iptables命令

iptables命令是Linux操作系統下常用的防火牆軟件，是netfilter項目的一部分。可以直接配置，也可以通過許多前端和圖形界面配置。

語法

iptables(選項)(參數)

選項

-t<表>：指定要操縱的表；
-A：向規則鏈中添加條目；
-D：從規則鏈中刪除條目；
-I：向規則鏈中插入條目；
-R：替換規則鏈中的條目；
-L：顯示規則鏈中已有的條目；
-F：清楚規則鏈中已有的條目；
-Z：清空規則鏈中的數據包計算器和字節計數器；
-N：創建新的用戶自定義規則鏈；
-P：定義規則鏈中的默認目標；
-h：顯示幫助信息；
-p：指定要匹配的數據包協議類型；
-s：指定要匹配的數據包源ip地址；
-j<目標>：指定要跳轉的目標；
-i<網絡接口>：指定數據包進入本機的網絡接口；
-o<網絡接口>：指定數據包要離開本機所使用的網絡接口。

iptables命令選項輸入順序：

iptables -t 表名<-A/I/D/R> 規則鏈名[規則號] <-i/o 網卡名> -p 協議名<-s 源IP/源子網> --sport 源端口<-d 目標IP/目標子網> --dport 目標端口-j 動作

表名包括：

raw：高級功能，如：網址過濾。
mangle：數據包修改（QOS），用於實現服務質量。
net：地址轉換，用於網關路由器。
filter：包過濾，用於防火牆規則。

規則鏈名包括：

INPUT鏈：處理輸入數據包。
OUTPUT鏈：處理輸出數據包。
PORWARD鏈：處理轉發數據包。
PREROUTING鏈：用於目標地址轉換（DNAT）。
POSTOUTING鏈：用於源地址轉換（SNAT）。

動作包括：

ACCEPT：接收數據包。
DROP：丟棄數據包。 REJECT：拒絕接收數據包。
REDIRECT：重定向、映射、透明代理。
SNAT：源地址轉換。
DNAT：目標地址轉換。
MASQUERADE：IP偽裝（NAT），用於ADSL。
LOG：日誌記錄。

實例

清除已有**iptables**規則

```
iptables -F
iptables -X
iptables -Z
```

開放指定的端口

```
iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT #允許本地回環接口(即運行本機訪問本機)
```

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT #允許已建立的或相關連的通行
iptables -A OUTPUT -j ACCEPT #允許所有本機向外的訪問
iptables -A INPUT -p tcp --dport 22 -j ACCEPT #允許訪問22端口
iptables -A INPUT -p tcp --dport 80 -j ACCEPT #允許訪問80端口
iptables -A INPUT -p tcp --dport 21 -j ACCEPT #允許ftp服務的21端口
iptables -A INPUT -p tcp --dport 20 -j ACCEPT #允許FTP服務的20端口
iptables -A INPUT -j reject #禁止其他未允許的規則訪問
iptables -A FORWARD -j REJECT #禁止其他未允許的規則訪問

mask(屏蔽) **IP**

iptables -I INPUT -s 123.45.6.7 -j DROP #針對單個IP的命令
iptables -I INPUT -s 123.0.0.0/8 -j DROP #封IP段即從123.0.0.1到123.255.255.254的命令
iptables -I INPUT -s 124.45.0.0/16 -j DROP #封IP段即從123.45.0.1到123.45.255.254的命令
iptables -I INPUT -s 123.45.6.0/24 -j DROP #封IP段即從123.45.6.1到123.45.6.254的命令是

查看已添加的**iptables**規則

```
iptables -L -n -vChain INPUT (policy DROP 48106 packets, 2690K bytes)
pkts bytes target prot opt in out source destination
5075 589K ACCEPT all -- lo * 0.0.0.0/0 0.0.0.0/0
191K 90M ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
1499K 133M ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
4364K 6351M ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED
6256 327K ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 3382K packets, 1819M bytes)
pkts bytes target prot opt in out source destination
5075 589K ACCEPT all -- * lo 0.0.0.0/0 0.0.0.0/0
```

刪除已添加的**iptables**規則

將所有iptables以序號標記顯示，執行：

```
iptables -L -n --line-numbers
```

比如要刪除INPUT裡序號為8的規則，執行：

```
iptables -D INPUT 8
```