防火墙

iptables的表、链结构

raw 表、(状态跟踪表)

mangle表、(包标记表)

nat 表、(地址转换表)

filter 表、(过滤表)

ACCEPT:允许通过/放行

DROP:直接丢弃,不给任何回应

REJECT:拒绝通过,必要时会给出提示

LOG:记录日志,然后传给下一条规则

INPUT-------------------进入防火墙的包

OUTPUT----------------从防火墙出去的包

FORWARD-------------经过防火墙的包

POSTROUTING-------路由后处理

PREROUTING----------路由前处理

常用管理选项

添加规则 -A 在链的末尾追加一条规则

-I 在链的开头(或指定序号)插入一条规则

查看规则 -L 列出所有的规则条目

-n 以数字形式显示地址、端口信息

--line-numbers 查看规则时,显示规则的序号

删除规则 -D 删除链内指定的序号(或内容)的一条规则

-F 删除所有规则

默认策略 -P 未指定的链设置默认规则

网络防火墙环境准备

[root@b ~]# iptables -t filter -P INPUT ACCEPT

[root@b ~]# iptables -t filter -F

[root@b ~]# iptables-save > /etc/sysconfig/iptables

打开路由转发功能

[root@b ~]# echo 'net.ipv4.ip\_forward=1' >> /etc/sysctl.conf

[root@b ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward

查看网关

[root@b ~]# route -n

给a和c添加网关(命令行临时有效)

[root@a ~]# route add default gw 192.168.4.51

[root@c ~]# route add default gw 192.168.2.51

删除网关

[root@c ~]# route del default gw 192.168.2.51

查看规则表

[root@b ~]# iptables -nL INPUT

[root@b ~]# iptables -nL INPUT --line-numbers

[root@b ~]# iptables -t filter -nL FORWARD --line-numbers

a ping c b主机抓包

[root@a ~]# ping 192.168.2.52

[root@b ~]# tcpdump -i eth0 -p icmp

定义防火墙规则默认模式drop

[root@b ~]# iptables -t filter -P FORWARD DROP

[root@a ~]# rpm -q httpd || yum -y install httpd

[root@a ~]# systemctl start httpd

[root@a ~]# echo A > /var/www/html/test.html

B主机放行目标访问80端口的,放行80端口回复目标的,

[root@b ~]# iptables -t filter -A FORWARD -p tcp --dport 80 -j ACCEPT

[root@b ~]# iptables -t filter -A FORWARD -p tcp --sport 80 -j ACCEPT

[root@b ~]# iptables-save > /etc/sysconfig/iptables

测试c访问a(成功看到A)

[root@c ~]# curl http://192.168.4.50/test.html

A

B主机放行22端口,访问和回复(a可以ssh c)

[root@b ~]# iptables -t filter -A FORWARD -p tcp --dport 22 -j ACCEPT

[root@b ~]# iptables -t filter -A FORWARD -p tcp --sport 22 -j ACCEPT

[root@a ~]# ssh -X 192.168.2.52

扩展匹配

MAC地址匹配

[root@b ~]# arp -n //查看要禁用的MAC地址

[root@b ~]# iptables -t filter -I FORWARD 3 -p icmp -m mac --mac-source 52:54:00:cf:4d:b7 -j DROP

[root@c ~]# ping 192.168.4.50 //c主机ping不通a主机

多端口匹配

[root@b ~]# iptables -t filter -F FORWARD //清空所有规则

[root@b ~]# iptables -t filter -A FORWARD -p tcp -m multiport --dport 22,80 -j ACCEPT //目标端口22和80

[root@b ~]# iptables -t filter -A FORWARD -p tcp -m multiport --sport 22,80 -j ACCEPT //源端口22和80

[root@b ~]# iptables-save > /etc/sysconfig/iptables //保存配置

放行icmp协议,可以ping

[root@b ~]# iptables -t filter -A FORWARD -p icmp -j ACCEPT

IP范围匹配

[root@b ~]# iptables -t filter -A FORWARD -p icmp -m iprange --src-range 192.168.2.50-192.168.2.60 -j DROP

NAT转换原理

SNAT源地址转换

环境准备:

删除规则为默认规则

[root@b ~]# iptables -t filter -P FORWARD ACCEPT

[root@b ~]# iptables -t filter -F

[root@b ~]# iptables-save > /etc/sysconfig/iptables

删除网关

[root@a ~]# route del default gw 192.168.4.51

[root@a ~]# route -n

[root@b ~]# iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -p tcp --dport 80 -j SNAT --to-source 192.168.4.51

[root@b ~]# iptables -t nat -nL POSTROUTING --line-numbers

[root@b ~]# iptables-save > /etc/sysconfig/iptables

c主机可以访问a主机http

[root@c ~]# curl http://192.168.4.50/test.html

A

查看a主机的访问日志就知道谁在访问

[root@a ~]# tailf /etc/httpd/logs/access\_log

192.168.4.51 - - [31/Jul/2019:16:59:10 +0800] "GET /test.html HTTP/1.1" 200 2 "-" "curl/7.29.0"

//显示是4.51主机访问a主机,而不是2.52主机访问的

公网地址是服务商动态分配,定义防火墙规则

地址伪装策略 (MASQUERADE)

[root@b ~]# iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -p tcp --dport 80 -o eth0 -j MASQUERADE