<http://s2.naes.tn.edu.tw/~kv/iptables.htm>

**iptables 設定入門**

如果防火牆設在Linux本機上，且Linux本機沒啟用NAT的功能，那只需考慮filter這個table的*INPUT*與*OUTPUT* 鏈就可！但如果Linux主機還考慮到NAT的功能，那麼nat table的*PREROUTING*與*POSTROUTING*還有filter table的*FORWARD*就要設定了！***ipchains* 和 *iptables* 在語法上的主要的差異，注意如下：**

|  |
| --- |
| 1. 在ipchains中，諸如input鏈，是使用小寫的chains名，在iptables中，要改用大寫INPUT。  2. 在iptables中，要指定規則是欲作用在那一個規則表上(用-t指定，如-t nat)，若不指定，則預設是作用在filter這個表。  3. 在ipchains中，-i是指介面(interface)，但在 iptables 中，-i則是指進入的方向，且多了-o，代表出去的方向。  4. 在iptables中，來源port要使用關鍵字 --sport 或 --source-port  5. 在iptables中，目的port要使用關鍵字 --dport 或 --destination-port  6. 在iptables中，"丟棄"的處置動作，不再使用DENY這個target，改用DROP。  7. 在ipchains的記錄檔功能-l，已改為目標-j LOG，並可指定記錄檔的標題。  8. 在ipchains中的旗標-y，在iptables中可用--syn或--tcp-flag SYN,ACK,FIN SYN  9. 在iptables中，imcp messages型態，要加上關鍵字--icmp-type，如：  *iptables -A OUTPUT -o eth0 -p icmp -s $FW\_IP --icmp-type 8 -d any/0 -j ACCEPT* |

**觀察目前的設定**

*[root@test root]#****iptables -L -n***  
*Chain INPUT (policy ACCEPT)   
target     prot opt source               destination   
Chain FORWARD (policy ACCEPT)   
target     prot opt source               destination   
Chain OUTPUT (policy ACCEPT)   
target     prot opt source               destination*  
# 因為沒有加上-t的參數，所以預設就是filter這個表格，  
# 在表格中有三條鏈，分別是INPUT, OUTPUT 與 FORWARD，因為沒有規則，所以規則裡都是空的！  
# 在每個chain的後面，括號()裡面，會發現有policy！這是『預設動作(政策)』！  
# 以上面來看，雖然啟動*iptables*，但沒有設定規則，政策又是ACCEPT，所以『任何封包都會接受』！

*[root@test root]#****iptables -t nat -L -n*** *Chain PREROUTING (policy ACCEPT)   
target     prot opt source               destination*

*Chain POSTROUTING (policy ACCEPT)   
target     prot opt source               destination*

*Chain OUTPUT (policy ACCEPT)   
target     prot opt source               destination*  
# 與filter類似的，nat這個表格裡面有的則是PREROUTING, POSTROUTING 以及OUTPUT三條鏈！

**清除所有的規則**

一開始先清除所有的規則，重新開始，以免舊的規則影響新的設定。參數說明：   
-F ：清除所有的已訂定的規則；   
-X ：殺掉所有使用者建立的 tables；   
-Z ：將所有的chain的計數與流量統計都歸零

|  |
| --- |
| # *iptables -F (*清除預設表filter中，所有規則鏈中的規則)  # *iptables -X (*清除預設表filter中，使用者自訂鏈中的規則)  # *iptables -F -t mangle (*清除mangle表中，所有規則鏈中的規則)  # *iptables -t mangle -X (*清除mangle表中，使用者自訂鏈中的規則)  # *iptables -F -t nat (*清除nat表中，所有規則鏈中的規則)  # *iptables -t nat -X (*清除nat表中，使用者自訂鏈中的規則) |

**※****選定預設的政策**

接著要選定各個不同的規則鏈，預設的政策為何。清除規則之後，接著要設定規則的政策！『當封包不在設定的規則內時，該封包的通過與否，以Policy的設定為準』，通常政策在filter table的*INPUT*鏈可定義嚴格一點，而*FORWARD*與*OUTPUT*則訂定鬆些！通常都是將*INPUT*的policy 定義為*DROP*！全部都擋掉再說！

*[root@test root]#****/sbin/iptables****[-t tables] [-P] [INPUT,OUTPUT,FORWARD| PREROUTING,OUTPUT,POSTROUTING] [ACCEPT,DROP]*  
參數說明：   
-P：定義政策(Policy)。**注意這個 P為大寫！**   
INPUT：封包為輸入主機的方向；   
OUTPUT：封包為輸出主機的方向；   
FORWARD：封包為不進入主機而向外再傳輸出去的方向；   
PREROUTING：在進入路由之前進行的工作；   
OUTPUT：封包為輸出主機的方向；   
POSTROUTING：在進入路由之後進行的工作。   
範例：   
*[root@test root]#****/sbin/iptables -P INPUT DROP*** *[root@test root]#****/sbin/iptables -P OUTPUT ACCEPT*** *[root@test root]#****/sbin/iptables -P FORWARD ACCEPT*** *[root@test root]#****/sbin/iptables -t nat -P PREROUTING ACCEPT*** *[root@test root]#****/sbin/iptables -t nat -P OUTPUT ACCEPT*** *[root@test root]#****/sbin/iptables -t nat -P POSTROUTING ACCEPT***  
# 除INPUT外，其他都設定為接受！在上面的設定後，主機發出的封包可出去，但任何封包都無法進入，  
# 包括回應給送出封包的回應封包(ACK)也無法進入！

**增加與插入規則**

接下來要定義規則！請注意，這小節裡面完全都針對Linux本機來設定(僅針對filter table！不包含NAT)

例一：所有的來自lo介面的封包，都予以接受   
*[root@test root]#****iptables -A INPUT -i lo -j ACCEPT***  
# 因-d, --dport, -s, --sport等參數都沒設定，表示：   
# 不論封包來自何處或去到哪裡，只要是lo介面就接受！這個觀念挺重要的，『沒有設定的規定，則表示該規定完全接受』！  
# 例如這個案例當中，關於 -s, -d...等等的參數沒有規定時！   
例二：來自 192.168.0.1 這個 IP 的封包都予以接受：   
*[root@test root]#****iptables -A INPUT -i eth0 -p tcp -s 192.168.0.1 -j ACCEPT***  
# 新增一條規則，只要來自於192.168.0.1的封包，不論要去哪裡，使用的是那個協定(port)主機都會予以接受～    
例三：來自 192.168.1.0 這個 C Class 的網域的任何一部電腦，就予以接受！   
*[root@test root]#****iptables -A INPUT -i eth0 -p tcp -s 192.168.1.0/24 -j ACCEPT***  
# 這是網域的寫法！針對整個網域開放！網域的寫法可以是：192.168.1.0/24或192.168.1.0/255.255.255.0！   
例四：來自192.168.1.25的封包都給他丟棄去！   
*[root@test root]#****iptables -A INPUT -i eth0 -p tcp -s 192.168.1.25 -j DROP***

例五：來自192.168.0.24這個 IP 的封包，想要到137,138,139埠口時，都接受   
*[root@test root]#****iptables -A INPUT -i eth0 -p tcp -s 192.168.0.24/24 --dport 137:139 -j ACCEPT***

**參數說明：**

[root@test root]# iptables [-t filter] [-AI INPUT,OUTPUT,FORWARD] \   
> [-io interface] [-p tcp,udp,icmp,all] [-s IP/network] [--sport ports]  \   
> [-d IP/network] [--dport ports] -j [ACCEPT,DROP]   
-A：新增加一條規則，該規則增加在最後面，例如原本已經有四條規則，使用-A就可以加上第五條規則！  
-I：插入一條規則，如沒有設定規則順序，預設是插入變第一條規則，如原本有四條規則，使用-I則該規則變成第一條，而原本四條變成 2~5   
　INPUT：規則設定為filter table的INPUT鏈   
　OUTPUT：規則設定為filter table的OUTPUT鏈   
　FORWARD：規則設定為filter table的FORWARD鏈   
-i：設定『封包進入』的網路卡介面   
-o：設定『封包流出』的網路卡介面   
　interface ：網路卡介面，例如 ppp0, eth0, eth1....   
-p：注意這是小寫！封包的協定啦！   
　tcp：封包為TCP協定的封包；udp：封包為UDP協定的封包；icmp：封包為ICMP協定；all ：表示為所有的封包！   
-s：來源封包的IP或者是Network(網域)；   
--sport：來源封包的port號碼，也可以使用port1:port2如21:23同時通過21,22,23的意思   
-d：目標主機的IP或者是Network(網域)；   
--dport：目標主機的 port 號碼；   
-j：動作，可以接底下的動作；   
　ACCEPT：接受該封包 ；DROP：丟棄封包   
　LOG：將該封包的資訊記錄下來 (預設記錄到/var/log/messages檔案)各個規則鏈的預設政策可獨立自主的設定，不必受其它鏈的影響。若目標為DROP，則policy設為ACCEPT；若目標為ACCEPT，則policy設為DROP，方可看出效果。

**定義變數**

|  |
| --- |
| *FW\_IP="163.26.161.253"* |

**打開核心 forward 功能**

|  |
| --- |
| # 打開 forward 功能  *echo "1" > /proc/sys/net/ipv4/ip\_forward* |

**開放某一個介面**

|  |
| --- |
| *iptables -A INPUT -i lo -j ACCEPT*  *iptables -A OUTPUT -o lo -j ACCEPT* |