防火牆和代理伺服器 - HOWTO

作者: Mark Grennan, markg@netplus.net
譯者: 趙平望 tchao@worldnet.att.net
v0.4, 1996年11月8日

v0.4, 1996年11月8日，這篇文章主要在于說明防火牆系統的各種基本概念，並示範在Linux爲基礎的個人電腦上安裝作爲過濾之用的防火牆和代理伺服器的詳細步驟。這份文件的HTML版本載于 *http://okcforum.org/~markg/Firewall-HOWTO.html*

目錄

1 導言

最初的這篇“防火牆 - HOWTO”是David Rudder**drig@execpc.com**的作品。他讓我在他的原稿上增訂內容，對此我深表感謝。 最近這一陣子, 防火牆（Firewall）成了網際網路的安全問題的熱門話題。但像許多其他熱門話題一樣，這也同時造成了許多人對它的誤解。這篇HOWTO 將會探討什麼是防火牆？如何安裝？何謂代理伺服器（Proxy Server）？如何設定代理伺服器？以及這些技術在安全領域以外的應用。

1.1 讀者回應

如果發現這篇文章中有任何錯誤, 請務必通知我。人非聖賢, 孰能無過! 任何錯誤我都樂于更正。來信我都會設法回覆, 但我相當忙, 如果沒有收到我的回信，還請包涵。回信地址***markg@netplus.net***

如果發現任何誤譯之處，請立即通知本文譯者：趙平望（tchao@worldnet.att.net)。

1.2 嚴正聲明

我不對任何依照本文所做行爲造成的損害負任何責任**(I AM NOT RESPONSIBLE FOR ANY DAMAGES INCURRED DUE TO ACTIONS TAKEN BASED ON THIS DOCUMENT)**。這篇文章只介紹防火牆和代理伺服器的作用。要知道，我不是電腦安全問題專家，也從來沒有裝成這方面的專家。我只是個喜歡讀書，而且愛電腦勝過愛人類的傢伙。我希望這篇文章能幫助你熟悉這個主題, 但不保証內容絕對無誤。

1.3 版權宣告 (譯注：版權宣告不譯)

1.4 寫這篇文章的動機

儘管去年在comp.os.linux上有許多關于防火牆問題的討論，但我發現很難找到設定防火牆所需的資料。這篇HOWTO的原先版本提供了一些幫助，但內容仍嫌不足。我根據David Rudder編寫的Firewall HOWTO作了增訂，希望這篇文章提供了足夠的資料，使你能在幾小時內就能設定一個可以運作的防火牆，而不再需要花幾星期之久。 我也認爲我應該略盡綿力，回報愛好Linux的朋友。

1.5 有待完成的工作

- 指導如何設定客户機
- 尋找能與Linux搭配的UDP代理伺服器

1.6 延伸讀物

- NET-2 HOWTO
- Ethernet HOWTO
- Multiple Ethernet Mini HOWTO
- Linux的聯網
- PPP HOWTO
- O'Reilly and Associates出版的TCP/IP Network Administrator's Guide
- TIS Firewall Toolkit的文件

在 Trusted Information System (TIS) 網址上收集了許多有關防火牆的文件和相關材料。**http://www.tis.com/**

此外，我也正在從事一項稱爲*Linux*安全（*Secure Linux*）的項目。在*Secure Linux*網址上，我收集了所有使Linux安全可靠的資料、文件和程式。如果你需要這方面的資料，請來信索取。

2 什么是防火牆

防火牆是汽車中一個部件的名稱。在汽車中，利用防火牆把乘客和引擎隔開，以便汽車引擎一旦著火，防火牆不但能保護乘客安全，而同時還能讓司機繼續控制引擎。 在電腦中，防火牆是一種裝置，可使個別網路不受公共部分（整個網際網路）的影響。 此後，文中將防火牆電腦稱爲“防火牆”，它能同時連接受到保護的網路和網際網路兩端。但受到保護的網路無法接到網際網路，網際網路也無法接到受到保護的網路。 如果要從受到保護的網路內部接到網際網路，就得telnet到防火牆，然後從防火牆聯上網際網路。 最簡單的防火牆是dual homed系統（具有兩個網路聯結的系統）。如果你能相信所有你的用户，那你只要裝設一台Linux（設定時將 IP forwarding/gatewaying 設爲 OFF），並讓每人設一帳户。他們隨後能登錄這一系統，使用telnet、FTP，閱讀電子函件和使用所有你提供的任何其他服務。根據這項設置，這一網路中唯一能與外界聯系的電腦便是這個防火牆。在這個網路中的其他電腦甚至不需要一條公用的路徑。 需要再次說明：要使上述防火牆發揮作用，就必須相信所有用户！不過，我可不敢這么建議。

2.1 防火牆的缺陷

用于過濾之用的防火牆的問題是這種防火牆不讓網際網路進入你的網路。只有通過過濾防火牆才能取用功能。在有代理伺服器的情況下，用户可登錄到防火牆，然後進入私有網路内的任何系統。 此外，目前幾乎每天都有新型客户機和伺服器上市。因此，得要有新的方法進入網路才能調用這些功能。

2.2 防火牆的種類

防火牆有兩種。

1. IP過濾防火牆 - 除一些網路功能外阻擋一切聯網功能。
2. 代理伺服器 - 替你進行網路聯結。

2.2.1 IP過濾防火牆

IP過濾防火牆在數據包一層工作。它依據起點、終點、埠號和每一數據包中所含的數據包種類信息控制數據包的流動。 這種防火牆非常安全，但是缺少有用的登錄記錄。它阻擋別人進入個別網路，但也不告訴你何人進入你的公共系統，或何人從內部進入網際網路。 過濾防火牆是絕對性的過濾系統。即使你要讓外界的一些人進入你的私有伺服器，你也無法讓每一個人進入伺服器。 Linux從1.3.x版開始就在內核中包含了數據包過濾軟件。

2.2.2 代理伺服器

代理伺服器允許通過防火牆間接進入網際網路。最好的例子是先telnet系統，然後從該處再telnet另一個系統。在有代理伺服器的系統中，這項工作就完全自動。利用客户端軟件連接代理伺服器後，代理伺服器啓動它的客户端軟件（代理），然後傳回數據。 由于代理伺服器重複所有通訊，因此能夠記錄所有進行的工作。 只要配置正確，代理伺服器就絕對安全，這最它最可取之處。它阻擋任何人進入，因爲沒有直接的IP通路。

3 設置防火牆

3.1 硬件需求

在範例中，所用的電腦配置是一塊486-DX66芯片，16M內存和500M Linux分割。系統內還裝了兩張網路卡，一張連到私有網路，另一張接到一個稱爲“非軍事區”的網路（譯註：指公用網路），而在這個非軍事區的網路上，有一個接到網際網路的路由器（router）。 這種配置極爲常見，甚至還可用一張網卡和一台數據機通過PPP接到網際網路，但關鍵之處是防火牆上必須有兩個IP號碼。 不少人家中都有小網路，把兩、三台電腦接在一起。不妨試試把所有數據機都接在跑Linux的電腦上（老舊的386機），然後利用負載平衡的方式把數據機都接到網際網路。利用這種裝置，如果要傳輸數據，兩部數據機同時工作，可加倍傳輸的速度。

4 設置防火牆的軟件

4.1 現有的套裝軟件

如果只要設置一個過濾防火牆，那只要Linux和基本網路軟件就夠了。有一套軟件可能不在你使用的Linux版本中，稱爲 IP Firewall Administration工具。 (IPFWADM) 可從**http://www.xos.nl/linux/ipfwadm/**取得。 如果要設置代理伺服器，就需要一個這種套裝軟件。

1. SOCKS
2. TIS Firewall Toolkit (FWTK)

4.2 TIS Firewall Toolkit 和SOCKS間的差異

Trusted Information System (**http://www.tis.com**)提供了一系列軟件，用以簡化安裝防火牆的工作。這些軟件基本上同SOCKS的軟件相同，但設計策略不同。SOCKS利用一套軟件執行所有與Internet有

關的工作，而TIS對每一個希望使用防火牆的utility都提供一個軟件。 爲了說明兩者之間的不同，就以world wide web和Telnet爲例吧！在SOCKS中，設定一個設置（configuration）檔和一個daemon後，telnet和WWW都能開始工作，同時其他沒有關閉的功能也都能夠運作。 但在TIS中，爲WWW和telnet都得設定各自的configuration檔和daemon。經此設定後，其他internet的功能仍無法運用，除非對這些功能也作出相關的設定。如果某一功能（例如talk）沒有daemon，雖然有"plug-in" daemon可用，但它不像其他工具那樣靈活，而且也不易設定。 這似乎是小事，但且大有差別。設置SOCKS時比較可以隨意。如果SOCKS伺服器的設置不太完美，從網路內部可以調用原先並不打算提供的internet功能。如使用TIS，從網路內部只能調用系統管理者規定的功能。 SOCKS易于設定、易于編輯，並且靈活性較高。如要管制受到保護的網路內的使用者，則TIS的安全性較高。不過兩者都提供了絕對保護，外界無法進入。 我會說明兩者的安裝和設定方法。

5 設定Linux系統

5.1 編輯內核

首先利用Linux版本重新安裝Linux系統（我用RedHat 3.0.3，此後實例均以這一版本爲準）。系統中安裝的軟件越少，毛病和漏洞也越少，因爲這些毛病和漏洞對系統的安全都會產生問題，所以只要安裝夠用的最少量軟件即可。 選用一個穩定的內核。我的系統用了Linux 2.0.14的內核。 因此，這份文件以這種內核設置爲基礎。 根據適當的選項（options）重新編輯內核。 如果以前沒有讀過Kernel HOWTO、 Ethernet HOWTO和NET-2 HOWTO，此時不妨利用這個機會讀一讀這些HOWTO。 以下是在‘make config’內與網路有關的設定。

1. 在General setup中
   (a) 設Networking Support 爲ON
2. 在Networking Options中
   (a) 設Network firewalls爲 ON
   (b) 設TCP/IP Networking爲 ON
   (c) 設IP forwarding/gatewaying爲 OFF （除非要用IP過濾）
   (d) 設IP Firewalling爲ON
   (e) 設IP firewall packet loggin爲 ON（不是必需，設了更好）
   (f) 設IP: masquerading 爲OFF（不屬本文范圍）
   (g) 設IP: accounting 爲ON
   (h) 設IP: tunneling 爲OFF
   (i) 設IP: aliasing 爲OFF
   (j) 設IP: PC/TCP compatibility mode 爲OFF
   (k) 設 IP: Reverse ARP 爲OFF
   (l) 設Drop source routed frames 爲ON
3. 在Network device support項下
   (a) 設Network device support 爲ON
   (b) 設Dummy net driver support 爲ON

(c) 設Ethernet (10 or 100Mbit) 爲ON

(d) 選擇網路卡

現在重新編輯，重新安裝內核，重新啓動。網路卡應在啓動的提示中顯示。如果沒有抓到網路卡，查閱其他HOWTO，直到設對爲止。

5.2 設定兩張網路卡

電腦中如有兩張網路卡，極可能需要在/etc/lilo.conf檔中增加一行，說明兩張網路卡的IRQ和地址。在我的機器中，lilo.conf檔增加的一行如下：

```
append="ether=12,0x300,eth0 ether=15,0x340,eth1"
```

5.3 設定Network Addresses

這部分比較有趣，而且得要做些決定。由于不打算讓網際網路進入自設網路的任何部分，因此網路中不需要用實際的網址。在網際網路中留了一些地址可讓網路隨意使用，因爲自設網路總得需要地址，而且這些地址也無法進入網際網路，攪渾全局。因此不妨選用這些地址。 在這些地址中，192.168.2.xxx是被留用的地址，因此就用這些地址來作說明。

由于代理伺服器同時身處兩個網路，因此它能居中傳送兩邊的數據。

```
          199.1.2.10   __________    192.168.2.1
  _  __  _        \ |          | /          ---------------
 | \/  \/ |        \|          |/           |             |
  網際網路 \-------------| 防火牆 |--------------------| 工作站      |
  \_/\_/\_/\_/          |_________|           |______________|
```

如要設置過濾防火牆，依舊可用這些網址，不過得使用IP masquerading。經過這種設定，防火牆就會轉送數據包，並加附實際的IP地址送往網際網路。 在網路卡的網際網路端（外端）得設定眞正的IP地址，在以太網卡的內端設爲192.168.2.1。這是這台電腦代理/網關的IP地址。受保護的網路內的所有其他電腦均可選用192.168.2.xxx中的任何一個作爲地址（從192.168.2.2 到192.168.2.254）。 在RedHat Linux 中，得在 /etc/sysconfig/network-scripts目錄下增加一個ifcfg-eth1檔，以便在啓動時，通過這個檔設定網路和routing表。 ifcfg-eth1的參數可設定如下：

```
#!/bin/sh
#>>>Device type: ethernet
#>>>Variable declarations:
DEVICE=eth1
IPADDR=192.168.2.1
NETMASK=255.255.255.0
NETWORK=192.168.2.0
BROADCAST=192.168.2.255
GATEWAY=199.1.2.10
ONBOOT=yes
#>>>End variable declarations
```

可試用這些參數使數據機與ISP自動連接。不妨看看 ipup-ppp檔。 如用數據機與網際網路連接，ISP會在連接時指定外端的IP地址。

5.4 測試網路

從測試ifconfig和route開始。如機器上有兩張網路卡，各項設置應有如下情況：

```
#ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.0  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:1
          RX packets:1620 errors:0 dropped:0 overruns:0
          TX packets:1620 errors:0 dropped:0 overruns:0

eth0      Link encap:10Mbps Ethernet  HWaddr 00:00:09:85:AC:55
          inet addr:199.1.2.10 Bcast:199.1.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:0
          Interrupt:12 Base address:0x310

eth1      Link encap:10Mbps Ethernet  HWaddr 00:00:09:80:1E:D7
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:0
          Interrupt:15 Base address:0x350
```

route 表應看起來如下：

```
#route -n
Kernel routing table
Destination   Gateway   Genmask     Flags  MSS  Window  Use  Iface
199.1.2.0     *        255.255.255.0   U   1500   0      15 eth0
192.168.2.0   *        255.255.255.0   U   1500   0       0 eth1
127.0.0.0     *        255.0.0.0      U   3584   0      2 lo
default      199.1.2.10   *           UG  1500   0      72 eth0
```

注： 199.1.2.0在防火牆的網際網路端，192.168.2.0在自設網路一端。 首先試試從防火牆ping 網際網路。不妨把nic.ddn.mil作試驗點。這個試驗點還不錯，只是不如我預期的可靠。如果沒聯上，試試ping幾個不是你網路上的地址。如果仍聯不上，則PPP的設定一定不對。再讀一次Net-2 HOWTO，然後再試。 然後，試驗從防火牆ping保護網路內的電腦。所有網路內的電腦應能ping網路內的任何其他一台電腦。如果不行，再讀讀Net-2 HOWTO，再試一次。 接著試驗從保護網路內ping防火牆以外的地址。（注意：不屬于192.168.2.xxx的任何地址）如果可以，表示IP Forwarding的功能沒有取消。想一想這是否符合原先的構想。如果保留IP Forwarding的功能，就別放過下面設定IP filtering的部分。 現在試試從防火牆後ping 網際網路。利用以前試通的同一地址（例如，nic.ddn.mil）。如果 IP Forwarding功能已經取消，就不應接通。不過如果這項功能沒有取消，就應該接通。 假設保留了IP Forwarding功能，而

在自設的網路中使用實際的IP地址（不是192.168.2.*），在這種設定下，如果無法ping 網際網路，但能夠ping網際網路邊的防火牆，就得檢查上一層的router有否把數據包傳送到自設網路的地址上。（可能得由ISP作這項檢查） 如果保護網路的地址定爲192.168.2.*，則任何數據包都不能傳送。如果沒有作這些設定，而使用了IP masquerading，這項試驗應該成功。 至此，各項設定基本完成。

5.5 加固防火牆

如果通過防火牆上沒有使用的功能能夠隨意進出防火牆，則這種防火牆也就沒有什么用處。"駭客"能到防火牆內作出必要的修改，供其所用。 首先關閉所有不用的功能。先檢查 /etc/inetd.conf檔。這個檔控制所謂的"超級伺服器"。它控制了許多伺服器的daemon，然後在需要時啓動這些daemon。 完全取消netstat、 systat、 tftp、 bootp和finger功能。取消功能的方法是把#作爲功能行的行首字母。設定完畢後，鍵入"**kill -HUP <pid>**"，執行SIG-HUP，其中<pid>是inetd的程序編號。inetd會再次讀取配置檔（inetd.conf），並從新啓動系統。 利用telnet 測試防火牆的埠號（port）15，這是netstat的埠號。如netstat回應網路情況，系統並沒有按要求正確地從新啓動。

6 IP filtering 的設置(IPFWADM)

首先設定內核的IP Forwarding功能，系統應開始轉送每一信息。路徑表（routing table）應已設定，因此應該可以通往任何地點，從網內可以聯到網外，從網外也可進到網內。 但是防火牆的作用是不讓任何人可以隨便進出網路。 在示範系統中設定了兩套指令（script），對防火牆的forwarding和accounting作了規定。系統在運行/etc/rc.d時取用這兩套指令，因此在系統啓動時就對系統作了設置。 Linux的內核自設轉送一切信息的IP Forwarding系統。因此，防火牆的指令應首先禁止一切進入系統的權利，清除上次運行後留下的任何ipfw規則。下面的指令應能達到這項目的。

```
#
# setup IP packet Accounting and Forwarding
#
#   Forwarding
#
# By default DENY all services
ipfwadm -F -p deny
# Flush all commands
ipfwadm -F -f
ipfwadm -I -f
ipfwadm -O -f
```

好了，現在有了絕對保險的防火牆。一切都被屏擋在外面，無法穿越防火牆一步。當然，有些功能還是需要的，下面的一些例子可作參考。

```
# Forward email to your server ：轉送電子郵件到伺服器
ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 192.1.2.10 25
```

```
# Forward email connections to outside email servers ：將電子郵件連到網路外的電子郵件伺服器
ipfwadm -F -a accept -b -P tcp -S 196.1.2.10 25 -D 0.0.0.0/0 1024:65535
```

```
# Forward Web connections to your Web Server：將Web連到Web伺服器
/sbin/ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 196.1.2.11 80

# Forward Web connections to outside Web Server：將Web連到外界Web伺服器
/sbin/ipfwadm -F -a accept -b -P tcp -S 196.1.2.* 80 -D 0.0.0.0/0 1024:65535

# Forward DNS traffic：轉送DNS信息
/sbin/ipfwadm -F -a accept -b -P udp -S 0.0.0.0/0 53 -D 196.1.2.0/24
```

如果想知道通過防火牆的信息來往情況，下列指令會統計所有數據包。

```
# Flush the current accounting rules
ipfwadm -A -f
# Accounting
/sbin/ipfwadm -A -f
/sbin/ipfwadm -A out -i -S 196.1.2.0/24 -D 0.0.0.0/0
/sbin/ipfwadm -A out -i -S 0.0.0.0/0 -D 196.1.2.0/24
/sbin/ipfwadm -A in -i -S 196.1.2.0/24 -D 0.0.0.0/0
/sbin/ipfwadm -A in -i -S 0.0.0.0/0 -D 196.1.2.0/24
```

如果只把電腦設爲過濾防火牆，到這裡就大功告成了！

7 安裝TIS代理伺服器

7.1 取得軟件

TIS FWTK軟件可從下列網址得到：**ftp://ftp.tis.com/**. 千萬記住：從TIS下載軟件後，首先閱讀README。TIS fwtk存放在伺服器的一個隱藏目錄內，需要發電子郵件給**fwtk-request@tis.com** 並在信文內填入**SEND**才能得知隱藏的目錄的名字。Subject欄內不必填入任何內容。在回覆的電子郵件內會告知存放軟件的目錄的名字，有效時間爲12小時，得趕快下載。 在編寫本文時，FWTK的最新版本爲2.0（beta）。除了幾個小地方之外，這個版本在編輯時沒有問題，運行時也正常，此處就以這一版本爲例。如有最後定本時，將在以後的HOWTO中增訂。 安裝FWTK時，首先在 /usr/src下建立fwtk-2.0目錄。將FWTK（fwtk-2.0.tar.gz）放在這個目錄內解壓（tar zxf fwtk-2.0.tar.gz）。 FWTK並無代理SSL的網路文件，Jean-Christophe Touvet寫了一些附加資料，可從**ftp://ftp.edelweb.fr/pub/contrib/fwtk/ssl-gw.tar.Z**取得。 Eric Wedel寫了修訂本，其中包括使用網景（Netscape）的新聞伺服器。這套軟件可從下列網址取得：**ftp://mdi.meridian-data.com/pub/tis.fwtk/ssl-gw/ssl-gw2.tar.Z** 以下以Eric Wedel的版本爲例。 要安裝，只要在/usr/src/fwtk-2.0目錄內建立一個 ssl-gw目錄，把文檔放在其中即可。 在安裝這個網關時，得要作些改動才能進行編輯。 首先改變ssl-gw.c檔，其中遺漏了必要的include檔。

```
#if defined(__linux)
#include        <sys/ioctl.h>
#endif
```

其次，也沒有Makefile檔。不妨從其他網關目錄拷貝一個，然後將網關的名字改爲ssl-gw。

7.2 編輯TIS FWTK

版本2.0的FWTK比以往任何一個版本都易于編輯。不過在編輯以前還需要對BETA版本作一些更動。希望這些更動會加附到最後定本中。修改方法如下：首先進入/usr/src/fwtk/fwtk目錄，拷貝Makefile.config.linux檔，以此檔替代Makefile.config檔。不要運行**FIXMAKE**。雖然在說明中建議執行這個程序。但運行後會破壞每一個目錄中的makefile。修改fixmake的方法是在每一個Makefile的sed指令的include行中添加‘.’和"。按下例更改，便可運行無礙。

```
sed 's/^include[        ]*\([^  ].*\)/include \1/' $name .proto > $name
```

然後需要編輯Makefile.config檔，但首先得作兩項修改。Makefile.config檔中的source目錄應改爲進行編輯的/usr/src，因此FWTKSRCDIR應作相應的改變。

```
FWTKSRCDIR=/usr/src/fwtk/fwtk
```

有些Linux系統使用gdbm數據庫。Makefile.config使用dbm。例如，RedHat 3.0.3就使用dbm，因此需要作出相應更動。

```
DBMLIB=-lgdbm
```

最後需要改x-gw。BETA版內socket.c中的下列數行必需刪除。

```
#ifdef SCM_RIGHTS  /* 4.3BSD Reno and later */
                     + sizeof(un_name->sun_len) + 1
#endif
```

如在FWTK源目錄中添加ssl-gw，則在Makefile的目錄單中也要加上ssl-gw。

```
DIRS=   smap smapd netacl plug-gw ftp-gw tn-gw rlogin-gw http-gw x-gw ssl-gw
```

完成上述修改後，運行**make**。

7.3 安裝TIS FWTK

運行**make install**。默認的安裝目錄是/usr/local/etc。可以改到更加安全可靠的目錄進行安裝，但也可以不改，也可將其特權改爲chmod 700。現在開始設定防火牆。

7.4 設置TIS FWTK

好！下面就比較有趣了！設定的系統要能調用這些新功能，並建立管制表管理這些功能。以下的說明並不是爲了要重寫TIS FWTK的使用手冊，其目的只是爲了顯示可行的設定、可能遇到的問題和解決的辦法。有三個文檔組成這些controls。

- /etc/services
  - 告訴系統所定功能在何埠號
- /etc/inetd.conf

  – 當服務埠有動作時告訴inetd啓動那個程式

- /usr/local/etc/netperm-table
  – 告訴FWTK同意和拒絕來往的用户

要FWTK發揮作用，應徹底編輯這些檔案。編輯這些功能檔而不正確設定 inetd.conf或netperm-table，可能使系統完全無法作用。

7.4.1 netperm-table檔

這個檔控制何人可以使用TIS FWTK的功能。首先應該想到防火牆兩邊的需求。網路外面的用户在進入網路之前應首先表明身份，但網路內部的用户則可直接通過。 在表明身份時，防火牆使用一個稱爲**authsrv**的程式，其中存有用户的ID和密碼。netperm-table中的authentication部分控制這一數據庫存放何處和誰可取用。 要不讓人取用這一功能並不容易，在premit-hosts這一行中使用“*”，以致每人都能取用這一功能。這一行的正確設定應該是“`authsrv: premit-hosts localhost`”，但似乎不起作用。

```
#
# Proxy configuration table： 代理伺服器設置表
#
# Authentication server and client rules
authsrv:      database /usr/local/etc/fw-authdb
authsrv:      permit-hosts *
authsrv:      badsleep 1200
authsrv:      nobogus true
# Client Applications using the Authentication server
*:            authserver 127.0.0.1 114
```

要啓動數據庫，以root在/var/local/etc內運行**./authsrv**，設立管理者的使用記錄。實際操作如下： 閲讀FWTK文檔了解如何添加用户和用户組。

```
#
# authsrv
authsrv# list
authsrv# adduser admin "Auth DB admin"
ok - user added initially disabled
authsrv# ena admin
enabled
authsrv# proto admin pass
changed
authsrv# pass admin "plugh"
Password changed.
authsrv# superwiz admin
set wizard
authsrv# list
Report for users in database
```

```
user   group  longname          ok?    proto   last
------ ------ ----------------- -----  ------  -----
admin         Auth DB admin     ena    passw   never
authsrv# display admin
Report for user admin (Auth DB admin)
Authentication protocol: password
Flags: WIZARD
authsrv# ^D
EOT
#
```

Telnet的網關（tn-gw）控制直接了當，應首先設定。例如，允許在保護網路內的用户不表明身份直接通過(permit-hosts 196.1.2.* -passok)。但其他用户必需提供用户ID和密碼才可使用代理伺服器(permit-hosts * -auth)。此外，有一個系統(196.1.2.202)也可直接使用防火牆。這只要設定inetacl-in.telnetd的內容即可。Telnet的timeout時間應該短暫。

```
# telnet gateway rules:
tn-gw:              denial-msg      /usr/local/etc/tn-deny.txt
tn-gw:              welcome-msg     /usr/local/etc/tn-welcome.txt
tn-gw:              help-msg        /usr/local/etc/tn-help.txt
tn-gw:              timeout 90
tn-gw:              permit-hosts 196.1.2.* -passok -xok
tn-gw:              permit-hosts * -auth
# Only the Administrator can telnet directly to the Firewall via Port 24
netacl-in.telnetd: permit-hosts 196.1.2.202 -exec /usr/sbin/in.telnetd
```

r-command如同telnet的同一方式設定。

```
# rlogin gateway rules:
rlogin-gw:    denial-msg      /usr/local/etc/rlogin-deny.txt
rlogin-gw:    welcome-msg     /usr/local/etc/rlogin-welcome.txt
rlogin-gw:    help-msg        /usr/local/etc/rlogin-help.txt
rlogin-gw:    timeout 90
rlogin-gw:    permit-hosts 196.1.2.* -passok -xok
rlogin-gw:    permit-hosts * -auth -xok
# Only the Administrator can telnet directly to the Firewall via Port
netacl-rlogind: permit-hosts 196.1.2.202 -exec /usr/libexec/rlogind -a
```

任何人均不得直接進入防火牆，其中包括FTP，因此，不要把FTP伺服器放在防火牆上。再者，permit-hosts行允許保護網路內的任何人自由進入網際網路，其他人則必需表明身份。下文附上送到和收到的每份文檔的記錄（-log { retr stor }）。FTP的timeout開關控制在多少時間後停止試接，以及在多少時間沒有動作後，放棄試接。

```
# ftp gateway rules:
ftp-gw:             denial-msg      /usr/local/etc/ftp-deny.txt
ftp-gw:             welcome-msg     /usr/local/etc/ftp-welcome.txt
ftp-gw:             help-msg        /usr/local/etc/ftp-help.txt
```

```
ftp-gw:            timeout 300
ftp-gw:            permit-hosts 196.1.2.* -log { retr stor }
ftp-gw:            permit-hosts * -authall -log { retr stor }
```

通過WWW、gopher和瀏覽器進行的ftp由http-gw控制。最上面的兩行建立一個目錄，用于儲存經由防火牆的ftp和WWW文件。在本例中，這些文件屬root所有，因此放在只有root能夠進入的目錄內。WWW的連接應該短暫。它控制使用者在連接不通時的等待時間。

```
# www and gopher gateway rules:
http-gw:     userid          root
http-gw:     directory       /jail
http-gw:     timeout 90
http-gw:     default-httpd   www.afs.net
http-gw:     hosts           196.1.2.* -log { read write ftp }
http-gw:     deny-hosts      *
```

ssl-gw實際上是一個任何人都可通過的網關。應當當心設定。在本例中，任何保護網路中的用戶，除127.0.0.* 和192.1.1.* 外，均可連接網路外的任何伺服器，並只能使用443至563 埠號。443至563埠號一般稱爲SSL埠號。

```
# ssl gateway rules:
ssl-gw:   timeout 300
ssl-gw:   hosts           196.1.2.* -dest { !127.0.0.* !192.1.1.* *:443:563 }
ssl-gw:   deny-hosts      *
```

下面的例子說明如何利用plug-gw連接到新聞伺服器。在本例中，保護網路內的用户只允許連接到一個系統，即連接到它的新聞埠。 第二行使新聞伺服器將其資料送到保護網路。 對新聞伺服器的timeout時間設定應該比較長，因爲多數用户大都聯機閱讀新聞。

```
# NetNews Pluged gateway
plug-gw:        timeout 3600
plug-gw: port nntp 196.1.2.* -plug-to 199.5.175.22 -port nntp
plug-gw: port nntp 199.5.175.22 -plug-to 196.1.2.* -port nntp
```

Finger網關的設定至爲簡單。保護網路內的用户只要首先登錄，就可使用防火牆上的finger程式。任何其他人就只收到一段message。

```
# Enable finger service --------設定finger功能
netacl-fingerd: permit-hosts 196.1.2.* -exec /usr/libexec/fingerd
netacl-fingerd: permit-hosts * -exec /bin/cat /usr/local/etc/finger.txt
```

在這份HOWTO中，沒有設定Mail和X-windows功能。如任何人有這方面的實例，請發email給我。

7.4.2 inetd.conf的設置檔

下面附上/etc/inetd.conf的全部文檔。所有不需要的功能都用#符號注銷。在這份全部文檔中顯示取消了何種功能，以及顯示如何設定新的防火牆功能。

```
#echo stream  tcp  nowait  root               internal
#echo dgram   udp  wait    root       internal
#discard              stream  tcp  nowait  root       internal
#discard              dgram   udp  wait    root       internal
#daytime              stream  tcp  nowait  root       internal
#daytime              dgram   udp  wait    root       internal
#chargen              stream  tcp  nowait  root       internal
#chargen              dgram   udp  wait    root       internal
# FTP firewall gateway --------FTP防火牆網關
ftp-gw      stream  tcp  nowait.400  root  /usr/local/etc/ftp-gw  ftp-gw
# Telnet firewall gateway------Telnet防火牆網關
telnet        stream  tcp  nowait      root  /usr/local/etc/tn-gw /usr/local/etc/tn-gw
# local telnet services------用户的telnet功能
telnet-a    stream  tcp  nowait      root  /usr/local/etc/netacl in.telnetd
# Gopher firewall gateway------Gopher防火牆網關
gopher        stream  tcp  nowait.400  root  /usr/local/etc/http-gw /usr/local/etc/http-gw
# WWW firewall gateway------WWW防火牆網關
http  stream  tcp  nowait.400  root  /usr/local/etc/http-gw /usr/local/etc/http-gw
# SSL firewall gateway------SSL防火牆網關
ssl-gw  stream  tcp     nowait  root /usr/local/etc/ssl-gw   ssl-gw
# NetNews firewall proxy (using plug-gw)------NetNews防火牆代理伺服器（使用plug-gw）
nntp    stream  tcp     nowait  root    /usr/local/etc/plug-gw plug-gw nntp
#nntp stream  tcp     nowait  root    /usr/sbin/tcpd  in.nntpd
# SMTP (email) firewall gateway------SMTP（email）防火牆網關
#smtp stream  tcp     nowait  root    /usr/local/etc/smap smap
#
# Shell, login, exec and talk are BSD protocols------ Shell, login, exec and talk均 屬
BSD協議
#
#shell        stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
#login        stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
#exec stream  tcp     nowait  root    /usr/sbin/tcpd  in.rexecd
#talk dgram   udp     wait    root    /usr/sbin/tcpd  in.talkd
#ntalk        dgram   udp     wait    root    /usr/sbin/tcpd  in.ntalkd
#dtalk        stream  tcp     waut    nobody  /usr/sbin/tcpd  in.dtalkd
#
# Pop and imap mail services et al------Pop和imap mail功能
#
#pop-2   stream  tcp  nowait  root  /usr/sbin/tcpd    ipop2d
#pop-3   stream  tcp  nowait  root  /usr/sbin/tcpd    ipop3d
#imap    stream  tcp  nowait  root  /usr/sbin/tcpd    imapd
#
# The Internet UUCP service------網際網路UUCP功能
#
#uucp    stream  tcp  nowait  uucp  /usr/sbin/tcpd  /usr/lib/uucp/uucico -l
#
```

```
# Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers." Do not uncomment
# this unless you *need* it.  ----- Tftp功能主要用于啓動。一般只有作爲"boot伺服器"時才
需要tftp。因此，不要取消注銷（#）符號。
#
#tftp dgram   udp     wait    root    /usr/sbin/tcpd  in.tftpd
#bootps       dgram   udp     wait    root    /usr/sbin/tcpd  bootpd
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers."  Many sites choose to disable
# some or all of these services to improve security.------ Finger, systat and netstat會
向駭客提供可貴的資料。許多網站取消一些或全部功能，以增安全。
#
# cfinger is for GNU finger, which is currently not in use in RHS Linux
# cfinger是GNU finger，目前在RHS Linux中並不使用。
#
finger        stream  tcp  nowait  root   /usr/sbin/tcpd  in.fingerd
#cfinger      stream  tcp  nowait  root   /usr/sbin/tcpd  in.cfingerd
#systat       stream  tcp  nowait  guest  /usr/sbin/tcpd  /bin/ps -auwwx
#netstat      stream  tcp  nowait  guest  /usr/sbin/tcpd  /bin/netstat -f inet
#
# Time service is used for clock syncronization.-----時間功能用于設定時間的同步。
#
#time stream  tcp  nowait  root  /usr/sbin/tcpd  in.timed
#time dgram   udp  wait    root  /usr/sbin/tcpd  in.timed
#
# Authentication-----查驗用户身份
#
auth          stream  tcp  wait    root  /usr/sbin/tcpd  in.identd -w -t120
authsrv       stream  tcp  nowait  root  /usr/local/etc/authsrv authsrv
#
# End of inetd.conf-----inetd.cong設置檔結束
```

7.4.3 /etc/services檔

當用户連接到防火牆時，會接到一個已知的埠（小于1024）。例如，telnet接到埠23。inetd deamon接到連接的動作，查看/etc/services上這些功能的名字。然後，它會啓動/etc/inetd.conf檔中這個名字所指定的程式。 有時使用的功能並不在/etc/services檔中。這些功能可指定到任何想指定的埠。例如，管理員的telnet埠（telnet-a）可設定到埠24，也可設定到埠2323，悉聽尊便。如果管理員（指你本人）要直接連接到防火牆，則需telnet到埠24而非埠23。如按照下例設定netperm-table，則只能從保護的網路中的一個系統設定。

```
telnet-a         24/tcp
ftp-gw          21/tcp           # this named changed
auth            113/tcp   ident    # User Verification
ssl-gw           443/tcp
```

8 SOCKS代理伺服器

8.1 設定代理伺服器

SOCKS代理伺服器可從 **ftp://sunsite.unc.edu/pub/Linux/system/Network/misc/socks-linux-src.tgz**取得。該檔內也有一個稱爲"socks-conf"的設置檔可作參考。可把該檔解壓，然後根據其中的說明使用該檔。但使用時並不簡單，應首先確定Makefile檔正確無誤。 在 /etc/inetd.conf中應該增添代理伺服器。因此，應該增加以下一行。

```
socks  stream  tcp  nowait  nobody  /usr/local/etc/sockd  sockd
```

這樣伺服器才會在需要時運行。

8.2 設置代理伺服器

SOCKS需要兩個設置檔進行設定。一個設置檔設定進入取用的權限，另一個設置檔設定路徑，以便找到適當的代理伺服器。權限檔應在伺服器上，路徑檔應在每一台UNIX機上。DOS機和Macintosh機都會確定自行的路徑。

8.2.1 權限檔

在socks4.2（beta）版中，權限檔稱爲"sockd.conf"，應該只有兩行，一行允許（permit），一行拒絕（deny）。每行都有三項設定：

- 識別標示行(permit/deny)
- IP地址行
- 修改地址行

識別標示用于permit或deny。應該有單獨的permit行和單獨的deny行。 IP地址使用標準的4byte方式表示，如I.E. 192.168.2.0.。 修改地址行也是標準的4位元 IP地址，用來作爲netmask。將這個地址想成32位元的數字。如果是1，則核對的地址的相應位置應符合IP地址中相應的位元。例如，此行的地址爲：

```
permit 192.168.2.23  255.255.255.255
```

則只允許每一位元相符的地址，即192.168.2.23。如果地址爲：

```
permit 192.168.2.0  255.255.255.0
```

則會允許192.168.2.0至192.168.2.255之間的每一個地址，即整個C級的地址。不得有下列這種地址出現：

```
permit 192.168.2.0  0.0.0.0
```

這會允許每一地址使用，不論其地址爲何。 因此，允許每一個應該允許的地址，然後拒絕其余地址。如允許192.168.2.xxx范圍中的每一用户，可用下列方式表示：

```
permit 192.168.2.0  255.255.255.0
deny 0.0.0.0  0.0.0.0
```

注意deny行中的第一個"0.0.0.0"。由于地址以0.0.0.0修改，因此IP爲何都沒有影響。用0作爲IP地址，因爲便于打字。 特別的用户可以給予或拒絕使用的權限。這可通過iden的查驗來實現。由于不是所有系統都支持iden，其中包括Trumpet Winsock，所以此處不預備多加說明。隨同socks提供的說明以夠使用。

8.2.2 路徑檔

SOCKS中的路徑檔稱爲"socks.conf"，極易與權限檔混淆。 路徑檔讓SOCKS用户知道何時用socks，何時不用。例如，在示範的網路中192.168.2.3並不需要使用socks與192.168.2.1防火牆對話。通過Ethernet，它們之間有直接的連接。又127.0.0.1自動設爲loopback。因此也不需要用socks同自已對話。它有三行輸入：

- deny
- direct
- sockd

Deny行告訴socks何時拒絕一項請求。在此添入的內容同sockd.conf的內容相同，地址標示行、IP地址和修改地址行。一般而言，權限檔sockd.conf也與此有關，修改地址部分則用0.0.0.0。如果不打算連到任何地方，在此可作出修改。

在direct行下列入不使用sock的地址。所有這些地址都可直接聯上網路，無須經過代理伺服器。在這裡又有三個位置要填：identifier、address和modifier。例如：

```
direct 192.168.2.0 255.255.255.0
```

Sockd行告訴電腦那一個用户的電腦上有socks server daemon。該行內容如下：

```
sockd @=<serverlist> <IP address> <modifier>
```

注意@= 填入的內容。利用這種方法可以填入一系列代理伺服器的IP地址。在這裡只用一個代理伺服器的地址爲例。但可以列上多個伺服器的地址，以便加大容量，並當有伺服器失靈時，有其他的伺服器頂替。

設定IP地址和modifier域的方法和其他例子相同。

8.2.3 防火牆後的DNS 從防火牆後設定Domain Name Service是件簡單不過的事。只要在作爲防火牆的電腦上設定DNS即可。然後在防火牆後的電腦上設定使用這個DNS。

8.3 代理伺服器

8.3.1 Unix

要使應用程序利用代理伺服器，這些應用程序需要"sockified"。在這裡需要兩個telnet，一個進行直接通訊，一個通過代理伺服器進行通訊。SOCKS軟件中有說明sock一個程式的方法，也附有幾個已經sock好

的程式。如果要直接使用sock好的程式，SOCKS軟件會直接設定。因此，應該將保護網路內的所有程式改名，然後再改用已經sock好的程式。例如，"Finger"變爲"finger.orig"，"telnet"變爲"telnet.orig"。 必須通過include/socks.h檔告訴SOCKS這種設定。 有些程式能自行處理routing和sockifying的問題。Netscape就使其中之一。例如在Netscape下要用用代理伺服器，只要在Proxies下SOCK欄內填入伺服器的地址即可（在此爲192.168.2.1）。當然，每種應用程式都得作些小變動，不論其處理代理伺服器的方法爲何。

8.3.2 微軟視窗與Trumpet Winsock

Trumpet Winsock中有自帶的代理伺服器功能。在"setup"選單中填入伺服器的IP地址和所有直接可聯的電腦的地址。然後，Trumpet就會處理所有外送的數據包。

8.3.3 使代理伺服器配合UDP數據包

SOCKS軟件只處理TCP數據包，而不處理 UDP。這多少減少了它的用處，因爲，許多有用的程式，例如talk和Archie，都利用UDP。有一套軟件，稱爲UDPrelay，由Tom Fitzgerald設計<fitz@wang.com>，主要作爲UDP數據包的代理伺服器使用。不過在編寫本文時，這套軟件不能用于Linux.

8.4 代理伺服器的缺點

歸根結底，代理伺服器是一個安全裝置。在有限的IP地址的情況下，用它使許多用户進入網際網路有許多缺點。代理伺服器可使保護網路內的用户聯到網路之外，但使網路之外的用户完全無法同網路之內的用户聯系。這表示無法同網路之內的電腦進行talk或archie聯網，也無法發送電子郵件。這些缺點看來並不嚴重，但是如果：

- 你有一份沒有完成的報告留在保護網路防火牆内的電腦上。回家後，你又想看看這份報告。但是沒有辦法。因爲電腦在防火牆後，無法聯網。如果首先login 防火牆，但由于每一個人都可進入代理伺服器，因此你在這個伺服器上並沒有個別帳户。
- 你女兒去了大學。你想寫封電子郵件給她。你想談些私事，因此最好能把電子郵件直接放到自己的電腦上。你當然信得過你的系統管理員，但這倒底與公務無關，是個人的信件。
- 不能使用UDP是代理伺服器的一個大缺陷。我想不久之後就會有UDP的功能。

FTP是代理伺服器的另一個問題。在取得或使用`ls`時，FTP伺服器在客户機上打開一個socket，並通過它傳送信息。代理伺服器不允許進行這項工作，因此FTP無法使用。 此外，代理伺服器運行緩慢。由于需要額外資源較多，幾乎任何其他能達成這項作用的伺服器都要比它快。 一般而言，如果有IP地址聯網，而又不必特別顧慮安全問題，那就不要使用防火牆和（或）代理伺服器。如果沒有IP地址聯網，但也不顧慮安全問題，那就不妨使用IP模擬器，象Term，Slirp或TIA。Term可從`ftp://sunsite.unc.edu`取得，Slirp可從`ftp://blitzen.canberra.edu.au/pub/slirp`取得，TIA可從marketplace.com取得。使用代理伺服器的理想網路是有許多用户需要聯網，那只要做一次設定之後就不必再做太多其他的工作。

9 高級設置

在結束此文時，不妨再舉一個例子，來説明設置的方法。前面的例子適合多數使用情況。下面再以一個高級設置爲例，以便能説明一些問題。如果前面的例子不能解答你的問題，或者還想了解代理伺服器和防火牆的其他特性，請注意下面的例子。

9.1 注重安全的大型網路

假設一個民團首腦要設置網路，其中共有50台電腦和有一個32個IP地址的次級網。由于隨從的級別不同，民團首腦想在網路上設置不同級別的使用權。因此，網路的一部分不能與另一部分互通。 各種級別有：

1. 外圍。這是人人都可到達的層面。這是吸引新成員的層面。
2. 部隊人員這一層面的人物已經超過外圍。這個層面的人可以知道一些計謀和製造武器的方法。
3. 外籍軍團這是眞正完成計劃之處。

9.1.1 網路的設定

IP號碼的設定方法如下：

- 一個地址爲192.168.2.255，這是broadcast的地址，不可使用。
- 32 IP地址中23個地址分配給23台機器，這些機器可同網際網路聯結。
- 一個IP地址用于網路上的linux機。
- 一個IP地址用于網路上的另一個linux機。
- 兩個IP #'s用于router
- 剩下的四個地址隨便定四個名字，使人捉摸不定眞正的用户。
- 保護網路的地址爲192.168.2.xxx

這樣就建立了兩個不同的網路。這兩個網路通過紅外線Ethernet聯網，外界完全看不到它們的存在。紅外線Ethernet的作用和一般Ethernet的作用相同。 這兩個網路各自連到有IP地址運行linux的電腦。 同時有一個文檔伺服器接連到這兩個保護網路，因爲征服世界的計劃中需要一些訓練精良的部隊。文檔伺服器中有部隊網路的IP地址192.168.2.17和外籍軍團網路的IP地址192.168.2.23。有不同IP地址的原因是因爲有不同Ethernet卡的緣故。網路上IP Forwarding的功能關閉停用。 兩台Linux機上IP Forwarding的功能也都停用。除非有明確規定，否則router不會轉送送往192.168.2.xxx的數據包，因此網路無由進入。關閉IP Forwarding功能的原因是部隊網路發出的數據包不讓到達外籍軍團網路，外籍軍團網路的數據包也不讓到達部隊網路。 可以設定NFS伺服器的設置，使其把不同文檔送往不同網路。這種方法頗爲好用，在symblic links上做番手腳可使文檔讓大家共享。利用這種設置和加一張ethernet卡可使一台文檔伺服器用于所有三個網路。

9.1.2 代理伺服器的設置

由于三批人馬都需要了解網上的情況，因此他們都需要上網。外部網路直接連到網際網路，因此在代理伺服器上不需要作出任何更動。外籍軍團網路和部隊網路在防火牆之後，因此需要在代理伺服器上作出一些設置。 兩個網路的設置非常類似。它們仍舊使用分配給它們的IP地址。不過在這裡得設定一些參數。

1. 任何人都不得使用文檔伺服器上網，否則文檔伺服器可能會遭到病毒或其他壞東西得入侵。這種問題至爲嚴重，因此不得使用文檔伺服器。

2. 不讓部隊人員上網。他們正在接受訓練，如果讓他們擁有這種檢索資訊的能力可能對他們有害。

因此，在部隊網路的linux機上sockd.conf檔內應有下列一行：

```
deny 192.168.2.17  255.255.255.255
```

並且在外籍軍團機內的設定是：

```
deny 192.168.2.23  255.255.255.255
```

同時，部隊網路的linux機內設定：

```
deny 0.0.0.0  0.0.0.0 eq 80
```

這行的意義是不讓任何機器使用埠號80，既http埠。不過這些機器仍然可用所有其他功能，只是不讓上網。 然後在兩台機器的sockd.conf檔內都添加：

```
permit 192.168.2.0  255.255.255.0
```

使所有在192.168.2.xxx網上的電腦都使用這台代理伺服器，但不讓使用的電腦除外（既從部隊網路進入文檔伺服器和網際網路）。

部隊網路的sockd.conf檔的內容如下：

```
deny 192.168.2.17  255.255.255.255
deny 0.0.0.0  0.0.0.0 eq 80
permit 192.168.2.0  255.255.255.0
```

外籍軍團網路的sockd.conf檔的內容如下：

```
deny 192.168.2.23  255.255.255.255
permit 192.168.2.0  255.255.255.0
```

這樣的配置應該沒有問題。每一個網路都能單獨作業，並有適當的相互關系。人人都應該心滿意足才對。 現在就可征服世界了！