**LINUX防火墙iptables入门**

**IPTABLES****的优点：**

（1）有状态的防火墙

（2）完全的规则控制

（3）免费

**IPTABLES的缺点：**

（1）配置复杂

（2）维护难（大型的配置环境不建议使用，一般只用在简单的环境）

**IPTABLES的功能：**

（1）数据包的过滤

（2）数据转发

（3）限速

（4）防攻击

**IPTABLES的四表五链：**

（1）filer ：实现包过滤

（2）nat ：实现地址转换

（3）mangle：重构 修改

（4）raw：数据跟踪处理

规则表之间的优先级： raw---managle ---nat ---filer 先后处理的顺序

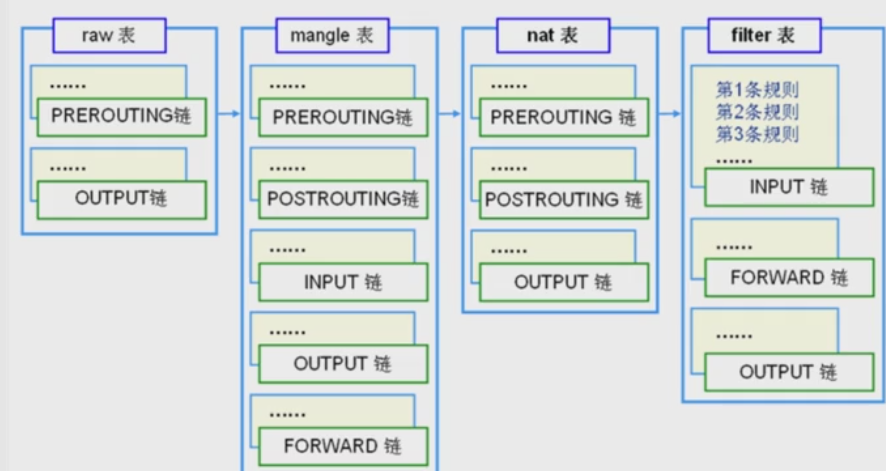
（1）PREROUTING

（2）POSTOUTING

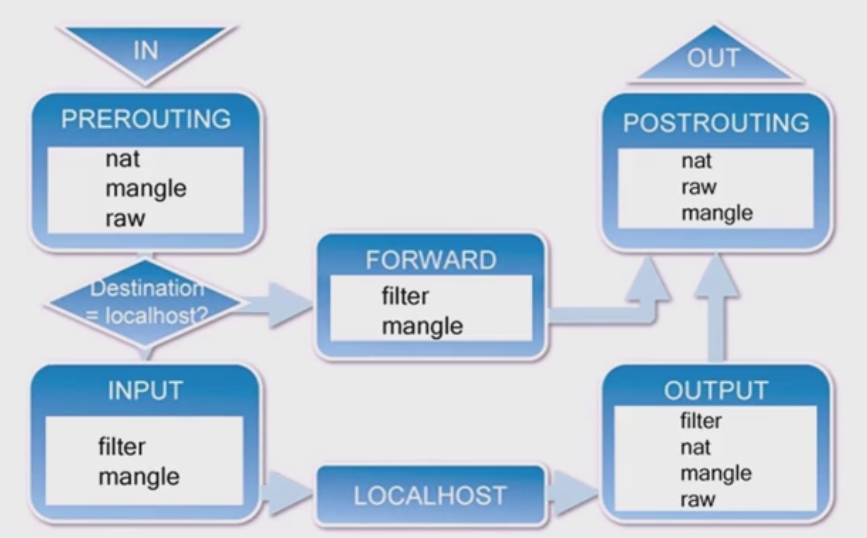
（3）INPUT

（4）OUTPUT

（5）FORWARD



当一个数据包进入iptables时首先进入PREROUTING链，包含此链的表有nat、managle、raw，然后判断目的地是哪里如果是本地进入INPUT链，包含此链的有filter、managle，之后进入OUTPUT链包含此链的有filter、nat、managle、raw最后进入POSTOUTING包含此链的有nat、raw、managle。直接进入转发FORWARD链包含此链的有filter、managle最后进入POSTOUTING。



**State连接状态：**

ESTABLISHED :只要数据包能够成功通过防火墙，那么之后的所有数据包状态都会是ESTABLSHED.

NEW:每条连接的第一条数据包。

RELATED:被动产生的数据包，访问外部服务器后返回的数据响应包为RELATED.

INVALID:状态不明的数据包，一般视为恶意的数据包并应该被丢弃。

**IPTABLES的配置与命令:**

1、 iptables的规则文件

[root@wudilinux sysconfig]# cat /etc/sysconfig/iptables

#Generated by iptables-save v1.3.5 on Tue May3 18:59:01 2016

\*filter

:INPUT DROP [69:4906]#默认规则drop 端口为69到4906的包

:FORWARD ACCEPT [0:0]#默认规则 端口不做限制

:OUTPUT ACCEPT [1298:137580]#默认规则 accept的端口为1298到137580

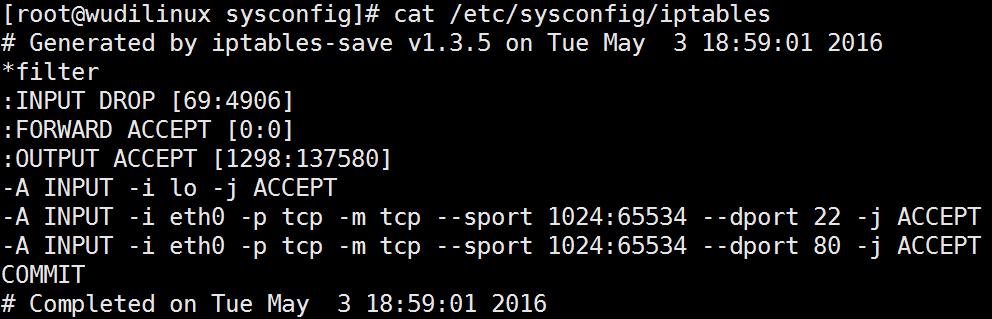
-A INPUT-i lo -j ACCEPT

-A INPUT-i eth0 -p tcp -m tcp --sport 1024:65534 --dport 22 -j ACCEPT

-A INPUT-i eth0 -p tcp -m tcp --sport 1024:65534 --dport 80 -j ACCEPT

COMMIT

# Completed on Tue May3 18:59:01 2016



2、 iptables的配置文件

[root@wudilinux sysconfig]# cat /etc/sysconfig/iptables-config

# Loadadditional iptables modules (nat helpers)

# Default: -none-

# Spaceseparated list of nat helpers (e.g. 'ip\_nat\_ftp ip\_nat\_irc'), which

# areloaded after the firewall rules are applied. Options for the helpers are

# storedin /etc/modprobe.conf.

IPTABLES\_MODULES="ip\_conntrack\_netbios\_ns"

# Unloadmodules on restart and stop

# Value: yes|no, default: yes

# Thisoption has to be 'yes' to get to a sane state for a firewall

# restartor stop. Only set to 'no' if there are problems unloading netfilter

#modules.

IPTABLES\_MODULES\_UNLOAD="yes"

# Savecurrent firewall rules on stop.

# Value: yes|no, default: no

# Savesall firewall rules to /etc/sysconfig/iptables if firewall gets stopped

# (e.g.on system shutdown).

IPTABLES\_SAVE\_ON\_STOP="no"

# Savecurrent firewall rules on restart.

# Value: yes|no, default: no

# Savesall firewall rules to /etc/sysconfig/iptables if firewall gets

#restarted.

IPTABLES\_SAVE\_ON\_RESTART="no"

# Save(and restore) rule and chain counter.

# Value: yes|no, default: no

# Savecounters for rules and chains to /etc/sysconfig/iptables if

#'service iptables save' is called or on stop or restart if SAVE\_ON\_STOP or

#SAVE\_ON\_RESTART is enabled.

IPTABLES\_SAVE\_COUNTER="no"

# Numericstatus output

# Value: yes|no, default: yes

# PrintIP addresses and port numbers in numeric format in the status output.

IPTABLES\_STATUS\_NUMERIC="yes"

# Verbosestatus output

# Value: yes|no, default: yes

# Printinfo about the number of packets and bytes plus the "input-" and

#"outputdevice" in the status output.

IPTABLES\_STATUS\_VERBOSE="no"

# Statusoutput with numbered lines

# Value: yes|no, default: yes

# Print acounter/number for every rule in the status output.

IPTABLES\_STATUS\_LINENUMBERS="yes"

3、 iptable恢复文件：

[root@wudilinux sysconfig]# cat /etc/sysconfig/iptables.save

4、 Iptables的参数：

（1）-h列出帮助信息

（2）-L 列出表的规则

（3）-A 追加规则 在末尾增加

（4）-I 插入规则 在规则最前端增加

（5）-D删除规则

（6）-P 默认规则,修改默认规则drop改为accept

[root@wudilinuxsysconfig]# iptables -L

Chain INPUT(policy DROP)

target prot opt source destination

ACCEPT all-- anywhere anywhere

ACCEPT tcp-- anywhere anywhere tcp spts:1024:65534 dpt:ssh

ACCEPT tcp-- anywhere anywhere tcp spts:1024:65534 dpt:http

Chain FORWARD(policy ACCEPT)

target prot opt source destination

Chain OUTPUT(policy ACCEPT)

target prot opt source destination

[root@wudilinuxsysconfig]# iptables -P INPUT ACCEPT

[root@wudilinuxsysconfig]# iptables -L

Chain INPUT(policy ACCEPT)

target prot opt source destination

ACCEPT all-- anywhere anywhere

ACCEPT tcp-- anywhere anywhere tcp spts:1024:65534 dpt:ssh

ACCEPT tcp-- anywhere anywhere tcp spts:1024:65534 dpt:http

Chain FORWARD(policy ACCEPT)

target prot opt source destination

Chain OUTPUT(policy ACCEPT)

target prot opt source destination

（7）-F 清除默认链中的规则 #当默认规则为input DROP时 执行iptables –F 后将导致所有连接断开无法连接到终端，只有在input链为accept后才可以执行-F.在没有保存的情况下可以重启恢复iptables。

（8）-X 清除自定义链中的规则

（9）-n 只显示IP地址，不显示域名

5、 Iptables的启动关闭重启保存：

Service iptables start

Service iptables stop

Service iptables restart

Service iptables save

IPTABLES的规则:

1、 规则的格式：

1、-t指定表名不指定默认为filter， 链名：五链

2、原地址和目的地址是针对数据流向来说的，input链中本地为目的地址，output中本地为原地址

3、实例：

清空规则

[root@wudilinux sysconfig]# iptables -P INPUT ACCEPT

[root@wudilinux sysconfig]# iptables -L

Chain INPUT (policy ACCEPT)

targetprot opt sourcedestination

ACCEPTall -- anywhere anywhere

ACCEPTtcp -- anywhere anywhere tcp spts:1024:65534 dpt:ssh

ACCEPTtcp -- anywhere anywhere tcp spts:1024:65534 dpt:http

Chain FORWARD (policy ACCEPT)

targetprot opt sourcedestination

Chain OUTPUT (policy ACCEPT)

targetprot opt sourcedestination

[root@wudilinux sysconfig]# iptables -F

[root@wudilinux sysconfig]# iptables -L

Chain INPUT (policy ACCEPT)

targetprot opt sourcedestination

Chain FORWARD (policy ACCEPT)

targetprot opt sourcedestination

Chain OUTPUT (policy ACCEPT)

targetprot opt sourcedestination

插入规则：

[root@wudilinux sysconfig]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

[root@wudilinux sysconfig]# iptables -L

Chain INPUT (policy ACCEPT)

targetprot opt sourcedestination

ACCEPTtcp -- anywhere anywhere tcp dpt:ssh

Chain FORWARD (policy ACCEPT)

targetprot opt sourcedestination

继续插入，查看插入后的规则顺序：

[root@wudilinux sysconfig]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

[root@wudilinux sysconfig]# iptables -I INPUT -p tcp --dport 443 -j ACCEPT

[root@wudilinux sysconfig]# iptables -L

Chain INPUT (policy ACCEPT)

targetprot opt sourcedestination

ACCEPTtcp -- anywhere anywhere tcp dpt:https

ACCEPTtcp -- anywhere anywhere tcp dpt:ssh

ACCEPTtcp -- anywhere anywhere tcp dpt:http

Chain FORWARD (policy ACCEPT)

targetprot opt sourcedestination

Chain OUTPUT (policy ACCEPT)

targetprot opt sourcedestination

Chain OUTPUT (policy ACCEPT)

targetprot opt sourcedestination

2、 IPTABLE的优先级问题

默认数字小的优先级高

[root@wudilinuxsysconfig]# iptables -L -n --line-number

ChainINPUT (policy ACCEPT)

num targetprot opt sourcedestination

1 ACCEPTtcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:443

2 ACCEPT tcp-- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22

3ACCEPT tcp --0.0.0.0/0 0.0.0.0/0 tcp dpt:80

ChainFORWARD (policy ACCEPT)

num targetprot opt sourcedestination

ChainOUTPUT (policy ACCEPT)

num target prot opt source destination

假如有限级高的已经定义了对22端口的拒绝，则后面在定义接受是没有意义的。

3、 常用模块：

（1）comment 增加备注让别人可以看懂

[root@wudilinux sysconfig]# iptables -IINPUT -p tcp --dport 443 -j ACCEPT -m comment --comment "allow ssl"

[root@wudilinux sysconfig]# iptables -L -n--line-number

Chain INPUT (policy ACCEPT)

numtarget prot opt source destination

1ACCEPT tcp --0.0.0.0/0 0.0.0.0/0 tcp dpt:443 /\* allow ssl \*/

2ACCEPT tcp --0.0.0.0/00.0.0.0/0 tcp dpt:443

3ACCEPT tcp --0.0.0.0/0 0.0.0.0/0 tcp dpt:22

4ACCEPT tcp --0.0.0.0/0 0.0.0.0/0 tcp dpt:80

（3）connlimit 并发20 个80端口的请求，超过将被丢弃

（4）iprang 指定地址段范围

（5）layer7 应用层过滤

（6）mac 基于mac地址的过滤

（7）muluiport 指定多个端口进行过滤

（8）recent限制连接次数

（9）state –m state –state 运行什么状态的数据包通过

实例：

（1）为只提供web服务的服务器编写一条安全的访问规则

[root@wudilinux sysconfig]# iptables -AINPUT -m state --stateRELATED,ESTABLISHED -j ACCEPT

[root@wudilinux sysconfig]# iptables -AINPUT -p tcp --dport 80 -j ACCEPT

[root@wudilinux sysconfig]# iptables -AINPUT -p tcp -m tcp --dport 22 -j ACCEPT

[root@wudilinux sysconfig]# iptables -AINPUT -i lo -j ACCEPT

[root@wudilinux sysconfig]# iptables -PINPUT DROP

[root@wudilinux sysconfig]# iptables -L

Chain INPUT (policy DROP)

targetprot opt sourcedestination

ACCEPTall -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPTtcp -- anywhere anywhere tcp dpt:http

ACCEPTtcp -- anywhere anywhere tcp dpt:ssh

ACCEPTall -- anywhere anywhere

Chain FORWARD (policy ACCEPT)

targetprot opt sourcedestination

Chain OUTPUT (policy ACCEPT)

targetprot opt sourcedestination