Iptables命令总结

·Iptables 软件包： iptables-services

服务 ： iptables.service

·Iptables基本框架

1. IP tables的4个表（区分大小写）

Iptables默认4个表，nat表（地址转换表） filter表(数据过滤表) raw表(状态跟踪表) mangle表（包 标记表）

1. iptables的5个链（区分大小写）

INPUT链 （入站规则）

OUTPUT链 （出站规则）

FORWARD链 （转发规则）

PREROUTING链 （路由前规则）

POSTROUTING链 （路由后规则）

·iptables命令的基本使用方法

语法格式：iptables -t [表名] 选项/增删改查 [链名] [条件] -j [目标操作]

1. //注意事项与规律：
2. //可以不指定表，默认为filter表
3. //可以不指定链，默认为对应表的所有链
4. //如果没有找到匹配条件，则执行防火墙默认规则
5. //选项/链名/目标操作用大写字母，其余都小写
6. ########################################################################
7. //目标操作：
8. // ACCEPT：允许通过/放行
9. // DROP：直接丢弃，不给出任何回应
10. // REJECT：拒绝通过，必要时会给出提示
11. // LOG：记录日志，然后传给下一条规则

iptables命令的常用选项如表-1所示。

表-1 iptables常用选项



·主机型防火墙，主要保护的是服务器本机（过滤威胁本机的数据包）。

·网络防火墙，主要保护的是防火墙后面的其他服务器，如web服务器

iptables防火墙规则的条件

iptables防火墙可以根据很多很灵活的规则进行过滤行为，具体常用的过滤条件如表-2所示。

表-2 iptables过滤条件



主机型防火墙案列

1. [root@proxy ~]# iptables -A INPUT -s 192.168.4.100 -j DROP
2. //丢弃192.168.4.100发给本机的所有数据包
3. [root@proxy ~]# iptables -A INPUT -s 192.168.2.0/24 -j DROP
4. //丢弃192.168.2.0/24网络中所有主机发送给本机的所有数据包
5. [root@proxy ~]# iptables -A INPUT -s 114.212.33.12 -p tcp --dport 22 -j REJECT
6. //拒绝114.212.33.12使用tcp协议远程连接本机ssh（22端口）

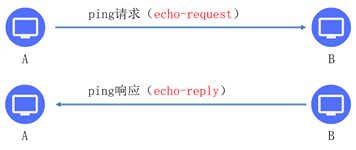
网络型防火墙案例

设置proxy主机的防火墙规则，保护防火墙后面的Web服务器

1. [root@proxy ~]# iptables -I FORWARD -s 192.168.4.100 -p tcp --dport 80 -j DROP

**禁ping的相关策略**

ping的流程（A主机pingB主机）如图-3所示。



禁止其他主机ping本机，允许本机ping其他主机

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. [root@proxy ~]# iptables -A INPUT -p icmp \
2. > --icmp-type echo-request -j DROP
3. //仅禁止入站的ping请求，不拒绝入站的ping回应包

[root@proxy ~]# iptables -A INPUT -p icmp \

> --icmp-type echo-request -j DROP

//仅禁止入站的ping请求，不拒绝入站的ping回应包

注意：关于ICMP的类型，可以参考help帮助，参考命令如下：

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. [root@proxy ~]# iptables -p icmp --help

## **防火墙扩展规则**

iptables在基本过滤条件的基础上还扩展了很多其他条件，在使用时需要使用-m参数来启动这些扩 展功能，语法如下：

iptables 选项 链名称 -m 扩展模块 --具体扩展条件 -j 动作

**根据MAC地址过滤**

根据MAC地址过滤，可以防止禁用的客户轻易更换IP地址的发生

1. [root@proxy ~]# iptables -A INPUT -p tcp --dport 22\
2. > -m mac --mac-source 52:54:00:00:00:0b -j DROP
3. //拒绝52:54:00:00:00:0b这台主机远程本机

**基于多端口设置过滤规则**

1）一次需要过滤或放行很多端口时会比较方便

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. [root@proxy ~]# iptables -A INPUT -p tcp \
2. > -m multiport --dports 20:22,25,80,110,143,16501:16800 -j ACCEPT
3. //一次性开启20,21,22,25,80,110,143,16501到16800所有的端口

提示，多端口还可以限制多个源端口，但因为源端口不固定，一般不会使用，限制多个源端口的参数是--sports.

**根据IP地址范围设置规则**

1）允许从 192.168.4.10-192.168.4.20 登录

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. [root@proxy ~]# iptables -A INPUT -p tcp --dport 22 \
2. > -m iprange --src-range 192.168.4.10-192.168.4.20 -j ACCEPT

[root@proxy ~]# iptables -A INPUT -p tcp --dport 22 \

> -m iprange --src-range 192.168.4.10-192.168.4.20 -j ACCEPT

注意，这里也可以限制多个目标IP的范围，参数是--dst-range,用法与--src-range一致。

2）禁止从 192.168.4.0/24 网段其他的主机登录

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. [root@proxy ~]# iptables -A INPUT -p tcp --dport 22 -s 192.168.4.0/24 -j DROP

## **配置SNAT实现共享上网**

**设置防火墙规则，实现IP地址的伪装（SNAT源地址转换）**

设置防火墙规则，实现SNAT地址转换

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. **[**root@proxy **~]**# iptables **-**t nat **-**A POSTROUTING **\**
2. **>** **-**s 192.168.4.0**/**24 **-**p tcp **--**dport 80 **-**j SNAT **--**to**-**source 192.168.2.5

扩展知识，对于proxy外网IP不固定的情况可以执行下面的地址伪装，动态伪装IP。

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. [root@proxy ~]# iptables -t nat -A POSTROUTING \
2. > -s 192.168.4.0/24 -p tcp --dport 80 -j MASQUERADE

[root@proxy ~]# iptables -t nat -A POSTROUTING \

> -s 192.168.4.0/24 -p tcp --dport 80 -j MASQUERADE

最后，所有iptables规则都是临时规则，如果需要永久保留规则需要执行如下命令:

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY06/CASE/01/index.html)

1. [root@proxy ~]# service iptables save