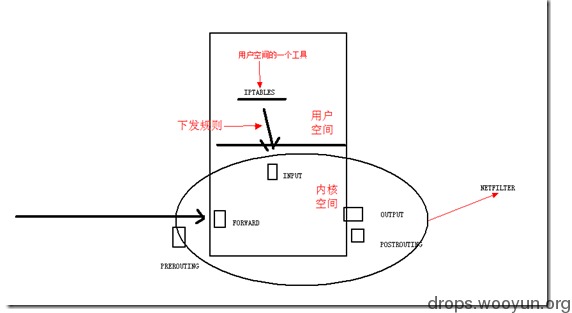
0x00 iptables介绍

linux的包过滤功能，即linux防火墙，它由netfilter 和 iptables 两个组件组成。

netfilter 组件也称为内核空间，是内核的一部分，由一些信息包过滤表组成，这些表包含内核用来控制信息包过滤处理的规则集。

iptables 组件是一种工具，也称为用户空间，它使插入、修改和除去信息包过滤表中的规则变得容易。

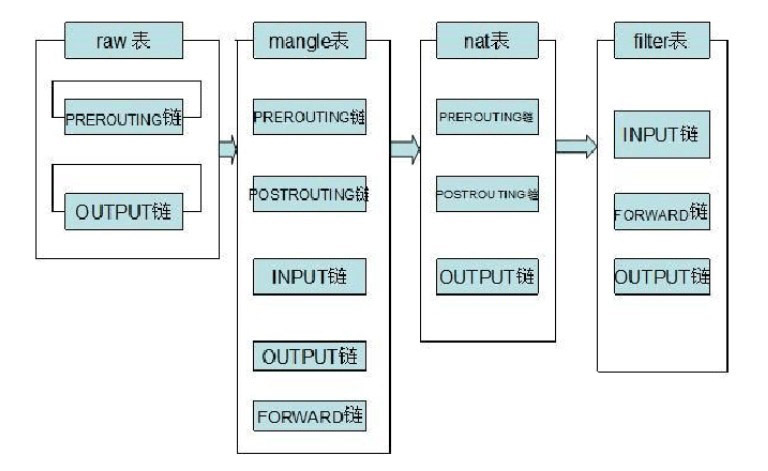


0x01 iptables的结构

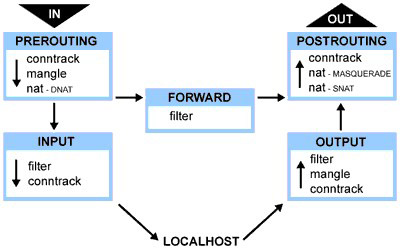
iptables的结构：

iptables -> Tables -> Chains -> Rules

简单地讲，tables由chains组成，而chains又由rules组成。iptables 默认有四个表Filter, NAT, Mangle, Raw，其对于的链如下图。



0x02 iptables工作流程



0x03 filter表详解

1. 在iptables中，filter表起过滤数据包的功能，它具有以下三种内建链：

INPUT链 – 处理来自外部的数据。

OUTPUT链 – 处理向外发送的数据。

FORWARD链 – 将数据转发到本机的其他网卡设备上。

2. 数据流向场景

访问本机：在INPUT链上做过滤

本机访问外部：在OUTPUT链上做过滤

通过本机访问其他主机:在FORWARD链上做过滤

3. Iptables基本操作

启动iptables：service iptables start

关闭iptables：service iptables stop

重启iptables：service iptables restart

查看iptables状态：service iptables status

保存iptables配置：service iptables save

Iptables服务配置文件：/etc/sysconfig/iptables-config

Iptables规则保存文件：/etc/sysconfig/iptables

打开iptables转发：echo "1"> /proc/sys/net/ipv4/ip\_forward

0x04 iptables命令参考

命令：

iptables [ -t 表名] 命令选项 [链名] [条件匹配] [-j 目标动作或跳转]

1. 表名

表名：Filter, NAT, Mangle, Raw

起包过滤功能的为表Filter，可以不填，不填默认为Filter

2. 命令选项

| **选项名** | **功能及特点** |
| --- | --- |
| -A | 在指定链的末尾添加（--append）一条新的规则 |
| -D | 删除（--delete）指定链中的某一条规则，按规则序号或内容确定要删除的规则 |
| -I | 在指定链中插入（--insert）一条新的规则，默认在链的开头插入 |
| -R | 修改、替换（--replace）指定链中的一条规则，按规则序号或内容确定 |
| -L | 列出（--list）指定链中的所有的规则进行查看，默认列出表中所有链的内容 |
| -F | 清空（--flush）指定链中的所有规则，默认清空表中所有链的内容 |
| -N | 新建（--new-chain）一条用户自己定义的规则链 |
| -X | 删除指定表中用户自定义的规则链（--delete-chain） |
| -P | 设置指定链的默认策略（--policy） |
| -n | 用数字形式（--numeric）显示输出结果，若显示主机的 IP地址而不是主机名 |
| -P | 设置指定链的默认策略（--policy） |
| -v | 查看规则列表时显示详细（--verbose）的信息 |
| -V | 查看iptables命令工具的版本（--Version）信息 |
| -h | 查看命令帮助信息（--help） |
| --line-number | 查看规则列表时，同时显示规则在链中的顺序号 |

3. 链名

可以根据数据流向来确定具体使用哪个链，在Filter中的使用情况如下：

INPUT链 – 处理来自外部的数据。

OUTPUT链 – 处理向外发送的数据。

FORWARD链 – 将数据转发到本机的其他网卡设备上。

4. 条件匹配

条件匹配分为基本匹配和扩展匹配，拓展匹配又分为隐式扩展和显示扩展。

a)基本匹配包括：

| **匹配参数** | **说明** |
| --- | --- |
| -p | 指定规则协议，如tcp, udp,icmp等，可以使用all来指定所有协议 |
| -s | 指定数据包的源地址参数，可以使IP地址、网络地址、主机名 |
| -d | 指定目的地址 |
| -i | 输入接口 |
| -o | 输出接口 |

b)隐式扩展包括：

隐含扩展条件需包含

扩展项  
说明

-m tcp

-p tcp

--sport

源端口

--dport

目标端口

--tcp-flags

示例（SYN,ACK,RST,FIN SYN）

--syn

第一次握手

-m udp

-p udp

--sport

源端口

--dport

目标端口

-m icmp

-p icmp

--icmp-type

8:echo-request  0:echo-reply

c)常用显式扩展

显式扩展条件

扩展项

说明

-m state

--state

用于实现连接的状态检测

NEW,ESTABLISHED,RELATED,INVALID

-m multiport

--source-ports

多个源端口

--destination-ports

多个目的端口

--ports

源和目的端口

-m limit

--limit

速率(如3/minute 表示每分钟3个数据包)

--limit -burst

峰值速率(如100 最大不能超过100个数据包)

-m connlimit

--connlimit-above n

多于n个表示满足条件取反要在选项前加!

-m iprange

--src-range ip-ip

源ip范围

--dst-range ip-ip

目的ip范围

-m mac

--mac-source

mac地址限制

-m string

--algo [bm|kmp]

匹配算法

--string “Pattern”

要匹配的字符串

-m recent

--name

设定列表名称，默认为DEFAULT

--rsource

源地址，此为默认

--rdest

目的地址

--set

添加源地址的包到列表中

--update

每次建立连接都更新列表

--rcheck

检查地址是否在列表

--seconds

指定时间内，必须与—rcheck或—update同时使用

--hitcount

命中次数，必须与—rcheck或—update同时使用

--remove

在列表种删除相应地址

5. 目标值

数据包控制方式包括四种为：

ACCEPT：允许数据包通过。

DROP：直接丢弃数据包，不给出任何回应信息。

REJECT：拒绝数据包通过，必须时会给数据发送端一个响应信息。

LOG：在/var/log/messages 文件中记录日志信息，然后将数据包传递给下一条规则。

QUEUE：防火墙将数据包移交到用户空间

RETURN：防火墙停止执行当前链中的后续Rules，并返回到调用链(the calling chain)

0x05 Iptables常见命令

a) 1. 删除iptables现有规则

iptables –F

b) 2. 查看iptables规则

iptables –L（iptables –L –v -n）

c) 3. 增加一条规则到最后

iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

d) 4.添加一条规则到指定位置

iptables -I INPUT 2 -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

e) 5.  删除一条规则

iptabels -D INPUT 2

f) 6.修改一条规则

iptables -R INPUT 3 -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

g) 7. 设置默认策略

iptables -P INPUT DROP

h) 8.允许远程主机进行SSH连接

iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

i) 9.允许本地主机进行SSH连接

iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INTPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

j) 10.允许HTTP请求

iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

k) 11.限制ping 192.168.146.3主机的数据包数，平均2/s个，最多不能超过3个

iptables -A INPUT -i eth0 -d 192.168.146.3 -p icmp --icmp-type 8 -m limit --limit 2/second --limit-burst 3 -j ACCEPT

l) 12.限制SSH连接速率(默认策略是DROP)

iptables -I INPUT 1 -p tcp --dport 22 -d 192.168.146.3 -m state --state ESTABLISHED -j ACCEPT

iptables -I INPUT 2 -p tcp --dport 22 -d 192.168.146.3 -m limit --limit 2/minute --limit-burst 2 -m state --state NEW -j ACCEPT

0x06 如何正确配置iptables

a) 1. 删除现有规则

iptables -F

b) 2.  配置默认链策略

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT DROP

c) 3. 允许远程主机进行SSH连接

iptables -A INPUT -i eth0 -p tcp –dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp –sport 22 -m state –state ESTABLISHED -j ACCEPT

d) 4. 允许本地主机进行SSH连接

iptables -A OUTPUT -o eth0 -p tcp –dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -i eth0 -p tcp –sport 22 -m state –state ESTABLISHED -j ACCEPT

e) 5. 允许HTTP请求

iptables -A INPUT -i eth0 -p tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT

0x07 使用iptables抵抗常见攻击

1.防止syn攻击

思路一：限制syn的请求速度（这个方式需要调节一个合理的速度值，不然会影响正常用户的请求）

iptables -N syn-flood

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

iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN

iptables -A syn-flood -j DROP

思路二：限制单个ip的最大syn连接数

iptables –A INPUT –i eth0 –p tcp --syn -m connlimit --connlimit-above 15 -j DROP

2. 防止DOS攻击

利用recent模块抵御DOS攻击

iptables -I INPUT -p tcp -dport 22 -m connlimit --connlimit-above 3 -j DROP

单个IP最多连接3个会话

iptables -I INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH

只要是新的连接请求，就把它加入到SSH列表中

Iptables -I INPUT -p tcp --dport 22 -m state NEW -m recent --update --seconds 300 --hitcount 3 --name SSH -j DROP

5分钟内你的尝试次数达到3次，就拒绝提供SSH列表中的这个IP服务。被限制5分钟后即可恢复访问。

3. 防止单个ip访问量过大

iptables -I INPUT -p tcp --dport 80 -m connlimit --connlimit-above 30 -j DROP

4. 木马反弹

iptables –A OUTPUT –m state --state NEW –j DROP

5. 防止ping攻击

iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/m -j ACCEPT