第十八章：iptables防火墙应用

一、iptables防火墙基础；

二、iptables规则编写；

三、实战演练；

一、iptables防火墙基础；

1.概述：保护内部主机和内部网络的安全，通过过滤的方式对网络层的ip地址和端口进行处理；

2.了解防火墙：

硬件防火墙：ASA

软件防火墙：iptables（linux平台）、ISA（windows自带的）

3.iptables防火墙结构：

netfilter内核模块、iptables用户工具、firewall用户工具

4.iptables的表：按照不同功能来划分；

raw（状态跟踪）、mangle（标记）、nat（修改）、filter（过滤）

raw：主要是为了提高效率使用的，raw本身的含义是指“原生的”、“未经过加工 的”，符合raw表所对应规则的数据包将会跳过一些检查，这样就可以提高效率；

mangle：mangle表的规则可以对数据包进行修改，比如修改ttl值等；

nat：进行源地址或目标地址修改转换；

filter：通过过滤数据包的ip地址、mac地址、协议、端口，对数据包进行控制；

5.iptables规则链：根据不同时机来划分链，在链中存放规则；

INPUT（入站）、OUTPUT（出站）、FORWARD（转发）、PREROUTING（路由前）、POSTROUTING（路由后）

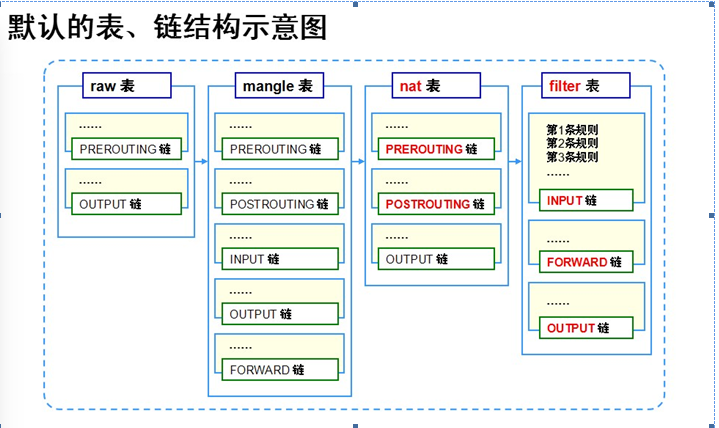
6.表中默认包含链：

raw：PREROUTING、OUTPUT

mangle：PREROUTING、INPUT、FORWARD、OUTPUT、POSTROUTING

nat： PREROUTING、POSTROUTING、OUTPUT

filter：INPUT、FORWARD、OUTPUT



总结：表相当于内核空间的一个容器，在表容器中又包含不同的链，在链中包含不同的规则；

7.iptables匹配流程：（根据数据流的方向确定匹配顺序）

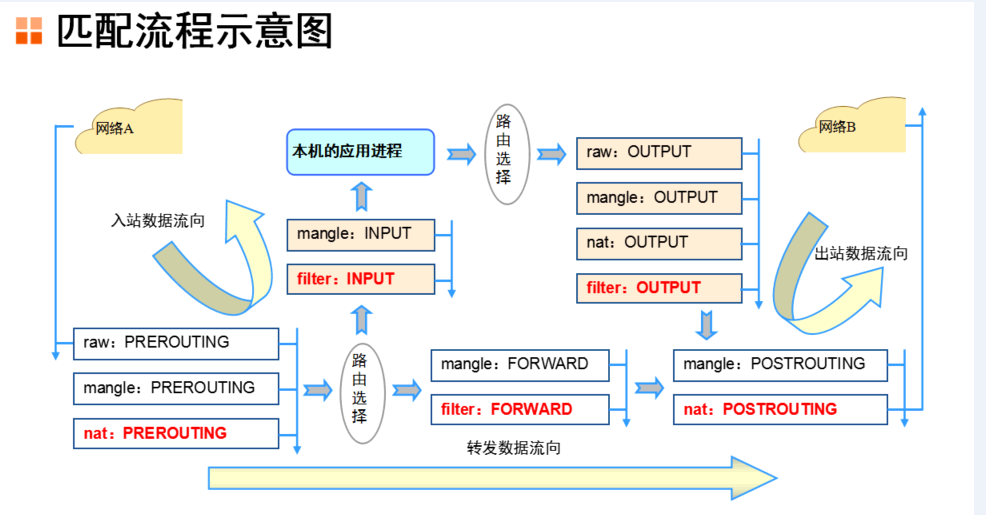
链：入站数据流向：PREROUTING、INPUT

出站数据流向：OUTPUT、POSTROUTING

转发数据流向：PREROUTING、FORWARD、POSTROUTING

表：raw--mangle--nat--filter

总结：链内规则匹配顺序：从上到下、匹配即停止、未匹配使用默认规则；



二、编写iptables规则：

语法：iptables -t 表名 选项 链名 条件 -j 动作

1.编写规则语法注意：

省略表名，默认表示filter表，省略链名，表示表内所有链；

除非设置默认规则，否则必须设置匹配的规则；

选项、链名、动作必须大写，其他小写；

2.动作：对匹配的条件进行处理；

ACCEPT：允许

DROP：丢弃

REJECT：拒绝

LOG：日志

3.选项：对链中的规则进行增删改查操作；

a.增加：-A链的末尾添加、-I 链的指定位置添加，需要指定序号（若不指定，默认作为第一条规则），例：-I INPUT 2

b.删除：-D 删除一条规则，-F清空链内所有规则，例：iptables -D 链名 2

c.查看：-L -n 查看规则，-L -n -v 查看更详细的信息，-L -n --line-number显示规则的序号（大写为选项，后边小写为子选项， 子选项需要跟在链名的后边）

d.设置默认规则：-P 链名 DROP或ACCEPT

4.匹配条件：

a.通用匹配条件：

-p 协议 ##常用的协议ICMP、TCP、UDP协议；

-s 源地址 ##控制源地址访问，网段书写格式：192.168.1.0/24

-d 目的地址 ##控制目的地址访问

-i 入站网卡名称 ##控制传输数据的入站网卡

-o 出站网卡名称 ##控制传输数据的出站网卡

注：编写规则时，需要判断主机数据的流向，如INPUT链只能用-i入站网卡；

b.隐含匹配条件：

端口：-p 协议 --dport 目的端口

-p 协议 -sport 源端口

c.显式匹配条件：

多端口：-m multiport -p tcp或udp --dports 端口号 ##指定多个端口，若连续端口11:22，若不连续端口11,22

mac地址：-m mac --mac-source MAC地址 ##MAC地址中间用：隔开，指定的mac地址为源地址

ip地址范围：-m iprange --src-range 192.168.1.1-192.168.1.10 ##指定的ip地址范围是源地址

数据包的状态：-m state --state NEW,ESTABLISHED,RELATED ##三个选项分别表示，新建，已经建立的连接，已经相关，例：默认规则为DROP并且无允许ssh22号端口，但是允许已经建立的连接，ssh不会断开，ss命令查看当前的连接；

三、实战演练：

[root@lwh ~]# /etc/init.d/iptables stop ##清空防火墙规则；

iptables：将链设置为政策 ACCEPT：filter [确定]

iptables：清除防火墙规则： [确定]

iptables：正在卸载模块： [确定]

[root@lwh ~]# iptables -A INPUT -i lo -j ACCEPT ##允许本地网卡所有访问

[root@lwh ~]# iptables -A INPUT -s 192.168.100.1-p tcp -m multiport --dports 80,443,20,21,22,25,45000:50000 -j ACCEPT ##设置开启的端口

[root@lwh ~]# iptables -A INPUT -m mac --mac-source 00:0C:29:D9:32:C9 -p icmp -j ACCEPT ##设置此mac地址可以ping访问本主机

[root@lwh ~]# iptables -A INPUT -m iprange --src-range 192.168.100.1-192.168.100.10 -d 192.168.100.150 -p icmp -j ACCEPT ##设置此ip地址范围可以访问ping此主机

[root@lwh ~]# iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT ##设置数据的状态，本机可以访问别的主机

[root@lwh ~]# iptables -P INPUT DROP ##设置INPUT入站链的默认规则为丢弃

[root@lwh ~]# iptables -P FORWARD DROP ##设置FORWARD转发链的默认规则为丢弃

[root@lwh ~]# /etc/init.d/iptables save ##保存防火墙配置到/etc/sysconfig/iptables文件中，每次开机都会加载这个文件中的防火墙规则

iptables：将防火墙规则保存到 /etc/sysconfig/iptables： [确定]

[root@lwh ~]# chkconfig iptables on ##设置开机启动防火墙