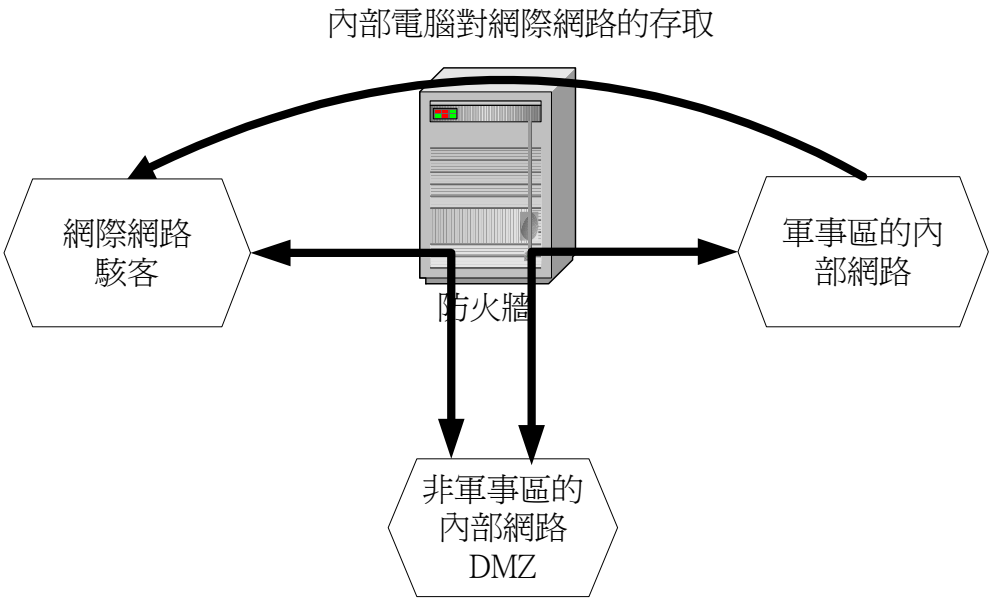
第 30 章
網路安全、防火牆與 NAT 伺服器

第 30 章

網路安全、防火牆與 NAT 伺服器



由於越多人使用網路，也因此網路成了一個社會。有很多人使用網路來作好事，但是也有少數的人使用網路犯罪。為了防止我們的網站或網域遭受到駭客的入侵破壞，我們使用防火牆將我們的網路資源分成軍事區和非軍事區(demilitarized zone 簡稱 DMZ)。軍事區的內部網路是放置受保護的網路資源，且嚴格禁止外部網際網路或駭客進入，例如資料庫、郵件伺服器….。而非軍事區放置一般可以讓外部網域使用的網路資源來供外部使用，如網站 www、FTP 檔案傳輸伺服器。我們軍事區的內部網路可以透過防火牆存取外部網際網路的資源。軍事區的內部網路和非軍事區的內部網路也可以透過防火牆的控制來互相存取資源。網際網路和非軍事區的內部網路也可以透過防火牆的控制來存取防火牆允許的資源。但是，如上圖，防火牆只允許軍事區的內部網路存取網際網路的資源，而不允許網際網路來存取軍事區內部網路的資源。

30-1 防火牆：iptables 和 NAT

一個好的網路安全基礎，就是在我們作業系統中建立防火牆，來保護我們作業系統來自未授權的攻擊。我們可以使用防火牆來作封包過濾或代理。封包過濾就是由我們的防火牆決定是否讓外面的網路封包進入到我們作業系統或內部網路。封包過濾檢查封包的來源位址和它要到達的目的地。網路過濾軟體套件實作套件過濾和 NAT(網路位址轉換)的工作。我們可以使用 iptables 指令來實作網路過濾和 NAT 的工作。iptables 軟體已經內建到 2.4Kernel(linux2.4 核心)，其名稱為 iptable_filter.o。iptables 指令是比 ipchains 指令還好用，而且還有延伸性。網路過濾器 iptables 指令的參數有封包過濾、使用者定義串列、ICMP 封包、連接埠、狀態、NAT(網路位址轉換)。

語法：

指令：iptables 參數

參數：

這是命令參數

-A chain 串列：將規則加入串列中。

-D chain 串列：從串列中刪除合適的規則。

-D chain 規則編號：從串列中刪除規則編號(1=first)。

-I 串列 規則編號：將規則編號插入串列中。

-R 串列 規則編號：取代在串列中的規則編號。

-L 串列：列出所有串列的規則。

-E 串列：修改串列的名稱。

-F 串列：刪除所有串列中的規則。

-R 串列：取代規則。

-Z 串列：將所有規則的封包和串列計數歸 0。

-N 串列：建立新的使用者定義串列。

-X 串列：刪除使用者定義串列。

-P 串列：改變目標串列的策略。

這是 iptables 命令的參數。

參數	功能
-p [!] 協定	指定 TCP、UDP、ICMP 或 ALL 協定
-s[!] 位址[遮罩] [!][連接埠[:port]]	我們可以指定來源位址，遮罩和連接埠
--sport [!][port[:port]]	我們可以指定來源連接埠的範圍
-d[!]位址[/遮罩][!][連接埠]	我們可以指定符合的目地位址，和連接埠。
--dport [!][連接埠[:port]]	指定目地的連接埠
--icmp-type [!]類型名稱	指定網路控制訊息協定 ICMP(Internet Assigned Numbers Authority)
-i [!]介面卡名稱[+]	指定輸入網路介面卡(例如 eth0)
-j 目標 [連接埠]	指定規則的目標。指定轉向目標的連接埠。
--to-source<ipaddr>[-<ipaddr>] [:port-port]	和 SNAT 目標一起使用。使用新的來源 IP 來覆寫封包。
--to-destination<ipaddr>[-<ipaddr>] [:port-port]	和 DNAT 目標一起使用。使用的的目地 IP 來覆寫封包。
-n	位址和連接埠的數字輸出，和-L 一起使用。
-o [!] 介面卡名稱[+]	指定輸出的網路介面卡(例如 eth0)。可以用來轉向或輸出串列。
-t table	指定使用的表格，例如-t nat 是指定 NAT 的表格。
-v	使用詳細模式。顯示詳細的規則，和-L 一起使用。
-x	顯示正確的數字。一般和-L 一起使用。
[!] – f	符合分割封包的最近分割時間。
[!]-v	列出封包的版本。
!	相反(not)的符號。不允許參數或位址。
-m	指定使用的模組。例如 state。
--state	指定參數給狀態模組，如 NEW、INVALID、RELATED 和 ESTABLISHED。這是用來偵測封包的狀態。NEW 參考 SYN 封包。
--syn	SYN 封包。新的連接。
--tcp-flags	Tcp 旗標：SYN、ACK、FIN、RST、URG、

	PS、和 ALL。
--limit	Limit 模組的選項。
--limit-burst	Limit 模組的選項。用來控制服務拒絕的攻擊。

這是 iptables 指令的目地。

目標	功能
ACCEPT	允許封包穿過防火牆
DROP	刪除封包
REJECT	刪除封包但會通告傳送者
QUEUE	傳送封包到使用者空間
RETURN	跳到 chain 串列的最後面，讓預設的目標處理

這是網路過濾內件的串列。

Chain 串列	說明
INPUT	輸入封包的規則
OUTPUT	輸出封包的規則
FORWARD	轉向封包的規則
PREROUTING	只用在 NAT 表上。轉向或修改輸入封包的規則
POSTROUTING	只用在 NAT 表上。轉向或修改輸出封包的規則。

30-1-1 iptables 指令範例

假如 iptables 被正確的組態，它應該回傳三個不同的項目 INPUT、FORWARD 和 OUTPUT。我們可以使用 iptables –L 觀看目前的組態。

```
#/sbin/iptables -L
```

```
[root@flash html]# /sbin/iptables -L
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
```

這個指令定義一個規則，這個規則拒絕所有從 192.168.75.0 的子網域，然後它會送出給該使用者"destination unreachable"的錯誤資訊。

/sbin/iptables -A INPUT -s 192.168.75.0/24 -j REJECT

這個指令定義一個規則，這個規則停止所有從 192.168.75.0 位址的電腦使用 ICMP 協定 pinging 我們的系統。

/sbin/iptables -A INPUT -s 192.168.25.200 -p icmp -j DROP

這個指令定義一個刪除規則，這個規則刪除 pinging 我們的系統的規則。

/sbin/iptables -D INPUT -s 192.168.25.200 -p icmp -j DROP

預設的規則是接受所有 INPUT、OUTPUT 和 FORWARD 的封包，我們可以使用下列方式來停止封包的 FORWARD。

/sbin/iptables -A FORWARD -j DROP

我們可以使用下列指令來儲存我們所設定的防火牆組態。這將儲存我們防火牆組態到/etc/sysconfig/iptables 中。

#/sbin/service iptables save

```
[root@flash html]# /sbin/service iptables save
儲存目前的設定到 /etc/sysconfig/iptables:[  確定  ]
```

當我們開機時會啟動 iptables。我們組態防火牆 iptables 的執行層級為 2、3、4、5。

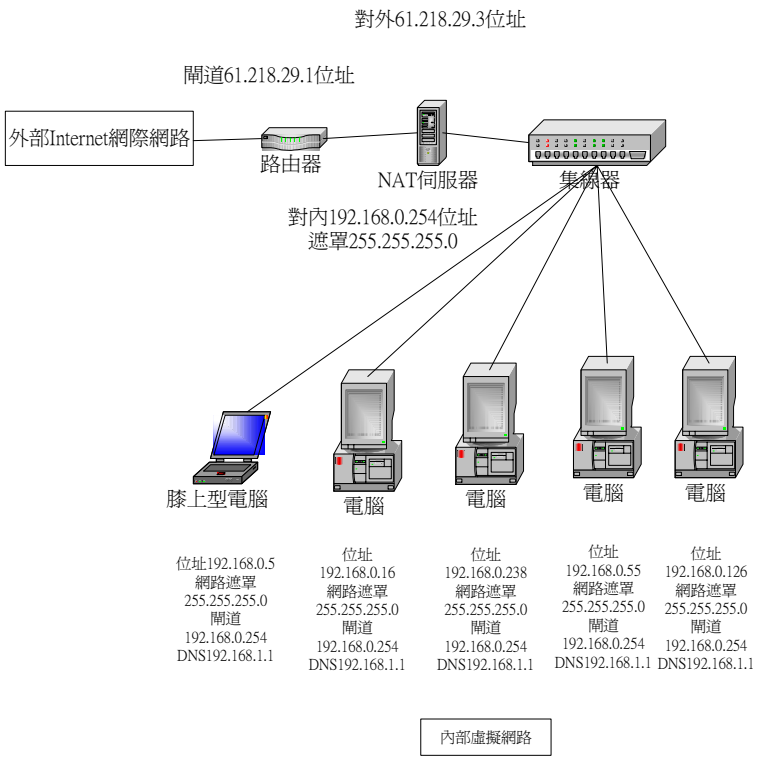
#/sbin/chkconfig --level 2345 iptables on

#/sbin/chkconfig --list iptables

```
[root@flash html]# /sbin/chkconfig  --level  2345 iptables on
[root@flash html]# /sbin/chkconfig  --list  iptables
iptables        0:關閉  1:關閉  2:開啓  3:開啓  4:開啓  5:開啓  6:關閉
```

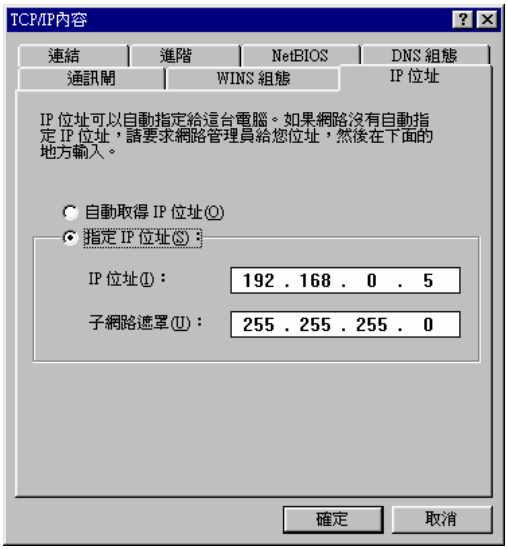
30-2 NAT 伺服器實務應用

我們可以使用 NAT 伺服器當作網址偽裝(MASQUERADE)。我們可以使用一個固定 IP 位址對外，然後有多台的電腦使用虛擬 IP 位址。這樣我們就可以讓我們的多台電腦只使用一個固定 IP 或浮動 IP 就可以上網了。我們在這裏使用 flash.aasir.com 的網站來作實務應用。網站的閘道為 61.218.29.1。而我們的網站 IP 為 61.218.29.3，它也是當作 NAT 伺服器，NAT 伺服器為網路轉換位址伺服器。我們對內的 IP 位址為 192.168.0.254，它的遮罩是 255.255.255.0，因此總共可有有 253 個虛擬 IP，也就是 253 台電腦可以使用 61.218.29.3 個位址。在這裏我們將以 192.168.0.5 這台網址偽裝電腦來作實務運用。



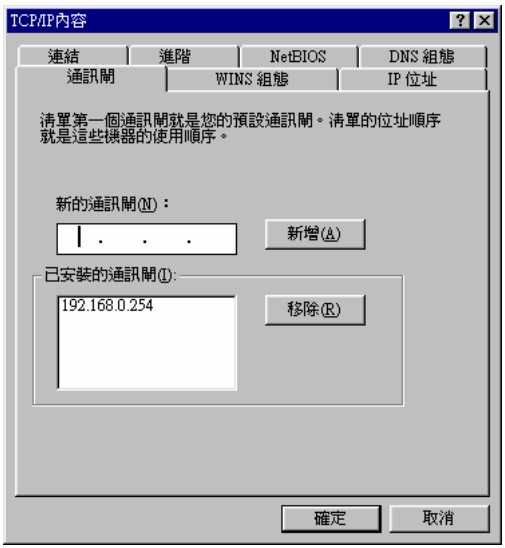
30-2-1 設定內部虛擬網路

這是我們內部虛擬網路的電腦，它的 IP 位址為 192.168.0.5。它的網路遮罩是 255.255.255.0。



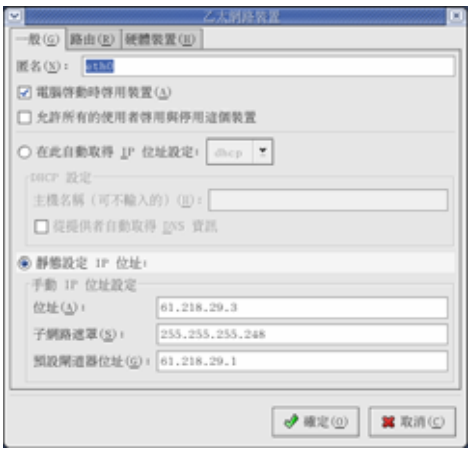
這是我們 DNS 的組態。我們要設定我們的名稱伺服器為 168.95.1.1。

我們要設定我們的通訊閘，閘道的 IP 為 192.168.0.254，也就是 NAT 網路位址轉換伺服器的內部 IP192.168.0.254。

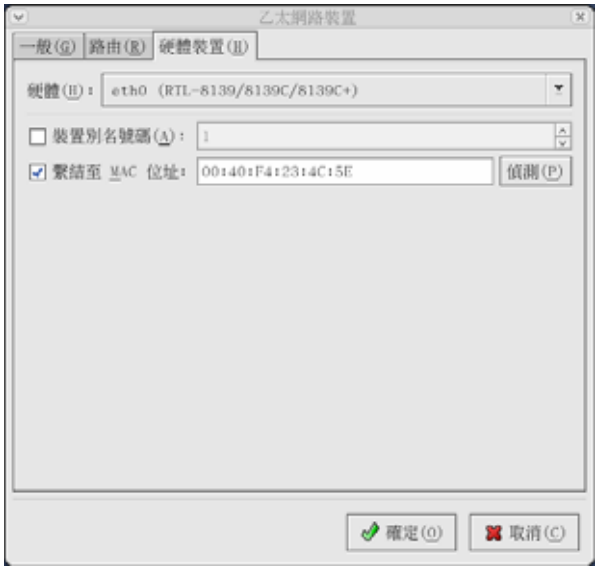


30-2-2 設定 NAT 伺服器的兩張網卡

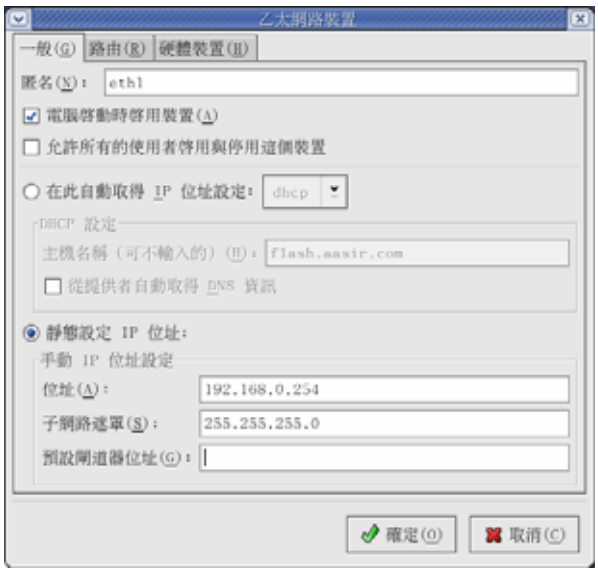
我們使用 eth0 網卡來對外，而使用 eth1 網卡來對內。eth0 是對外的網路卡，它的位址是 61.218.29.3、網路遮罩是 255.255.255.248、閘道是 61.218.29.1。



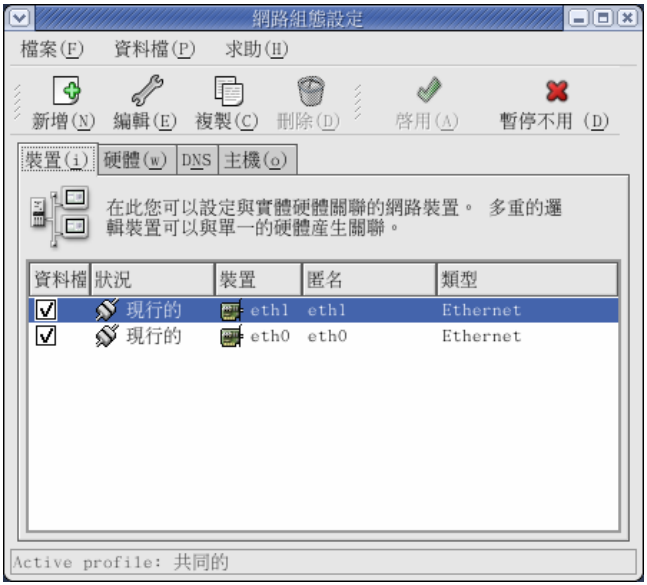
這是 eth0 網路卡的硬體裝置。



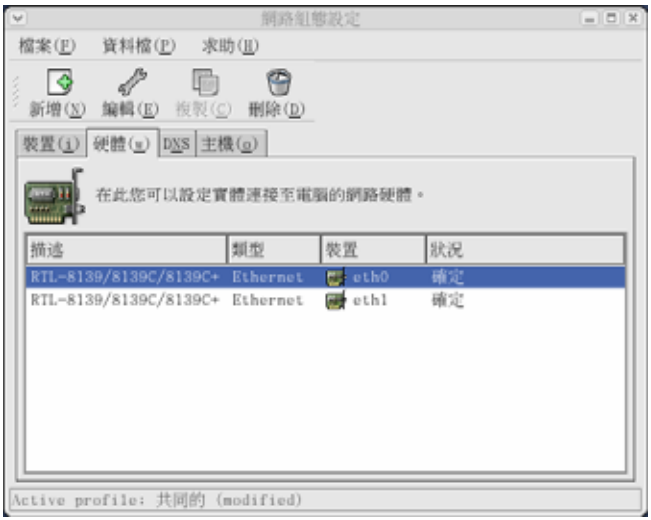
這是第二張網路卡 eth1 的設定，它的匿名為 eth1，而它的位址為 192.168.0.254，而它的網路遮罩是 255.255.255.0，它的閘道位置不用設。



這是兩張網路卡 eth0 和 eth1 裝在 NAT 伺服器上。



這是 eth1 和 eth0 網路卡的硬體，都是螃蟹卡 RTL8139。



這是 NAT 伺服器的主機，名稱為 flash.aasir.com，而其 IP 為 61.218.29.3。

這是 eth0 網路卡 DNS 的設定，我們設定其名稱伺服器為 168.95.1.1。

30-2-3 NAT 上設定偽裝的 iptables

我們使用 iptables –t nat –L –n，就可以觀看我們 iptables 網路濾器在 NAT 伺服器上的串列規則。-t nat 是指定使用 NAT 表。-L 串列是列出所有串列的規則。-n 是位址和連接埠的數字輸出。

```
[root@flash 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
You have new mail in /var/spool/mail/root
[root@flash root]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@flash 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
[root@flash root]# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[root@flash root]# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@flash root]#
```

我們使用 echo 1 > /proc/sys/net/ipv4/ip_forward 來啟動 IP 轉向 forwarding。

```
[root@flash root]# echo 1 > /proc/sys/net/ipv4/ip_forward
```

我們使用 iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE 來輸出偽裝的封包。-t nat 是指定使用 NAT 表。-A 是指將規則加入串列中。POSTROUTING 只用在 NAT 表上，是轉向或修改輸出封包的規則。-o eth0 是指定輸出的網路介面卡 eth0，用來轉向或輸出串列。-j 指定轉向目標的連接埠。MASQUERADE 為偽裝。

```
[root@flash root]# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

我們也可以將我們的串列規則寫到 filter，然後再執行串列規則./filter，這樣比較方便，只要執行./filter。

```
[root@flash 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
You have new mail in /var/spool/mail/root
[root@flash root]# ./filter
[root@flash root]# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

我們可以使用 vi　filter 來編輯串列規則。

```
[root@flash root]# vi filter
```

我們在第一行使用 echo 1 > /proc/sys/net/ipv4/ip_forward 來啟動 IP 轉向 forwarding。我們在第二行使用 iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE 來輸出偽裝的封包。MASQUERADE 為偽裝。

```
1 echo 1 > /proc/sys/net/ipv4/ip_forward
2 iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

30-3 ipchains

我們也可以使用 ipchains 指令來作位址 IP 的偽裝以及封包的過濾。ipchains 也可以用來作封包的過濾，ipchains 封包過濾有三個類型 input、forward 和 output。

語法：

指令：

ipchains	加入或刪除	input forward output	過濾對象	來源位址	目地位址	-j	拒絕或接受或轉向

參數：

選項	說明
-A 串列	將規則加入串列中
-D 串列	從串列中刪除合適的規則
-D 串列 規則編號	從串列中刪除規則編號
-I 串列 規則編號	插入新的 ipchains 規則(預設 1=first)
-R 串列 規則編號	取代串列中的規則編號
-L 串列	列出指定串列或所有串列的規則
-F 串列	刪除串列中的所有規則
-Z 串列	將所有規則的封包和串列計數歸 0
-C 串列	在串列中測試封包。
-N 串列	建立新的使用者定義串列。
-X 串列	刪除使用者定義串列。
-P 串列目標	更改串列或目標的策略。
-M – L	列出顯示目前偽裝的連接
-M – S tcp tcpfin udp	設定偽裝終止時間的數值。
-h	顯示指令說明
--version	版本
目標選項(拒絕、接受、轉向、偽裝、會回傳)	說明
ACCEPT	允許封包穿越防火牆
DENY	刪除封包。

REJECT	刪除封包，但會通知傳送者。
MASQ	將封包偽裝。
REDIRECT	重新轉向封包到本地端 像在 iptables 中的 NAT 工作。
RETURN	跳到串列的最後，而且讓目標選項處理它。

我們使用 ipchains 指令。-A 表示加入 input 輸入串列，來允許所有來自(-s 參數)192.168.0.55 位址的封包，允許穿越(-j ACCEPT 目標選項)防火牆。

```
[root@aasir chaiyen]# ipchains -A input -s 192.168.0.55 -j ACCEPT
```

我們可以使用目標選項的-j DENY 來拒絕來自指定網站(www.aasir.com)的存取。在 iptables 中這是 DROP 選項。

```
[root@aasir chaiyen]# ipchains -A input -s www.aasir.com -j DENY
```

我們可以指定在 192.168.0.1~192.168.0.255 的網域範圍內的來源皆可存取和通過我們的防火牆。我們使用 192.168.0.1/24 或者我們也可以使用 192.168.0.1/255.255.255.0。在這裏 255.255.255.0 是網路遮罩。

```
[root@aasir chaiyen]# ipchains -A input -s 192.168.0.1/24 -j ACCEPT
```

我們使用!(not)來指定在 192.168.0.1~192.168.0.255 的網域範圍內的來源皆不可存取和通過我們的防火牆。

```
[root@aasir chaiyen]# ipchains -A input ! -s 192.168.0.1/24 -j ACCEPT
```

我們使用 ipchains 指令來增加(-A 參數)轉向。從 192.168.0.0 的網域(-s 192.168.0.0/24)使用偽裝(-j MASQ 選項參數)轉送到目的地為網域網路(-d 0.0.0.0/0)。

```
[root@aasir chaiyen]# ipchains -A forward -s 192.168.0.0/24 -d 0.0.0.0/0 -j MASQ
```

課後練習

1.大大公司最進將他們公司的網路連接到 Internet，而大大公司有一台 P4 的電腦，和下列的一些作業系統，請問大大公司應該選擇哪一台電腦和作業系統，這樣才能夠控制大大公司的網路安全?

(A). 使用 windows98 加趨勢科技，並將它們安裝到 P4 的電腦

(B). 使用 Macintosh 麥金塔電腦加上諾頓

(C). 使用 Linux 作業系統加上 iptables，並將它們安裝到 P4 電腦

(D). 使用 windows me 並將它們安裝到 P4 電腦

2. 為了防止我們的網站或網域遭受到駭客的入侵破壞，我們使用防火牆將我們的網路資源分成軍事區和非軍事區(demilitarized zone 簡稱 DMZ)。下列何者的內部網路是放置受保護的網路資源，且嚴格禁止外部網際網路或駭客進入？

(A). 軍事區

(B). 非軍事區

(C). 環狀網路

(D). 乙太網路

3. 一個好的網路安全基礎，就是在我們作業系統中建立防火牆，來保護我們作業系統來自未授權的攻擊。我們可以使用下列何者來作封包過濾或代理?

(A). 軍事區

(B). 乙太網路

(C). 防火牆

(D). 環狀網路

4. 下列何者指令定義一個規則，而這個規則拒絕所有從 192.168.75.0 的子網域，然後它會送出給該使用者”destination unreachable”的錯誤資訊。

(A). A./sbin/iptables -A INPUT -s 192.168.75.0/24 -j REJECT

(B). B./sbin/iptables -A INPUT -s 192.168.75.0 -p icmp -j DROP

(C). C./sbin/iptables -A FORWARD -j DROP

(D). D./sbin/iptables -A INPUT -s 192.168.75.0/24 -p icmp -j DROP

5. 我們可以使用下列何者伺服器當作網址偽裝(MASQUERADE)?我們可以使用一個固定 IP 位址對外，然後有多台的電腦使用虛擬 IP 位址。這樣我們就可以讓我們的多台電腦只使用一個固定 IP 或浮動 IP 就可以上網了。

(A). DHCP 伺服器

(B). NAT 伺服器

(C). FTP 伺服器

(D). NIS 伺服器

6. 我們使用下列何者來啟動 Linux 核心提供 IP 轉向 forwarding 的功能。

(A). /sbin/chkconfig --level 2345 iptables on

(B). /sbin/iptables -A FORWARD -j DROP

(C). iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE

(D). echo 1 > /proc/sys/net/ipv4/ip_forward

【答案】

1.→C 2.→A 3.→C 4.→A 5.→B 6.→D