Linux 防火墙 iptables 学习笔记（二）参数指令

iptables 指令

语法：

```
iptables[-ttable]command[match][-jtarget/jump]
```

-t 参数用来指定规则表，内建的规则表有三个，分别是：nat、mangle 和 filter，当未指定规则表时，则一律视为是 filter。个规则表的功能如下：

nat 此规则表拥有 Prerouting 和 postrouting 两个规则链，主要功能为进行一对一、一对多、多对多等网址转译工作（SNATDNAT），由于转译工作的特性，需进行目的地网址转译的封包，就不需要进行来源网址转译，反之亦然，因此为了提升改写封包的率，在防火墙运作时，每个封包只会经过这个规则表一次。如果我们把封包过滤的规则定义在这个数据表里，将会造成无法对同一包进行多次比对，因此这个规则表除了作网址转译外，请不要做其它用途。

mangle 此规则表拥有 Prerouting、FORWARD 和 postrouting 三个规则链。

除了进行网址转译工作会改写封包外，在某些特殊应用可能也必须去改写封包（TTL、TOS）或者是设定 MARK（将封包作记号，以进行后续的过滤），这

时就必须将这些工作定义在 mangle 规则表中，由于使用率不高，我们不打算在这里讨论 mangle 的用法。

filter 这个规则表是预设规则表，拥有 INPUT、FORWARD 和 OUTPUT 三个规则链，这个规则表顾名思义是用来进行封包过滤的理动作(例如 :DROP、LOG、ACCEPT 或 REJECT ），我们会将基本规则都建立在此规则表中。

常用命令列表：

```
命令-A,--append
```

范例 iptables-AINPUT...

说明新增规则到某个规则链中，该规则将会成为规则链中的最后一条规则。

```
命令-D,--delete
```

范例 iptables-DINPUT--dport80-jDROP

```
iptables-DINPUT1
```

说明从某个规则链中删除一条规则，可以输入完整规则，或直接指定规则编号加以删除。

```
命令-R,--replace
```

范例 iptables-RINPUT1-s192.168.0.1-jDROP

说明取代现行规则，规则被取代后并不会改变顺序。

```
命令-I,--insert
```

范例 iptables-IINPUT1--dport80-jACCEPT

说明插入一条规则，原本该位置上的规则将会往后移动一个顺位。

```
命令-L,--list
```

范例 iptables-LINPUT

说明列出某规则链中的所有规则。

```
命令-F,--flush
```

范例 iptables-FINPUT

说明删除某规则链中的所有规则。

```
命令-Z,--zero
```

范例 iptables-ZINPUT

说明将封包计数器归零。封包计数器是用来计算同一封包出现次数，是过滤阻断式攻击不可或缺的工具。

```
命令-N,--new-chain
```

范例 iptables-Nallowed

说明定义新的规则链。

```
命令-X,--delete-chain
```

范例 iptables-Xallowed

说明删除某个规则链。

```
命令-P,--policy
```

范例 iptables-PINPUTDROP

说明定义过滤政策。也就是未符合过滤条件之封包，预设的处理方式。

```
命令-E,--rename-chain
```

范例 iptables-Ealloweddisallowed

说明修改某自订规则链的名称。

常用封包比对参数：

```
参数-p,--protocol
```

范例 iptables-AINPUT-ptcp

说明比对通讯协议类型是否相符，可以使用!运算子进行反向比对，例如：-p!tcp，意思是指除 tcp 以外的其它类型，包含 udp、icmp...等。如果要比对所有类型，则可以使用 all 关键词，例如：-pall。

```
参数-s,--src,--source
```

范例 iptables-AINPUT-s192.168.1.1

说明用来比对封包的来源 IP，可以比对单机或网络，比对网络时请用数字来表示屏蔽，例如：-s192.168.0.0/24，比对 IP 时可以使用!运算子进行反向比对，例如：-s!192.168.0.0/24。

```
参数-d,--dst,--destination
```

范例 iptables-AINPUT-d192.168.1.1

说明用来比对封包的目的地 IP，设定方式同上。

```
参数-i,--in-interface
```

范例 iptables-AINPUT-ieth0

说明用来比对封包是从哪片网卡进入，可以使用通配字符+来做大范围比对，例如：-ieth+表示所有的 ethernet 网卡，也以使用!运算子进行反向比对，例如：-i!eth0。

```
参数-o,--out-interface
```

范例 iptables-AFORWARD-oeth0

说明用来比对封包要从哪片网卡送出，设定方式同上。

```
参数--sport,--source-port
```

范例 iptables-AINPUT-ptcp--sport22

说明用来比对封包的来源埠号，可以比对单一埠，或是一个范围，例如：--sport22:80，表示从 22 到 80 埠之间都算是符合件，如果要比对不连续的多个埠，则必须使用--multiport 参数，详见后文。比对埠号时，可以使用!运算子进行反向比对。

```
参数--dport,--destination-port
```

范例 iptables-AINPUT-ptcp--dport22

说明用来比对封包的目的地埠号，设定方式同上。

参数--tcp-flags

范例 iptables-ptcp--tcp-flagsSYN,FIN,ACKSYN

说明比对 TCP 封包的状态旗号，参数分为两个部分，第一个部分列举出想比对的旗号，第二部分则列举前述旗号中哪些有被设，未被列举的旗号必须是空的。TCP 状态旗号包括：SYN（同步）、ACK（应答）、FIN（结束）、RST（重设）、URG（紧急）

PSH（强迫推送）等均可使用于参数中，除此之外还可以使用关键词 ALL 和 NONE 进行比对。比对旗号时，可以使用!运算子行反向比对。

参数--syn

范例 iptables-ptcp--syn

说明用来比对是否为要求联机之 TCP 封包，与 iptables-ptcp--tcp-flagsSYN,FIN,ACKSYN 的作用完全相同，如果使用!运算子，可用来比对非要求联机封包。

参数-mmultiport--source-port

范例 iptables-AINPUT-ptcp-mmultiport--source-port22,53,80,110

说明用来比对不连续的多个来源埠号，一次最多可以比对 15 个埠，可以使用!运算子进行反向比对。

参数-mmultiport--destination-port

范例 iptables-AINPUT-ptcp-mmultiport--destination-port22,53,80,110

说明用来比对不连续的多个目的地埠号，设定方式同上。

参数-mmultiport--port

范例 iptables-AINPUT-ptcp-mmultiport--port22,53,80,110

说明这个参数比较特殊，用来比对来源埠号和目的埠号相同的封包，设定方式同上。注意：在本范例中，如果来源端口号为 80 目的地埠号为 110，这种封包并不算符合条件。

参数--icmp-type

范例 iptables-AINPUT-picmp--icmp-type8

说明用来比对 ICMP 的类型编号，可以使用代码或数字编号来进行比对。请打 iptables-picmp--help 来查看有哪些代码可用。

参数-mlimit--limit

范例 iptables-AINPUT-mlimit--limit3/hour

说明用来比对某段时间内封包的平均流量，上面的例子是用来比对：每小时平均流量是否超过一次 3 个封包。除了每小时平均次外，也可以每秒钟、每分钟

或每天平均一次,默认值为每小时平均一次,参数如后 :/second、/minute、/day。除了进行封

数量的比对外，设定这个参数也会在条件达成时，暂停封包的比对动作，以避免因骇客使用洪水攻击法，导致服务被阻断。

参数--limit-burst

范例 iptables-AINPUT-mlimit--limit-burst5

说明用来比对瞬间大量封包的数量,上面的例子是用来比对一次同时涌入的封包是否超过 5 个（这是默认值），超过此上限的封将被直接丢弃。使用效果同上。

参数-mmac--mac-source

范例 iptables-AINPUT-mmac--mac-source00:00:00:00:00:01

说明用来比对封包来源网络接口的硬件地址，这个参数不能用在 OUTPUT 和 Postrouting 规则炼上，这是因为封包要送出到网后，才能由网卡驱动程序透过 ARP 通讯协议查出目的地的 MAC 地址，所以 iptables 在进行封包比对时，并不知道封包会送到个网络接口去。

参数--mark

范例 iptables-tmangle-AINPUT-mmark--mark1

说明用来比对封包是否被表示某个号码，当封包被比对成功时，我们可以透过 MARK 处理动作，将该封包标示一个号码，号码最不可以超过 4294967296。

参数-mowner--uid-owner

范例 iptables-AOUTPUT-mowner--uid-owner500

说明用来比对来自本机的封包，是否为某特定使用者所产生的，这样可以避免服务器使用 root 或其它身分将敏感数据传送出，可以降低系统被骇的损失。可惜这个功能无法比对出来自其它主机的封包。

参数-mowner--gid-owner

范例 iptables-AOUTPUT-mowner--gid-owner0

说明用来比对来自本机的封包，是否为某特定使用者群组所产生的，使用时机同上。

参数-mowner--pid-owner

范例 iptables-AOUTPUT-mowner--pid-owner78

说明用来比对来自本机的封包，是否为某特定行程所产生的，使用时机同上。

参数-mowner--sid-owner

范例 iptables-AOUTPUT-mowner--sid-owner100

说明用来比对来自本机的封包，是否为某特定联机（SessionID）的响应封包，使用时机同上。

参数-mstate--state

范例 iptables-AINPUT-mstate--stateRELATED,ESTABLISHED

说明用来比对联机状态，联机状态共有四种：INVALID、ESTABLISHED、NEW 和 RELATED。

INVALID 表示该封包的联机编号（SessionID）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联机。

NEW 表示该封包想要起始一个联机（重设联机或将联机重导向）。

RELATED 表示该封包是属于某个已经建立的联机，所建立的新联机。例如：FTP-DATA 联机必定是源自某个 FTP 联机。

常用的处理动作：

-j 参数用来指定要进行的处理动作，常用的处理动作包括：ACCEPT、REJECT、DROP、REDIRECT、MASQUERADE、LOG、DNAT、

SNAT、MIRROR、QUEUE、RETURN、MARK，分别说明如下：

ACCEPT 将封包放行，进行完此处理动作后，将不再比对其它规则，直接跳往下一个规则炼（natostrouting）。

REJECT 拦阻该封包，并传送封包通知对方，可以传送的封包有几个选择：ICMPport-unreachable、ICMPecho-reply 或是

tcp-reset（这个封包会要求对方关闭联机），进行完此处理动作后，将不再比对其它规则，直接中断过滤程序。范例如下：

```
iptables-AFORWARD-pTCP--dport22-jREJECT--reject-withtcp-reset
```

DROP 丢弃封包不予处理，进行完此处理动作后，将不再比对其它规则，直接中断过滤程序。

REDIRECT 将封包重新导向到另一个端口（PNAT），进行完此处理动作后，将会继续比对其它规则。这个功能可以用来实作通透式

```
porxy 或用来保护 web 服务器。例如：iptables-tnat-APREROUTING-ptcp--dport80-jREDIRECT--to-ports8080
```

MASQUERADE 改写封包来源 IP 为防火墙 NICIP ,可以指定 port 对应的范围，进行完此处理动作后，直接跳往下一个规则（mangleostrouting）。这个功能与 SNAT 略有不同，当进行 IP 伪装时，不需指定要伪装成哪个 IP，IP 会从网卡直接读，当使用拨接连线时，IP 通常是由 ISP 公司的 DHCP 服务器指派的，这个时候 MASQUERADE 特别有用。范例如下：

```
iptables-tnat-APOSTROUTING-pTCP-jMASQUERADE--to-ports1024-31000
```

LOG 将封包相关讯息纪录在/var/log 中，详细位置请查阅/etc/syslog.conf 组态档，进行完此处理动作后，将会继续比对其规则。例如：

```
iptables-AINPUT-ptcp-jLOG--log-prefix"INPUTpackets"
```

SNAT 改写封包来源 IP 为某特定 IP 或 IP 范围，可以指定 port 对应的范围，进行完此处理动作后，将直接跳往下一个规则（mangleostrouting）。范例如下：

```
iptables-tnat-APOSTROUTING-ptcp-oeth0-jSNAT--to-source194.236.50.155-194.236.50.160:1024-32000
```

DNAT 改写封包目的地 IP 为某特定 IP 或 IP 范围，可以指定 port 对应的范围，进行完此处理动作后，将会直接跳往下一个规炼（filter:input 或 filter:forward）。范例如下：

```
iptables-tnat-APREROUTING-ptcp-d15.45.23.67--dport80-jDNAT--to-destination
```

192.168.1.1-192.168.1.10:80-100

MIRROR 镜射封包，也就是将来源 IP 与目的地 IP 对调后，将封包送回，进行完此处理动作后，将会中断过滤程序。

QUEUE 中断过滤程序，将封包放入队列，交给其它程序处理。透过自行开发的处理程序，可以进行其它应用，例如：计算联机费.....等。

RETURN 结束在目前规则炼中的过滤程序，返回主规则炼继续过滤，如果把自订规则炼看成是一个子程序，那么这个动作，就相当提早结束子程序并返回到主程序中。

MARK 将封包标上某个代号，以便提供作为后续过滤的条件判断依据，进行完此处理动作后，将会继续比对其它规则。范例如下：

```
iptables-tmangle-APREROUTING-ptcp--dport22-jMARK--set-mark2
```