**防火墙配置**

一 简介

防火墙有软硬件之分，但主要功能还是一句策略对外部请求进行过滤。

1 功能：

分割内网和外网

划分要被保护的服务器

2 分类

防火墙会监控每一个数据包并进行判断其是否有相应的匹配策略规则，直到满足一条规则为止，而防火墙规则策略可以是：

1. 基于来源请求地址
2. 请求动作
3. 请求协议

最终让合法的用户请求流入到内网中，其余的均被抛弃。

3 防火墙限制

1）防火墙不能有效防止病毒和木马

2）防火墙一般不设定对内部访问规则，所以对内部攻击无效

4 linux常见防火墙

2.4---- iptables

2.2 ipchains

注意：其实上面的两种都不是真正的防火墙。他们都是用来定义防火墙规则功能的防火墙管理软件，将定义好的规则交到内核中的netfilter(网络过滤器)来读取，从而实现防火墙的功能。

二 iptables防火墙

1 结构

表-------链--------规则

1. 规则与链

在iptables命令中设置数据过滤或处理数据包的策略叫做规则。

将多个规则合成一个链。

1. iptables命令中常见的控制类型
2. ACCEPT：允许通过
3. LOG:记录日志信息，然后传给下一条规则继续匹配
4. REJECT:拒绝通过，必要时给出提示
5. DROP:直接丢弃，不给出任何回应

注意：REJECT和DROP的操作都是将数据包拒绝，但是REJECT会给出一条回复信息。

2 规则链的分类

依据规则链处理数据包的位置不同进行分类：

1. PREROUTING：在进行路由选择前处理数据包
2. INPUT：处理入站的数据包
3. OUTPUT：处理出站的数据包
4. FORWARD：处理转发的数据包
5. POSTROUTING：在进行路由选择后处理数据包

3 规则表

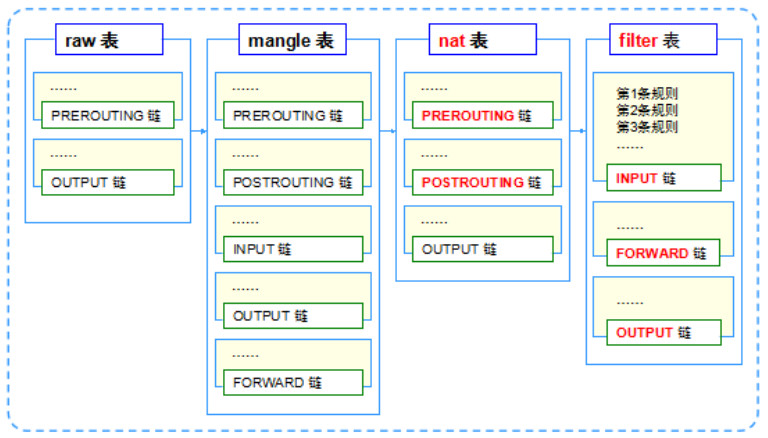
Iptables中的规则表是用于容纳规则链的，规则表默认是允许状态的，那么规则链就是设置被禁止的规则。反之，如果规则表示禁止状态的，那么规则链就是设置允许状态的。即防火墙的原则：

允许所有，逐个拒绝

拒绝所有，逐个允许

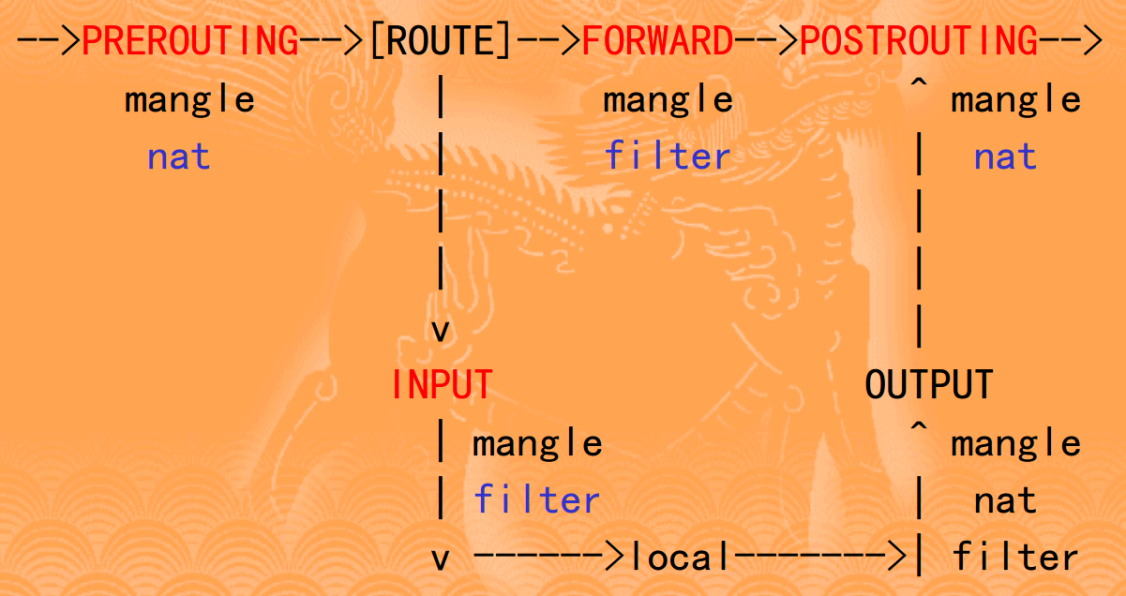
1. raw表：确认是否对改数据包进行状态跟踪
2. mangle表：为数据设置标记
3. nat表：修改数据包中的源、目标IP地址或端口
4. filter表：确定是否放行该数据包（过滤）

规则表的先后顺序：raw->mangle->nat->filter



4 规则链的先后顺序：

1. 入站顺序：PREROUTING->INPUT
2. 出站顺序：OUTPUT->POSTROUTING
3. 转发顺序：PREROUTING->FORWAED->POSTROUTING



5 注意事项

1. 没有指定规则表则默认指filter表
2. 不指定规则链则指表内所有的规则链
3. 在规则链中匹配规则时会依次检查，匹配即停止（LOG规则例外），若没匹配项则按链的默认状态处理。

三 iptables基础语法

1. iptables命令用于管理防火墙的规则策略格式为：

iptable [-t 表名] 选项 [链名][条件][-j 控制类型]

|  |  |
| --- | --- |
| 参数 | 作用 |
| -P | 设置默认策略：iptables -P INPUT (DROP | ACCEPT) |
| -F | 清空规则链 |
| -L | 查看规则链 |
| -A | 在规则链的末尾加入新规则 |
| -I num | 在规则链的头部加入新规则 |
| -D num | 删除某一条规则 |
| -s | 匹配来源地址IP/MASK，加叹号‘！’表示除这个IP外 |
| -d | 匹配目标地址 |
| -i 网卡名称 | 匹配从这块网卡流入的数据 |
| -o 网卡名称 | 匹配从这块网卡流出的数据 |
| -p | 匹配协议，如tcp、udp、icmp |
| -dport num | 匹配目标端口号 |
| -sport num | 匹配来源端口号 |
| -X | 清除自定义链 |
| -Z | 清除所有链统计 |
| -n | 以端口和ip显示 |

iptables -t nat -L

查看nat表中规则

iptables -L

查看filter表中规则

2 定义默认策略

iptables -t 表名 -P 链名 ACCEPT|DROP

-P（大） 定义默认策略

iptables -t filter -P INPUT DROP

注意：不要把自己踢出服务器，应该最后设定。

3 ip和网卡接口设置

iptables [-AI 链] [-io 网卡接口] [-p 协议] [-s 源IP] [-d 目标ip] -j 动作

-A 追加链规则 在链规则最后加入此规则

-I INPUT 2 把此规则插入到INPUT链，变成第二条规则

-D 链 条数 删除指定链的指定条数防火墙

iptables -D INPUT 2 产出input链第二条规则

-i eth0 指定进入接口 要在INPUT链上定义

-o eth0 指定传出接口 要在OUTPUT链上定义

-p 协议 tcp udp icmp all

-j 动作 ACCEPT DROP

iptables -A 　INPUT -i lo -j ACCEPT

允许本机回环网卡通信，在INPUT链

iptables -A INPUT -i eth0 -s 192.168.140.254 -j ACCEPT

允许254进入eth0

iptables -A INPUT -i eth0 -s 192.168.140.0/24 -j DROP

拒绝140网段访问

4 设定端口访问

iptables -A INPUT -i eth0 -p all -s 源ip --sport 源端口 -d 目标ip --dport 目标端口 -j 动作

iptables -A INPUT -i eth0 -p tcp -s 192.168.140.0/24 --dport 22 -j DROP

iptables -A INPUT -i eth0 -p tcp -s 192.168.140.0/24 --dport 137:139 -j ACCEPT

指定端口时，协议不能用all，要指定确切协议

5 模块调用

1）

-m 模块名 模块选项 加载iptables功能模块

-m state --state ESTABLISHED,RELATED

iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

state 状态模块 常见状态 ESTABLISHED 联机成功的状态 RELATED 返回包状态

2）

-m mac --mac-source 按照mac地址限制访问

iptables -A INPUT -m mac --mac-source aa:bb:cc:dd:ee:ff -j DROP

Windows查看mac地址：ipconfig/all

拒绝某mac访问

3）

-m string --string "想要匹配的数据包中字串"

iptables -A FORWARD -p udp --dport 53 -m string --string "tencent" --algo kmp -j DROP

通过dns拒绝qq登录

--algo 选择模式匹配策略，支持KMP和BM两种字符串搜索算法，任意指定一个即可

6 简易防火墙

iptables -F

iptables -A INPUT -i lo -j ACCEPT

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

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

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

iptables -A INPUT -p tcp --dport 873 -j ACCEPT

iptables -A INPUT -p tcp --dport 139 -j ACCEPT

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

iptables -P INPUT DROP

7 防火墙服务开机自启动

chkconfig iptables on

8 防火墙规则开启自启动

1） service iptables save

会把规则保存到 /etc/sysconfig/iptables文件中，重启会自动读取

2） 手工写防火墙脚本

如 vi /root/iptables.rule

iptables -F

iptables -A INPUT -i lo -j ACCEPT

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

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

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

iptables -A INPUT -p tcp --dport 873 -j ACCEPT

iptables -A INPUT -p tcp --dport 139 -j ACCEPT

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

iptables -P INPUT DROP

赋予执行权限 chmod 755 /root/iptables.rule

开机运行 vi /etc/rc.local

写入 /root/iptables.rule