Iptables表和链

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  | | --- | | 应用层 |  |  | | --- | | TCP UDP |  |  | | --- | | 路由判决 |  |  | | --- | | 路由判决 |   IPNPUT链 OUTPUT链    FORWARD链    POSTROUTING链 POSTROUTING链 |

Linux服务器双网卡路由器

应用层

传输层

网络层

物理层和数据链路层 物理层和数据链路层

Filter表：INPUT链 OUTPUT链 FORWARD链

NAT表 ：PREROUTING链 OUTPUT链 POSTROUTING链

mangle表：PREROUTING链 FORWARD链 INPUT链 OUTPUT链 POSTROUTING链

iptables

iptables –t table 命令 chain rules –j target

table:filter nat mangle, 默认filter

命令

-P 或 --policy定义默认策略

-A 或 --append 在规则列表的最后一条增加一条规则

-I 或 –insert 在指定的位置插入一条规则，如果不指定默认第一条

#iptables –t filter –I INPUT 3 –p icmp –j DROP

-D 或 –delete 删除一条规则

#iptables –t filter –D INPUT 1

-R 或 –replace 替换规则列表中的规则

#iptables –L

#iptables –filter –R INPUT 2 –p icmp –j DROP 替换

-F 或 –flush 删除表中所有规则

#iptables –t filter –F INPUT #指定删除表中一个链的规则，不指定就删除这个表中所有链的规则

Iptables匹配选项

-i 或 –in-interface 指定数据包从哪个网络接口进入

-o 或 --out-interface 指定数据包从那块网卡接口出去

-p 或 --protocal 协议类型，如TCP,UDP和ICMP等

-s 或 --source 指定数据包匹配的源地址

-d 或 --destination 指定数据包匹配的目标地址

--sport 指定数据包匹配的源端口号，可以使用“起始端口号：结束端口号”的格式指定一个范围端口

--dport指定数据包匹配的目标端口号，可以使用“起始端口号：结束端口号”的格式指定一个范围端口

xp

win 2003

LinuxServer

Linux

Router2

Linux

Router1

在Linux Router1上配置，使xp无法远程win 2003

#iptables –t filter –I FORWARD –p tcp –s 192.168.80.123/32 –d 192.168.123.123/32 --dport 3389 –j DROP

扩展的匹配选项

参数 –m state

基于状态检测的包过滤，指定检测那种状态

--state {NEW,ESTABLISHED,INVALID,RELATED}

INVALID 表示该封装的连接编号（session ID）无法辨识或编号不正确

ESTABLISHED 表示该封包属于某个已经建立的连接

NEW 表示该封包要起始一个连接（重设连接或将连接重导向）

RELATED 表示该封包是属于某个已经建立的连接，所建立的新连接。例如：FTP-DATA连接必定是属于某个FTP连接

范例：iptables –A INPUT –m state --state RELATED,ESTABLISHED –j ACCEPT

server

xp

Linux Router

单方向建立会话 保护服务器安全

#iptables –t filter –I FORWARD –s 192.168.10.0/24 –d 192.168.80.0/24 –m state --state NEW –j DROP

TCP 80 NEW

Linux web server

使服务器不主动与外界建立会话

#iptables –t filter -I OUTPUT –m state --state NEW –j DROP

参数 –m icmp --icmp-type 实现单方向的ping通

icmp有两种常用类型的数据包即icmp-type:echo-request和echo-reply，PC1 ping PC2，PC1发出去的是echo-request，PC2返回的是echo-reply,通过控制这两种数据包即可控制单方向的ping通

Linux

Xp

2003

192.168.80.123 192.168.10.123

禁止192.168.10.0/24ping通192.168.80.0/24

允许192.168.80.0/24ping通192.168.10.0/24

#iptables –t filter –I FORWARD –s 192.168.10.0/24 –d 192.168.80.0/24 –p icmp –m icmp --icmp-type echo-request –j DROP

Xp

Linux

不允许其他ping通linux服务器，但允许linux服务器ping通其他计算机

#iptables –t filter –I INPUT –p icmp –m icmp --icmp-type echo-request –j DROP

参数 –m multiport {--sport --dport --port} 实现端口访问控制

#iptables –t filter –I FORWARD –p tcp –s 192.168.80.0/24 –d 192.168.10.0/24 –m multiport --dport 1:1024,3389 –j DROP

参数 –m iprange {--src-range --dst-range} 实现IP地址范围访问控制

禁止192.168.80.1-100地址段访问192.168.10.0/24

#iptables –t filter –I FORWARD –m iprange --src-range 192.168.80.1-192.168.80.100 –j DROP

参数 -m connlimit --connlimit-above 限制最大连接数

只允许192.168.80.0/24使用远程桌面连接192.168.10.123/32最多两个会话。

#iptables –t filter –I FORWARD –s 192.168.80.0/24 –d 192.168.10.123/32 –p tcp --dport 3389 –m connlimt --connlimit-above 2 –j DROP

流量控制

参数 -m limit --limit 使用扩展选项限制网速（某段时间内平均流量）

192.168.10.0/24网段每秒钟向192.168.80.0/24发送的数据包不能超过300个，300\*1500=450 000=450k

#iptables –t filter –I FORWARD –s 192.168.10.0/24 –d 192.168.80.0/24 –m limit --limit 300/second –j ACCEPT

# iptables –t filter –A FORWARD –s 192.168.10.0/24 –d 192.168.80.0/24 –j ACCEPT

192.168.10.0/24网段每台计算机每秒钟向192.168.80.0/24发送的数据包不能超过300

for (i=2;i<254;i++)

do

iptables –I FORWARD –s 192.168.10.$i –j DROP

iptables –I FORWARD –s 192.168.10.$i –m limit --limit 300/sec --limit-burst 1000 –j ACCEPT

done

参数 --limit-burst 瞬时流量控制

--limit-burst一般与--limit结合使用，如何单独使用--limit-burst表示只允许这些通过

例：允许192.168.10.123/32 ping通192.168.80.123/32 4个包

#iptables –t filter –I FORWARD –s 192.168.10.123/32 –d 192.168.80.123/32 –p icmp –m limit --limit-burst 4 –j ACCEPT

#iptables –t filter –A FORWARD –s 192.168.10.123/32 –d 192.168.80.123/32 –p icmp –j DROP

#iptables –t filter –Z #清空iptables的计数器

保存和还原iptables设置

#/etc/rc.d/init.d/iptables save 将当前配置保存到配置文件（/etc/sysconfig/iptables）

#iptables-save > iptables.conf1 将当前配置保存到另外文件

#iptables-restore < iptables.conf1 导入

保护服务器安全

web服务器对internet开放80端口

SSH端口只允许192.168.10.123访问

#itptables –t filter –I INPUT –p tcp --dport 80 –j ACCEPT

#iptables –A INPUT –s 192.168.10.123/32 –p tcp --dport 22 –j ACCEPT

#iptables –P INPUT DROP

recent模块实现服务器网络安全

设定常用模块：

--name #设定列表名称，默认DEFAULT

--resource #源地址

--rdest #目的地址

--seconds #指定时间内

--hitcount #命中次数

--set #将地址添加进列表，并更新信息，包含地址加入的时间戳

--rcheck #检查地址是否在列表，以第一个匹配开始计算时间

--update #和rcheck类似，以最后一个匹配计算时间

--remove #在列表里删除相应地址，后跟列表名称

示例 1

SSH允许客户端60秒只能连接两次（针对暴力破解软件）

用来设置多次时间 几次 拒绝

#iptables –t filter –A INPUT –p tcp --dport 22 –m state --state NEW –m recent --name SSHPOOL --rcheck --seconds 60 --hitcount 2 –j DROP

连接计数

#iptables –t filter –A INPUT –p tcp --dport 22 –m state --state NEW –m recent --name SSHPOOL --set –j ACCEPT #将新建立的会话记录到SSHPOOL表中，并允许

已建立会话的连接允许

#iptables –t filter –A INPUT –m state --state ESTABLISHED –j ACCEPT

#iptables –P INPUT DROP

设置打开端口的钥匙

#iptables -t filter -I INPUT -p icmp -m icmp --icmp-type echo-request -m length --length 1078 -m recent --set --name sshopen -j ACCEPT

#iptables -t filter -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name sshopen --rcheck --seconds 60 --hitcount 10 -j DROP

#iptables -t filter -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name sshopen --rcheck --seconds 60 --hitcount 5 -j ACCEPT

# iptables -t filter -A INPUT -m state --state ESTABLISHED -j ACCEPT

#iptables -P INPUT DROP

(-p icmp --icmp-type等价于-p icmp –m icmp --icmp-type )

#iptables –A input –p icmp –m icmp --icmp echo-request –m length --length 1078 –m recent --set --name sshopen --rsource –j ACCEPT 将ping包源地址加入列表

#iptables –A input –p tcp --dport 22 –m state --state NEW–m recent --rcheck --seconds 60 --name sshopen --rsource –j ACCEPT 检查源地址，允许22端口

#iptables –A input –p icmp –m icmp --icmp echo-request –m length --length 1178 –m recent --remove --name sshopen --rsource –j ACCEPT 移除源地址

#iptables –A INPUT –m state --state ESTABLISHED –j ACCEPT

#iptables –P INPUT DROP