmp -j DROP

1. iptables实际的应用

系统化介绍iptables的规则配置

介绍iptables中的其他模块

防攻击策略补充

modprob ipt\_MASQUERADE

modprob ip\_conntrack\_ftp

modprob ip\_nat\_ftp

iptables -F

iptables -t nat -F

iptables -X

iptables -t nat -X

iptables -P INPUT DROP

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

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -p tcp -m multiport --dports 100,80,25 -j ACCEPT

iptables -A INPUT -p tcp -s 10.0.0.0/24 --dport 139 -j ACCEPT

iptables -A INPUT -i eth1 -p udp -m multiport --dports 53 -j ACCEPT

iptables -A INPUT -p tcp --dport 1723 -j ACCEPT

iptables -A INPUT -p gre -j ACCEPT

iptables -A INPUT -s 192.168.0.0/24 -p tcp -m state ESTABLISHED,RELATED -j ACCEPT

iptables -A INPUT -i ppp0 -p tcp --syn -m connlimit --connlimit-above 15 -j DROP

iptables -A INPUT -p icmp -j DROP

iptables -t nat -A POSTROUTING -o ppp0 -s 10.10.0.0/24 -j MASQUERADE

iptables -N syn-flood

iptables -A INPUT -p tcp --syn -j syn-flood

iptables -I syn-flood -p tcp -m limit --limit 3/s --limit-burst 6 -j RETURN

iptables -A syn-flood -j REJECT

iptables -P FORWARD DROP

iptables -A FORWARD -p tcp -s 10.10.0.0/24 -m multiport --dports 80,110,21,25,1723 -j ACCEPT

iptables -A FORWARD -p udp -s 10.10.0.0/24 --dport 53 -j ACCEPT

iptables -A FORWARD -p gre -s 10.10.0.0/24 -j ACCEPT

iptables -A FORWARD -p icmp -s 10.10.0.0/24 -j ACCEPT

iptables -I FORWARD -p udp --dport 53 -m string --string “TENCENT” -m time --timestart 8:15 --timestop 12:30 -days Mon,Tue,Web,Thu,Fri, Sat -j DROP

iptables -I FORWARD -p udp --dport 53 -m string --string “tencent” -m time --timestart 8:15 --timestop 12:30 -days Mon,Tue,Web,Thu,Fri, Sat -j DROP

iptables -I FORWARD -p udp --dport 53 -m string --string “qq.com” -m time --timestart 8:15 --timestop 12:30 -days Mon,Tue,Web,Thu,Fri, Sat -j DROP

iptables -I FORWARD -s 10.10.0.0/24 -m string --string “ay200.net” -j DROP

iptables -I FORWARD -s 10.10.0.0/24 -m string --string “eroticisim” -j DROP

sysctl -w net.ipv4.for\_ward=1 &> /dev/null

sysctl -w net.ipv4.tcp\_syncookies=1 &> /dev/null

#管理员一定允许通过

iptables -I INPUT -s 10.10.0.50 -j ACCEPT

iptables -I FORWARD -s 10.10.0.50 -j ACCEPT

1. 总结

介绍iptables的原理规则 四表五链

多场景的iptables的应用

Iptables的NAT模式 SNAT DNAT

Iptables中的防止CC攻击模块的介绍