IBM eNetwork Firewall for Windows NT

使用指南

版本 3 版次 2.1.1

GC40-0213-01

IBM eNetwork Firewall for Windows NT

使用指南

版本 3 版次 2.1.1

GC40-0213-01

註

在使用本資訊及支援的產品之前，請務必閱讀第131頁的『附錄. 注意事項』下的一般資訊。

第二版 (1998 年 6 月)

本書適用於版本 3 版次 2.1.1 的 IBM eNetwork Firewall for Windows NT (產品編號 5765-C16)。本版應取代 GC40-0213-00。

目錄

關於本書

本書將說明如何架構及管理 Windows NT** 系統上的 IBM eNetwork Firewall，讓您避免不要的或未授權的通信進出您的安全網路。

本書適合那些要安裝、管理以及使用 IBM Firewall 的網路或系統安全管理者閱讀。雖然本書說明如何使用從屬站程式來存取防火牆，但本書不是從屬站程式的使用者指南。要使用從屬站程式 (如 telnet 或 FTP) 時，請參閱 TCP/IP 從屬站程式的使用者指南。

使用本書之前，請使用 CDROM 外盒隨附的「設定與安裝」來安裝本產品。

啓動架構從屬站之後，線上解說資訊會協助您填寫架構從屬站欄位，以及在對話框之間移動。

必備的知識

您在安裝及架構「IBM Firewall」之前，必須對 TCP/IP 位址設定、遮罩及網路管理有充份的了解。因爲您將要設定及架構一個在您的網路上控制進出存取的防火牆，所以您必須先瞭解網路運作的情形。尤其，您需要瞭解 IP 位址的基本資訊、完整名稱和子網路遮罩。

有關 TCP/IP (涵蓋 netstat、arp、ifconfig、 ping、nslookup、DNS、sendmail、routing 及其它資訊) 的優良書籍爲 *TCP/IP Network Administration*。有關詳細資訊，請參閱*參考書目*。

有關執行 UNIX 管理，並提供 TCP/IP 概觀 (包括遞送路徑、網路硬體、DNS 及 sendmail) 的優良書籍爲 *UNIX System Administration Handbook*。有關詳細資訊，請參閱「參考書目」。

本版次所提供的功能

IBM eNetwork Firewall for Windows NT 提供各式各樣的功能，並包括防火牆的全部三個結構：

1. 應用程式 proxy
   - FTP
   - HTTP，包括 Gopher 及 WAIS
   - Telnet
   - SafeMail

   HTTP、Telnet 及 FTP 都有鑑證的功能。
2. 透過「Socks 通訊協定第 5 版」的電路層閘道，一種 Internet 標準。
3. 過濾 -- 廣泛且健全的一組基準，可根據它來允許或拒絕資料傳輸。基準包括 TCP/IP 位址、連接埠、通訊協定、方向、配接卡 (安全/非安全) 及其它。

許多預先定義的服務程式會快速設定。

Socks 通訊協定第 5 版

「Socks 通訊協定第 5 版」除了簡單又具有彈性之外，它還提供下列優點：

- 部署鑑證及加密方法時非常簡單
- UDP 連結可建立虛擬 proxy 電路，以在 UDP 型的 proxy 電路上傳輸資料。
- Socks V5 Watcher，會顯示即時 socks 效能資訊

網路位址轉換

由於 Internet 的急速發展，突顯出 IP 位址殆盡的問題。「網路位址轉換」(NAT) 提供一個解決方案，以位址的重新使用爲基礎，來解決 IP 位址殆盡的問題。

NAT 的好處是，透通式容許使用專用或非法位址的網路與 Internet 上的主電腦通信；因而可以有效地讓專用網路擁有寬廣的位址空間。此外，若使用 NAT，則專用網路中的位址就會被隱藏起來，不會被外界看到，進而提供多一層的安全性。

簡易的管理

您可以透過使用 Java** 應用程式來從遠端機器進行管理，以便輕鬆地更新防火牆架構。此外，可以爲不同的管理者指派不同層次的權限，以進一步控制防火牆的存取。這個單一、且易於瞭解的使用者圖形介面 (GUI) 可用來管理 Windows NT Firewall 及 AIX Firewall。

NT 的強化

安裝防火牆時會停用非 TCP/IP 通訊協定、不需要的系統服務程式，以及非管理者帳戶的本端登入。

有力的鑑證

支援所有受歡迎的記號基本鑑證機制，像是安全 ID、SecureNet 密碼鎖及其它。

報告公用程式

報告公用程式可讓您在系統日誌匯出到資料庫引擎時執行 SQL 查詢。

警示、監督及記載

廣泛且詳細的記載，包括所有的防火牆活動，以及 TCP/IP 位址、使用者 ID、 TOD、檔案名稱、埠號等等。同時也包含「日誌監督程式」，可監視可疑的活動，並且在超過臨界值時，能夠向您發出警示。

隔離各個網路

使用防火牆中的多個「網路介面卡」(NIC)，您就可以隔離多個子網路。

國家語言支援

國家語言支援有英文、日文、韓文、法文、簡體中文、繁體中文、義大利文、西班牙文及巴西的葡萄牙文。

輸入 IP 位址

架構防火牆時，會要求您鍵入 IP 位址。 您必須以下面的格式輸入一個具有 4 個八位元組的完整帶點十進位數 IP 位址：

```
nnn.nnn.nnn.nnn
```

其中，每一個 `nnn` 代表三個數字的組合，其範圍從 000 到 255。

如何連絡 IBM 以尋求服務

關於問體診斷及解決方法，「IBM 支援中心」會提供電話協助。您可隨時連絡「IBM 支援中心」，服務人員在 8 小時的上班時間內會回答您的問題（客戶當地時間星期一到星期五早上 8:00 到下午 5:00）。連絡電話是 1-800-237-5511。

美國或波多黎各以外地區，請連絡當地 IBM 代表或授權的 IBM 供應商。

第1章 介紹 IBM Firewall

IBM eNetwork Firewall 是 AIX 及 Windows NT** 的網路安全性程式。 在本質上，防火牆是介於安全內部專用網路及其他（非安全性）網路或 Internet 之間的一道封鎖。防火牆的目的在於避免不必要的或未經授權的通信進出安全性網路。防火牆的工作有三：

- 厲行 Internet 安全性策略
- 讓您自己的網路使用者使用來自外部網路的授權資源，而不必犧牲您網路的資料和其他資源的安全性。
- 將未授權的使用者排除在您的網路之外。

防火牆概念

Internet 的任意連通性會產生許多安全問題。您必須保護自己的專用資料，也必須保護自己專用網路內的機器存取，以免被外界濫用。要達成這個保護的第一步驟就是限制專用網路連線至 Internet 的連接點數目。建議您在架構中讓專用網路只透過一個閘道連線至 Internet，這樣您就可以控制進出 Internet 的資料傳輸。我們稱這種閘道爲防火牆。

要瞭解防火牆如何運作時，請考慮這個範例。想像您要控管一棟建築物的人員進入。建築物的大廳是唯一入口。在大廳中，由接待人員負責接待進入此建築物的訪客，保全人員會監視這些訪客，且攝影機會錄下他們的動作，訪客的身份則經由識別證閱讀機鑑證。

對於私有建築物的門禁控制而言，這些都是非常好的措施。但如果有非授權者闖過大廳，則根本無從保護此建築物免受此人的破壞舉動。不過，只要如果監督此人的一舉一動，便能偵測任何可疑行爲。

定義防火牆策略時，您可能會認爲只要阻止所有可能會對組織造成危害的事物進入，其餘就可以不必管了。不過，因爲侵入方法日新月異，您必須預先設想如何防止入侵，就像前述建築物的例子一樣，您必須監督防禦措施是否出現遭受破壞的癥兆。一般而言，要從闖入損害中復原所付出的代價，遠超過事先的預防。

IBM Firewall 工具

IBM Firewall 就像是建置各種防火牆架構的工具箱一樣，一旦選定結構及安全策略之後，您就已經選擇了必要的 IBM Firewall 工具。 IBM Firewall 架構從屬站提供方便的圖形使用者介面以供管理之用。 IBM Firewall 提供所有重要事件的綜合記載，如管理變更以及破壞安全的嘗試。

因爲 IBM Firewall 實質上是一個 IP 閘道，所以它將整個環境分割成兩個以上的網路：一或數個非安全性網路以及一或數個安全網路。 例如，非安全性網路是 Internet。安全網路通常是公司的 IP 網路。IBM Firewall 所提供的工具包括：

- 專用過濾器
- Proxy 伺服器
- Socks 伺服器
- 特定的服務程式，像是領域名稱服務程式 (DNS) 和 SafeMail

專用過濾器

專用過濾器是根據多個基準 (像是時間、IP 位址及子網路) 來檢查階段作業層次上之封包的工具。 過濾規則與 IP 閘道功能一起運作，因此機器必須有兩個或以上的網路介面，分別位於各 IP 網路或子網路中。其中一組介面會宣告爲非安全性，而別組介面則會宣告爲安全。過濾器會在這兩組介面之間運作，如第2頁的圖 1 所示。

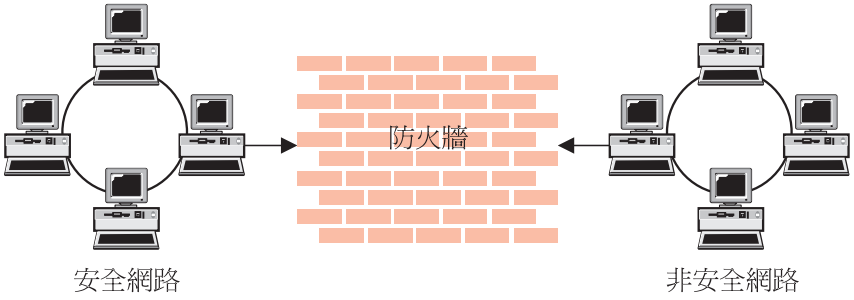

圖 1. 具有專用過濾處理的防火牆

專用過濾器的作用

專用過濾處理提供了防火牆的基本保護機制。過濾器可讓您根據 IP 階段作業明細來決定通過防火牆的資料傳輸，藉此保護安全網路不受外來威脅，例如掃瞄是否有安全伺服器或 IP 位址的欺騙行爲。將過濾機能當成建構其它工具的基礎。

Proxy 伺服器

不像過濾處理只會檢查封包的傳遞， proxy 伺服器不僅是防火牆部份的應用程式，而且會代表網路使用者執行特定的 TCP/IP 功能。該使用者會連絡使用其中一個 TCP/IP 應用程式 (Telnet 或 FTP) 的 proxy 伺服器。proxy 伺服器會代表使用者與遠端主電腦連絡，因此在對外部使用者隱藏網路結構時會控制存取權。 第3頁的圖 2 說明截斷來自外部使用者之要求的 proxy Telnet 伺服器。

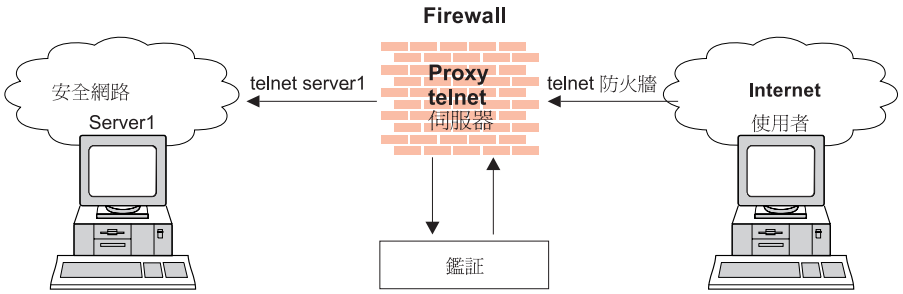

圖 2. 具有 Proxy 伺服器的防火牆

可用的 proxy 服務程式爲 telnet、FTP、HTTP、 WAIS、GOPHER、HTTPS 及 SafeMail。

IBM Firewall proxy 伺服器可以使用各種的鑑證方法來鑑證使用者。使用者可在 Internet 中存取有用資訊，而不致於危及內部網路的安全。

Proxy 伺服器的目標

透過 Proxy 伺服器連接之後，會在防火牆中斷 TCP/IP 連線，而減少危及安全網路的可能性。使用者可能也需要使用其中一種鑑證方法來鑑證自己。

Proxy 伺服器的一個主要優點就是會隱藏位址。所有離埠 proxy 連線都會使用防火牆位址。Proxy 伺服器的另一個優點就是安全。 IBM 專家已研發這些 proxy 伺服器，來防衛從屬站機器上的安全弱點。

Proxy 伺服器的另一個優點在於從屬站機器上不需特殊版本的從屬站程式。因此，一旦安裝好 Firewall 之後， Firewall 所記錄的每一個使用者都能存取非安全性網路，而不必安裝任何其它的軟體。

Socks 伺服器

Socks 是電路閘道的標準，它不需要有傳統 proxy 伺服器的額外執行時間，就可隱藏位址。

Socks 伺服器與 Proxy 伺服器相似，其階段作業都會在防火牆中斷。它們之間的不同在於，socks 可支援所有的應用程式，而不像每一個應用程式都需要唯一的 proxy。顯然地，Socks 從屬站會用 IBM Firewall 主電腦上的 Windows NT Socks 服務程式來啓動階段作業，然後會驗證是否允許來源位址及使用者 ID 建立連接到非安全性網路的連線，之後再建立第二個階段作業。 第4頁的圖 3 以圖示說明具有 Socks 伺服器的防火牆。

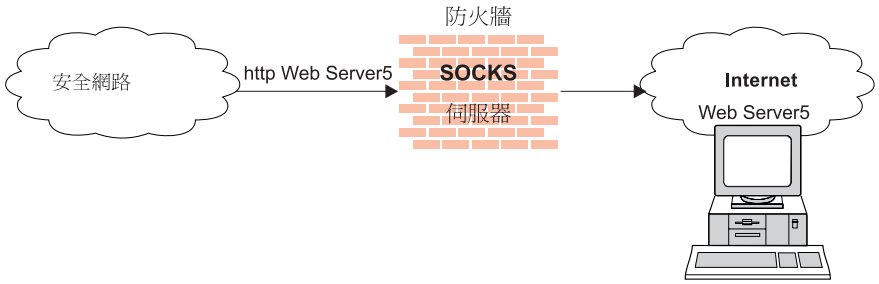

圖 3. 具有 Socks 伺服器的防火牆

很多應用程式都有 Socks 化的從屬站 (知道 Socks 的從屬站)，例如 Netscape Navigator** 或 Microsoft** Internet Explorer；或是透過 TCP/IP 軟體的應用程式，如 Aventail** AutoSocks**。

Socks 伺服器的作用

就離埠的階段作業而言 (從安全從屬站離開至非安全伺服器)， Socks 伺服器與 Proxy 伺服器的作用相同，即中斷防火牆上的階段作業，並且提供安全門，使用者必須證明其身份才能通過此安全門。 這對使用者而言非常簡單，額外的管理工作不多。

領域名稱服務程式

存取安全網路的領域名稱記錄對侵入者有很大的幫助，因爲它會提供一份可侵入的主電腦清單。而被破壞的領域名稱服務程式伺服器也會提供存取路徑。從外部網路中，防火牆上的名稱伺服器只知道它自己，而且絕不會洩露內部 IP 網路的資訊。從內部網路中，此名稱伺服器知道 Internet 網路，使用機器名稱存取 Internet 上任何機器時，名稱伺服器是非常好用的。

DNS 伺服器的作用

執行防火牆上的 DNS 伺服器具有以下兩項優點：防止名稱解析要求通過防火牆，以及在非安全性環境中隱藏安全網路主電腦。

SafeMail

郵件是組織想要存取 Internet 的主因之一。 SafeMail 是一種設計來隱藏您內部網路的領域名稱之 IBM 郵件閘道。 SafeMail 功能不會將郵件儲存在閘道上，也不會在 root 使用者 ID 下執行。防火牆閘道公用領域名稱會取代送出郵件上的專用領域名稱，因此，郵件會顯示爲從防火牆的位址送入，而非使用者的位址。 SafeMail 支援「簡易郵件傳送通訊協定」(SMTP) 及「多功能 Internet 郵件副檔名」(MIME)。

使用網路安全審核程式

「網路安全審核程式」會掃瞄網路是否有安全漏洞或架構錯誤。「網路安全審核程式」會掃瞄伺服器和防火牆是否有問題或弱點，如開放式連接埠和其它曝露問題，然後編譯一個列示讓您能夠更正問題。「網路安全審核程式」可用作重要主電腦的定期掃瞄器，或作爲單次資訊收集工具。「網路安全審核程式」的管理會透過易於使用的命令行介面完成。有了「網路安全審核程式」，可以使防火牆維持警戒。

「網路安全審核程式」的特性包含：

- 掃描 TCP 和 UDP 連接埠
- 辨識在非標準連接埠中的伺服器
- 報告危險服務程式、已知的弱點、已作廢的伺服器版本，以及違反自行設定站台策略的伺服器或服務程式。
- 以 HTML 格式產生報告以方便瀏覽

第2章 規劃

開始架構 IBM Firewall 之前，請使用核對列示及規劃工作清單，來協助您瞭解網路架構。

規劃核對列示

1. 定義目的。 請問您要：
   - 存取 Internet (telnet、匿名 FTP 等等)?
   - 分割內部網路？
   - 提供外*部*存取權給網路嗎？
2. 評估 IP 子網路層次上的網路拓樸。
   - 一個安全介面和一個非安全介面已正確地架構嗎？
   - 您的位址能夠支援規則中的子網路遮罩？
3. 決定要如何使用 DNS。 請參閱第31頁的『第6章 處理領域名稱服務程式』。
4. 決定要如何使用 safemail。請參閱第41頁的『第7章 SafeMail』。
5. 如果要使用 socks，請確定已安裝使用 socks 化的從屬站，像是 Netscape Navigator 或 Microsoft 瀏覽器。關於使用 Socks 的資訊，請參閱第73頁的『第11章 架構 Socks 伺服器』。
6. 需要何種類型的鑑證呢？
   - 如果要使用 Security Dynamics** ACE/Server** 來鑑證使用者，請在防火牆主電腦中安裝 ACE/Server 從屬站字碼。 建議您在安全網路內的其他一些主電腦上，安裝 ACE/Server 伺服器字碼。

     關於安裝和使用 Security Dynamics ACE/Server 以及 SecurID** 卡的資訊，請參閱 Security Dynamics Technologies Inc. 所提供的資訊。
   - 如果要使用 AssureNet Pathways** SecureNetKey** 卡，請在 IBM Firewall 之外單獨購買該卡。
   - 如果使用自己的鑑證方法，請參閱 *IBM eNetwork Firewall 參考手冊* 中的「提供自己的鑑證方法」章節。
   - 爲了鑑證目的，您必須架構搜尋可靠 Windows NT 領域的 Windows 從屬站程式碼，來使用 TCP (而非 NETBIOS)。將會停用 NETBIOS。可靠的 Windows NT 伺服器必須具備 TCP/IP 主電腦名稱及位址，而且在它們與防火牆之間必須具備 TCP/IP 連通性。防火牆管理者需要在防火牆與可靠的 NT 伺服器之間建立連線，以允許它們兩個之間的資料傳輸。

     請使用下列預先定義的服務程式來設定這個連線：

     a. 領域控制器的鑑證 - 可使用使用者鑑證的領域控制器

     b. NetBT 名稱服務程式廣播 - 准許 NetBIOS over TCP/IP 名稱服務程式廣播

此外，請使用 Windows NT 架構公用程式，來定義信任關係。

7. 若您使用過濾，請從簡單的過濾規則開始，並使它們具有高度的限制性。熟悉您所需的服務程式所使用的連接埠及通訊協定。
8. 決定一種用來儲存日誌檔的方法。儲存是 Windows NT Scheduler 服務程式中已排程工作的理想方法。 請參閱第113頁的『第15章 管理日誌與保存檔』。

網路架構規劃工作清單

填寫下列資訊，作爲規劃 IBM Firewall 架構的一部份。

防火牆的主電腦名稱 _____

安全網路介面 (連線到內部安全網路)

IP 位址 _____ 子網路遮罩 _____

IP 位址 _____ 子網路遮罩 _____

IP 位址 _____ 子網路遮罩 _____

IP 位址 _____ 子網路遮罩 _____

非安全網路介面（連線到不可靠的非安全網路）

IP 位址 _____ 子網路遮罩 _____

IP 位址 _____ 子網路遮罩 _____

IP 位址 _____ 子網路遮罩 _____

IP 位址 _____ 子網路遮罩 _____

路由器名稱 _____

路由器位址 _____

安全領域名稱 _____

安全領域名稱伺服器 (DNS) 的 IP 位址 _____

非安全領域名稱伺服器 (DNS) 的 IP 位址 _____

安全郵件伺服器 _____

公用領域名稱 _____

架構從屬站的 IP 位址 _____

遠端從屬站的 IP 位址 _____

Windows NT 防火牆的根目錄 _____
(在整份說明文件中，皆稱其爲 ROOTDIR)

c:\winnt (我們假定 Windows NT 安裝在這個目錄中)

第3章 設定架構伺服器及架構從屬站

本章將告訴您如何爲 IBM Firewall 設定架構伺服器及架構從屬站（其爲使用者圖形介面 - GUI）。

設定架構伺服器

架構伺服器是架構從屬站與 Firewall 之間的介面。 架構伺服器會處理來自架構從屬站的要求。它在 Firewall 機器上執行，並且能夠處理本端或遠端機器上的架構從屬站的要求。只要您將它設定好，便可把它當作 Firewall 機器的一部份，

NT 服務程式檔 (位於您已安裝 Windows 作業系統的目錄：c:\winnt\system32\drivers\etc\services) 中已指定架構伺服器的埠號。埠號預設值爲 1014，但是若您要將它變更，以增加其安全性的話，您可以停止「架構伺服器服務程式」，然後修改服務程式檔案，再重新啓動架構伺服器服務程式，即可變更。

架構伺服器一開始的設定只接受本端機器上的架構從屬站的要求。一開始的要求並未加密。若要變更這個選項，請從命令行使用 `fwcfgsrv cmd=change`。

localonly=

指定是否只能從本端機器管理 Firewall。

localonly=yes

架構只能在本端機器上進行；此爲預設值。

localonly=no

架構可在任何機器上進行。

encryption

指示架構伺服器是否要透過 secure socket layer (ssl) 將傳入的資料加密。

不管您是變更加密選項或 sslfile，都必須停止架構伺服器服務程式，然後再重新啓動。

encryption=none

不進行任何加密作業；此爲預設值。

encryption=ssl

進行 SSL 加密作業。

sslfile=

指定要用 SSL 加密的 SSL 密碼鎖檔案名稱；預設值爲 `ROOTDIR\config\fwkey.kyr`。 *ROOTDIR* 爲您在進行安裝作業時，所選定的 IBM Firewall 目標位置目錄。如何建立密碼鎖檔案的相關資訊，請參閱 *IBM eNetwork Firewall 參考手冊*。

如果架構從屬站無法與「防火牆」機器連線，而且是在其他機器上的話，請用 fwcfgsrv cmd=list 來檢查是否已設定 localonly=no。另外，從屬站所使用的語言也必須和伺服器相符。 最後，請開啓服務程式畫面，來確認架構伺服器是否處於執行中的狀態。 要這樣做時，請跳至主控台，然後按兩下「服務程式」圖記，來檢查每一個服務程式的狀態。 如果不在執行中，則應該重新啓動該服務程式。

設定架構從屬站 (GUI)

當您安裝 IBM Firewall 時，會自動安裝架構從屬站。 架構從屬站亦可個別安裝在沒有 Firewall 的任何 Windows NT 機器上，如此可讓您執行遠端管理。 欲啓動架構從屬站應用程式，請在 IBM Firewall 程式群組中的架構從屬站圖記上按兩下。當架構從屬站啓動時，您必須先使用 Windows NT 管理者帳戶，來登入 Firewall。

只有擁有適當管理鑑證的「Windows NT 管理者」及「防火牆管理者」，才可以用「架構從屬站」來登入 Firewall。

完成 Firewall 安裝之後，所有的 Windows NT 管理者都會被指定爲主要的防火牆管理者。您可以使用「架構從屬站」來登入使用主要的防火牆管理者的「架構伺服器」，若有必要的話，還可以定義其他防火牆管理者的使用者名稱。關於如何使用架構從屬站，來定義防火牆管理者的資訊，請參閱第79頁的『第12章 管理防火牆的使用者』。

若要爲較快或較慢的機器設定登入逾時值，按一下「IBM Firewall 架構從屬站」圖記，然後按一下**內容**，以變更下列項目。使用**捷徑**標籤來修改「內容」。將參數 timeout 變更爲 *20*，其中 20 代表等待連線出現的秒數。速度較快的機器可設爲 10，而速度較慢的機器則應使用預設值。

若要提升 JAVA 控制台中除錯資訊的層次，請執行 ROOTDIR\cfgcli\gui 中的 ibmfw.bat，而不是使用架構從屬站圖記。然而，請注意！啓用主控台記載功能可能會降低效能。

登入架構從屬站

欲登入架構從屬站 (在本端機器或遠端機器上)，請：

- 使用者必須是防火牆管理者
- 防火牆管理者必須具有已定義的鑑證計劃。請參閱第84頁的『使用者鑑證方法』。
- 使用者必須有權執行特定架構功能

透過架構從屬站啓動遠端架構

若要透過架構從屬站啓動遠端架構，請確定要登入的管理者具有下列在 Firewall 機器上定義的屬性：

- 如果管理者處於網路的安全端，且使用 Firewall 機器上的安全介面，則使用者必須已用安全管理的適當鑑證方法加以定義。 （不可設成全部拒絕)。此限制亦適用於從區域登入 Firewall。
- 同樣地，若管理者處於非安全端，且使用 Firewall 機器上的非安全介面，則使用者必須已用非安全管理的適當鑑證方法加以定義。 （不可設成全部拒絕)。

所有的使用者屬性都可透過架構從屬站中的「修改使用者」對話框或使用 `fwuser` 命令來設定。安裝好「防火牆」之後，所有的防火牆管理者都將擁有已正確設定的上述所有欄位。相關資訊，請參閱第79頁的『第12章 管理防火牆的使用者』。

遠端架構伺服器的記載輸出範例

以下是遠端架構伺服器的記載輸出範例：

```
Feb 03 13:52:15 1998 mr16n18: ICA9005i: 正在啓動遠端架構伺服器。

Feb 03 13:52:21 1998 mr16n18: ICA2024i: 使用者管理者已順利地從安全性網路：
127.0.0，使用 NT 鑑證方法來鑑證。
Feb 03 13:52:21 1998 mr16n18: ICA2169i: 使用者管理者已順利地從安全性網路：
127.0.0.1，使用 NT 來為「遠端管理伺服器」鑑證。
```

第4章 使用架構從屬站

使用者圖形介面的架構從屬站是用來架構及管理 IBM Firewall。

若您是第一次安裝 IBM Firewall，它一開始的設定是只接受本端機器上的架構從屬站的要求。不過，您可以在其它機器上安裝架構從屬站，並從遠端管理 Firewall。如何做的相關資訊，請參閱第11頁的『設定架構伺服器』。

若要將架構從屬站設定爲以您特定的語言環境來啓動，按一下「IBM Firewall 架構從屬站」圖記，然後按一下**內容**，以變更下列項目。使用**捷徑**標籤來修改「內容」。在預設的狀況下，會使用主電腦機器的語言環境。 IBM Firewall 支援下列語言環境：

- en_US - 美語
- ja_JP - 日語 PC
- ko_KR - 韓語
- zh_CN - 簡體中文 EUC
- zh_TW - 繁體中文 (Big 5)
- fr_FR - 法語
- it_IT - 義大利文
- pt_BR - 巴西葡萄牙語
- es_ES - 西班牙語 PC

使用架構從屬站需要用到滑鼠。

解說按鈕在靠近架構從屬站主畫面頂端處。按一下**解說**，即可取得任一功能的相關資訊。

如何登入架構從屬站

1. 在「登入類型」中，如果您是在防火牆的機器上，請選取「本端」。「本端」爲預設值。果您要進行遠端存取另一個 Firewall，請選取「遠端」， 若選取「遠端」，需要輸入主電腦名稱。
2. 若您選擇「遠端」登入，則需輸入您所要登入之防火牆機器的 IP 位址或主電腦名稱。
3. 根據「防火牆」所使用的加密，選取 SSL 或無。在「從屬站」這個選項下，「本端」的預設值爲「無」，「遠端」的預設值爲 SSL。
4. 輸入防火牆管理者或 Windows NT 管理者的使用者名稱。
5. 輸入伺服器進行傾聽的埠號，預設值是 1014。
6. 在「模態」選項下，如果您想架構您登入的 Windows NT 防火牆機器，請選取「主電腦」。管理者可以透過主電腦管理以區域或遠端方式一次更新一個 Firewall。爲 AIX 防火牆的「企業防火牆管理」(EFM) 管理選取「企業」。

7. 登入之後，您會看到鑑證訊息，如果這是您使用者名稱的鑑證方法設定，可能會出現提示，要求您輸入通行碼。如果有提示要求您輸入通行碼，請在「使用者回應」欄位中輸入您的通行碼，然後按下 Enter 鍵或按一下「提交」。如果您輸入的通行碼錯誤，就會收到一則訊息，請按一下「關閉」後重新啓動登入處理。如果沒有提示您輸入通行碼，則您的使用者鑑證方法可能是「全部允許」。在此情形下，您將立即看到 IBM Firewall 架構從屬站畫面。
8. 在順利完成鑑證之後，就會看到主要架構畫面。

圖 4. 架構從屬站登入畫面

導覽樹狀結構

架構從屬站左側有一個可收合的樹狀導覽輔助工具，如第17頁的圖 5 中所示。

如果節點或功能下面有項目，則檔案資料夾圖記會出現在節點左側。若要查看次功能，您可以連按兩下該圖記來展開檢視畫面。再連按兩下該圖記，即可收合此節點的檢視畫面，回到原先的檢視畫面中。

您按一下的功能都視爲已選取的功能，而且會強調方式顯示。您可以展開及收合節點，而右側的視窗檢視畫面不會有任何變更。當展開的樹狀結構超出可用的垂直空間時，捲軸即出現在導覽樹狀結構右方；如果有任何功能名稱未能完整顯示於導覽樹狀結構中，則出現水平捲軸。

圖 5. 架構從屬站導覽樹狀結構

主畫面上的一般功能

您會在**警示顯示畫面**上方看到下列三個按鈕，如第17頁的圖 5 所示：

解說　**解說**按鈕在靠近架構從屬站主畫面頂端處。按一下**解說**，可查看啓動及執行 IBM Firewall的步驟說明。

使用指南

使用指南按鈕在靠近架構從屬站主畫面頂端。按一下**使用指南**，可查看此線上出版品。

參考手冊

參考手冊按鈕在靠近架構從屬站主畫面頂端。按一下**參考手冊**，即可查看此線上出版品。

您會在主畫面上看到其它的按鈕爲：

最新　**最新**按鈕位於架構從屬站主畫面底端。按一下**最新**，可查看最近的警示。

登出/登入

登出/登入 按鈕位於架構從屬站右上角。它是一個重新連接按鈕。您可重新啓動登入順序，以連接不同的「防火牆」或登入爲不同的管理者。

若要登出，請按一下「登出」，按一下登入畫面上的「取消」，然後關閉應用程式。

日誌檢視器

日誌檢視器按鈕位於架構從屬站右下角，它可讓您瀏覽防火牆日誌。

前一個　**前一個**按鈕位於架構從屬站主畫面底端。按一下**前一個**，可查看先前的警示。

警示顯示畫面

您可以檢視由「系統日誌監督程式」(在主要架構從屬站視窗右下方) 所產生的警示記錄，如第19頁的圖 6 所示。

所顯示的「警示記錄」是 ROOTDIR\config\syslog.conf 檔案中所定義的第一個警示日誌機能所識別的檔案。 如果沒有定義警示日誌機能，您將會看到空白的顯示畫面。有關定義警示日誌機能的解說，請參閱第114頁的『新增日誌機能』。

此畫面顯示警示檔的名稱及目前所顯示的該檔案行號。您可以按一下**最新的**來查看最近的警示；按一下**先前的**，可讓您查看先前的警示。

出現的每一行會顯示警示的日期與時間、發生警示的防火牆之主電腦名稱、警示訊息標籤及警示訊息文字。標籤可指出警示的類型。

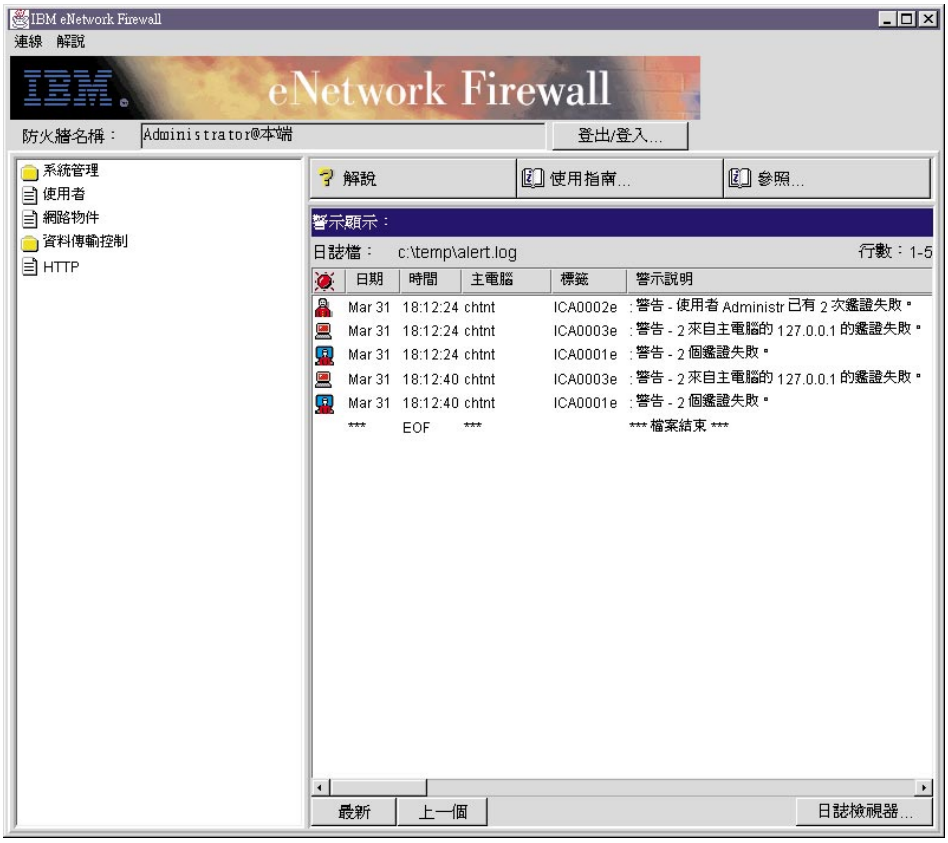

圖 6. 警示顯示畫面

日誌檢視器

按一下**日誌檢視器**，即出現日誌檢視器視窗，如第20頁的圖 7 所示。 日誌檢視器可讓您檢視防火牆日誌記錄。您可以指定日誌檔及記錄的數目 (預設值是 25)。

預設日誌爲 ROOTDIR\config\syslog.conf 中所定義之第一個防火牆日誌機能所識別的檔案。您可以從檔名欄位的下拉功能表中，選取一個不同的目標日誌檔，或鍵入要檢視的檔案名稱。

欲要求特定的開始行數，在「開始行號」旁邊的欄位中輸入行號之後，再按一下**開始行號：**。欲要求最後的字行，則按一下**底端**。**下一個**可讓您前進到檔案中的下一組字行。**上一個**可讓您退回到檔案中的前一組字行。**頂端**會帶您到檔案的頂端。若您按 **Yes**，您就可以選擇將防火牆日誌展開爲可讀取的文字。

關於日誌檔、機能、監督程式及警示的詳細資訊，請參閱第113頁的『使用架構從屬站來建立與保存日誌檔』 及第101頁的『第14章 監督防火牆記載』。

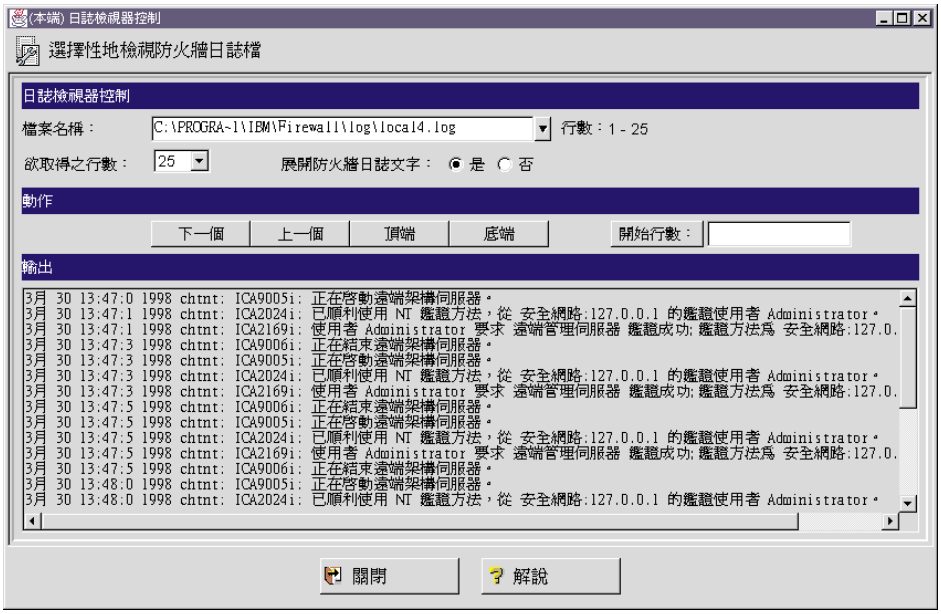

圖 7. 日誌檢視器

其它功能

搜尋欄位在靠近某些畫面左上角的頂端。您可以輸入一搜尋字串，然後按一下**尋找**。

您會在許多架構從屬站功能表上看到其它的按鈕爲：

引用 按一下**引用**，用您目前的選項填入先前一畫面的欄位中，或儲存您在畫面上所作的變更。**引用**按鈕不會讓視窗消失。

底端 按一下**底端**，跳至畫面底端。

取消 按一下**取消**，即關閉視窗但不儲存任何變更。

關閉 按一下**關閉**，從顯示畫面上除去視窗。

複製 **複製**按鈕可在新增項目至列示時節省時間。選取列示中項目後，按一下**複製**來建立類型選定項目的項目。按一下**複製**來建立一個類似選定項目的項目，並開啓複製列示中選定項目上欄位值的新項目，然後您就可以按照您的需要修改新項目欄位值。

刪除 按一下**刪除**，從列示中刪除選定的項目。

往下移 選取列示中的項目，然後按一下**向下移**，在列示中降低該項目的相對位置，每按一下，項目就往下移一個位置。

往上移 選取列示中的項目，然後按一下**往上移**，在列示中升高該項目的相對位置。每按一下，項目就往上移一個位置。

OK 按一下 **OK**，以儲存所作變更並關閉視窗。

開啓 在選取列示中項目之後，按一下**開啓**來檢視或修改該項目。若要新增項目，請按一下列示中的**新增**項目，然後按一下**開啓**。

復新 按一下**復新**，重新存取防火牆上的資料，並將資料重新顯示在畫面上。

移除 按一下**移除**，除去列示中選定的項目。此動作僅能移除列示中的項目。此動作在定義項目的其它位置中無效。

選取 按一下**選取**，來存取對這個功能有效的候補項目列示。

頂端 按一下**頂端**，即跳至畫面頂端。

一般欄位

您在許多架構從屬站對話框中會看到的一般欄位如下：

輸出 當您起動的命令執行時，進度資訊會顯示在此處。

名稱 爲項目提供名稱。對於防火牆中此特定功能而言，這個項目名稱必須是唯一的。此名稱「不可」包含直線符號 (|)、單引號字元 (') 或雙引號字元 (")，因爲這些字元是用來作 SMIT 及檔案的定界符號。使用這些字元會產生不可靠的資料。

解說 本欄位是選用性欄位，當您要提供有關此項目的其他資訊或備註時，系統即提供此欄位。

獨特功能

有一些架構從屬站的獨特功能您應該知道。

對 Windows 95 或 Windows NT 架構從屬站而言，架構從屬站須至少使用 1024 圖點 x 768 圖點的解析度，才能獲致最佳的效果。

如果您按住滑鼠左鍵繼續進行旋轉控制，但意外拉動滑鼠方位而沒有放開滑鼠按鈕，則旋轉控制會繼續執行。若要停止自旋控制，請以滑鼠左鍵按一下自旋控制方向箭頭之一。

如果您用 SSL 連續登入 Firewall 二次或以上，連線會遭拒絕。請結束或重新啓動架構從屬站。

第5章 IBM Firewall 入門

本章將告訴您在開始 IBM Firewall 設定時所需的基本架構步驟。 本章說明如何定義安全介面、如何決定安全性策略及如何定義網路物件的方法。

基本架構步驟

IBM Firewall 的基本設定，步驟如下：

1. 規劃您的 IBM Firewall 設定。儘早決定要使用的防火牆功能，以及使用它們的方法。以下章節對您很有幫助：
   - 第1頁的『第1章 介紹 IBM Firewall』
   - 第7頁的『第2章 規劃』
   - 第55頁的『規劃考量』
2. 指示 Firewall，哪些介面要連線至安全網路。您必須擁有安全介面及非安全介面，才能讓防火牆正常運作。請從「架構從屬站導覽樹狀結構」中，開啓「系統管理」資料夾，並按一下**介面**，就可以看到您防火牆上的網路介面列示。若要變更介面的安全狀態，請選取該介面，然後按一下**變更**。詳細相關資訊，請參閱第24頁的『指定網路介面』。

   如果您打算要連接 Internet，請聯絡您的 ISP，以取得 Firewall 非安全介面的 IP 登記位址。
3. 存取「系統管理」資料夾中的**安全性策略**對話，以設定一般安全性策略。對於標準的防火牆架構，請設定：
   - 允許 DNS 查詢
   - 拒絕對非安全介面廣播訊息
   - 拒絕 Socks 到非安全配接卡

   詳細相關資訊，請參閱第25頁的『使用架構從屬站來定義安全性策略』。
4. 設定領域名稱服務程式與郵件服務程式請從「架構從屬站」導覽樹狀結構中的「系統管理」資料夾存取這些功能。請參閱第31頁的『第6章 處理領域名稱服務程式』。
5. 您可使用在架構從屬站導覽樹狀結構中的**網路物件**功能，來定義防火牆的網路重要元素。「網路物件」會控制通過 Firewall 的資料傳輸。將下列重要元素定義爲網路物件：
   - Firewall 的安全介面
   - Firewall 的非安全介面
   - 安全網路
   - 安全網路上的每一個子網路
   - SDI 伺服器及 NT 領域伺服器的主電腦網路物件 (如果適用的話)

詳細的相關資訊，請參閱第27頁的『網路物件』。

6. 啓動 Firewall 上的服務程式。 這些都是安全網路中的使用者，可用來存取非安全網路（如 Socks 或 Proxy）的方法。您在規劃階段所作的決定，是執行服務程式的依據。執行服務程式通常需要設定某些連線架構，來容許某些類型的資料傳輸。例如，若您想讓您的安全使用者利用 HTTP Proxy 來瀏覽 Internet 上的 Web，您不僅需要在 Firewall 上架構 HTTP Proxy 常駐程式，而且必須設定連線，才能容許 HTTP 資料傳輸。 如何設定支援某些服務程式連線的相關資訊，請參閱第55頁的『第9章 服務程式範例』。
7. 設定防火牆使用者。若您要對離埠的 Web 存取等功能或是對防火牆管理者執行鑑證，您必須在 Firewall 上定義這些使用者。詳細相關資訊，請參閱第79頁的『第12章 管理防火牆的使用者』。
8. 若您想用 Windows NT 領域通行碼來鑑證，爲了要鑑證資料，您必須架構 Windows 從屬站程式碼，執行搜尋可靠 Windows NT 領域的功能，以使用 TCP 而非 NETBIOS。將會停用 NETBIOS。可靠的 Windows NT 伺服器必須擁有 TCP/IP 主電腦名稱及位址，而且在它們及 Firewall 之間，必須要有 TCP/IP 連通性。防火牆管理者必須在 Firewall 及可靠的 Windows NT 伺服器之間建立連線，才能在兩者之間傳輸資料。
9. 若您要使用網路位址轉換，請先聯絡您的 ISP，以取得 Internet 登記位址，才能使用 Many-to-one 位址轉換。然後，跳至*新增 NAT 架構*畫面，將登記的 Internet 位址新增至 *Many-to-one IP 位址*欄位。詳細相關資訊，請參閱第121頁的『第16章 轉換網路位址』。

遵循這些步驟可協助您啓動與執行基本的防火牆架構。 IBM Firewall 也提供其它功能，如系統日誌，來協助您確保網路的安全性。詳細的相關資訊，請參閱第113頁的『第15章 管理日誌與保存檔』。

指定網路介面

本書中，我們會區別安全與非安全介面、網路以及主電腦。安全介面會將 IBM Firewall 主電腦連線到您內部網路（您要保護的網路）中的主電腦網路。 **您的防火牆至少必須具備一個安全介面，才能運作**。 非安全介面會將 IBM Firewall 連線到一或數個外部網路或 Internet。IBM Firewall 至少必須具備一個非安全介面。

透過安全介面來連接的所有網路，都視爲安全網路。要區別連接至安全介面的各種子網路時，請使用專門過濾規則，來根據 IP 位址或位址遮罩，以拒絕或允許在同一個介面上存取數個子網路。

要指出安全與非安全介面時，請使用架構從屬站導覽樹狀結構上的「系統管理」資料夾。 所有已知介面（配接卡）都會顯示出來，並識別爲安全或非安全。

您必須先提供每個介面的名稱，才能執行特定的介面過濾處理。

若要將網路介面識別成安全或非安全，請：

1. 選取介面，然後按一下**變更**。
2. 必要時可重複上述步驟。
3. 按一下**關閉**。

若要鑑定該介面爲安全或非安全介面，並且要提供一有意義的名稱給該介面時，請按**開啓**。過濾器會使用此名稱，來過濾特定的介面。

使用架構從屬站來定義安全性策略

架構 IBM Firewall 時，必須先考量的其中一點，就是安裝作業的一般安全性策略。

「IBM Firewall」提供對話框，可協助您設定安全性策略，如第26頁的圖 8 所示。

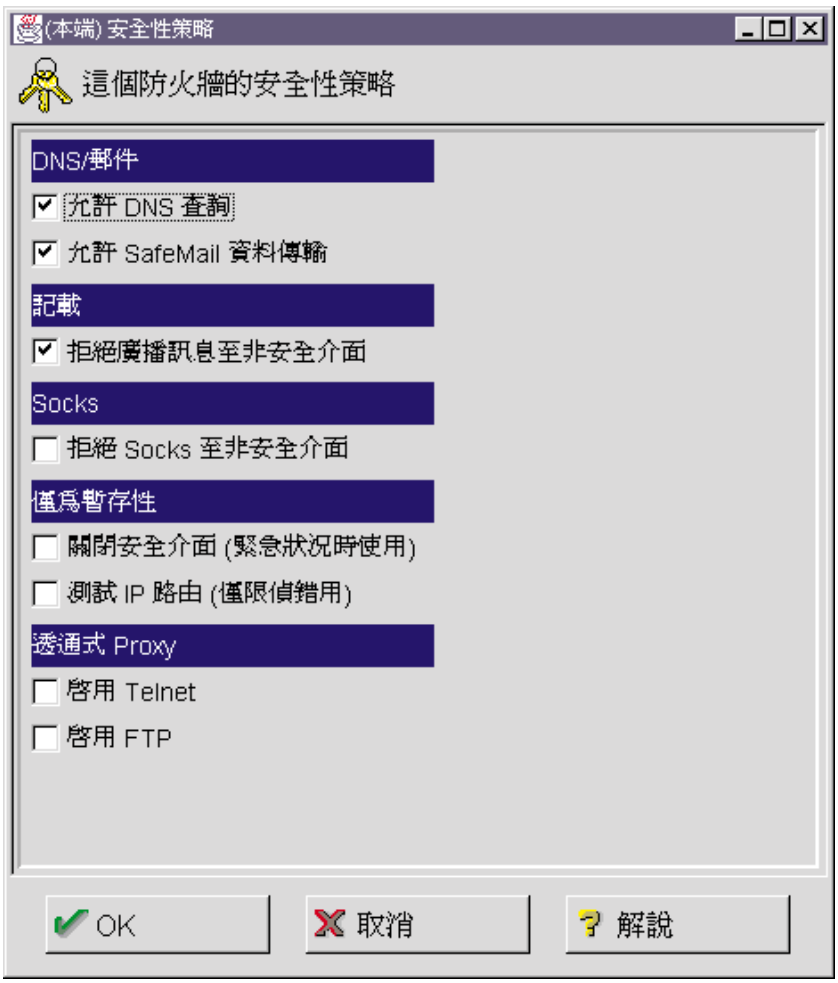

圖 8. 安全性策略

按一下「解說」，即可得知更多有關安全性策略畫面的資訊。

「安全性策略」提供一種迅速簡單的方法，可供管理者設定防火牆的綜合策略。 「安全性策略」視窗中所顯示的大部份勾選框，都提供捷徑來選取某些「預先定義的服務程式」，這些服務程式將引用於「防火牆」所接收的網路傳輸資料上。但「透通式 Proxy」選項例外，它們只是單純用來啓動或停止「透通式 Telnet」和「透通式 FTP」。

當您選取安全性策略時，Firewall 會建立啓動時所需的過濾規則。 Firewall 會啓用選定的服務程式，並且會使這些服務程式在系統的任何地方皆可使用。

請注意：每當選取專屬於「預先定義的服務程式」的勾選框，並按一下 **OK** 之後，就必須透過「連線啓動」視窗來啓動變更。 您不必啓動「透通 Proxy」選項，因爲這些選項不屬於「預先定義的服務程式」。欲取得預先定義的服務程式列示，請參閱第66頁的『預先定義的服務程式』。

此時即顯示以下的勾選框列示，您可從該列示中選取屬性，反映出您站台的安全性策略。選取的屬性可引用於 IBM Firewall 兩端的所有位址。

- 選取**允許 DNS 查詢**，來允許「領域名稱服務程式」分辨要求及回應。
- 選取 **SafeMail**，以讓郵件資料傳輸通過 Firewall。
- 選取**拒絕廣播訊息到非安全介面**，以防止「非安全連接埠」接收廣播訊息。如果防火牆的非安全介面連線至 Internet，則本服務程式可協助減少 Firewall 上的記載量。
- 選取**拒絕 socks** 到非安全配接卡，來禁止 Socks 資料傳輸從非安全網路進入 Firewall。
- 選取**關閉安全介面 (緊急情況時)**，來禁止所有資料傳輸透過安全介面進出 Firewall。只有緊急時才使用這一項。
- 選取**測試 IP 遞送路徑 (只適用於除錯**），讓全部資料傳輸透過任何介面進出 Firewall。請注意：若您變更此勾選框的值，則您必須按 **OK** 來儲存該值，並且在「連線啓動」視窗中「啓動」它。**使用本「服務程式」可能導致 Firewall 的安全性曝光。 所以請務必小心謹慎**。
- 選取**啓動 Telnet** 來允許「透通 Proxy Telnet」。
- 選取**啓動 FTP** 來允許「透通 Proxy FTP」。

網路物件

「網路物件」代表存在於網路的元件，如主電腦、網路、路由器、虛擬專用網路或使用者。 當您建立連線時，「網路物件」會指定服務程式的來源與目的位址。

物件可根據名稱、圖記表示、類型以及說明來加以識別。網路上有許多種類型的網路物件，其中以「主電腦」和「防火牆」最爲常見。 IBM Firewall 所附的網路物件預設值爲 ″The World″。 這是一個全域物件，它包含所有可能的 IP 位址。在您填好網路架構工作清單之後 (請看第8頁的『網路架構規劃工作清單』)，您就可以開始建立物件了。

您可建立單一或群組物件。所有的網路物件是由 IP 位址及位址遮罩 (子網路遮罩) 所定義，所以若要用一個物件來代表一個範圍的網路位址，也是有可能的。

使用架構從屬站來定義網路物件

若要定義單一網路物件，請從架構從屬站導覽樹狀結構選取**網路物件**，即會出現「網路物件」對話框。 連按兩下**新增**。即顯示**新增網路物件**對話框，如第28頁的圖 9 所示。

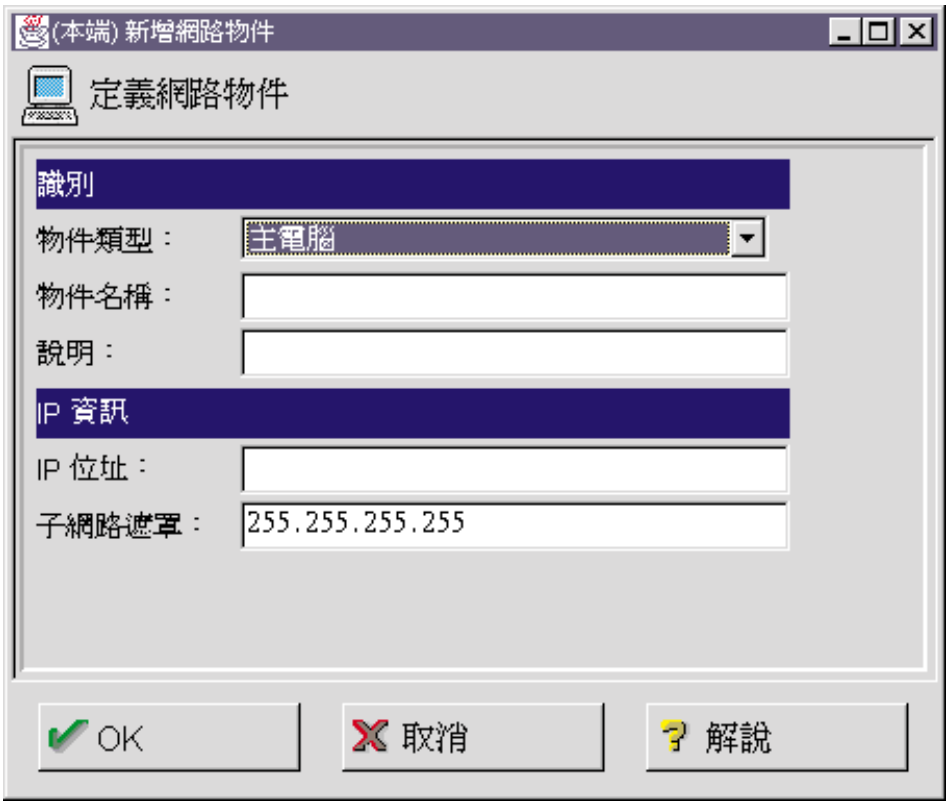

圖 9. 新增網路物件

1. 請輸入物件類型。按一下**物件類型**箭頭，以查看您可以建立的物件類型。基於效能的考量，您最好建立網路類型物件，而非主電腦類型物件。您可以建立的物件類型有：
   - 主電腦 - 網路中的特定節點，其遮罩爲 255.255.255.255。
   - 網路 - 以位址範圍和特定子網路遮罩描繪出的網路位址集體範圍。
   - 防火牆 - 已安裝防火牆的單一機器，其遮罩爲 255.255.255.255。 只有防火牆網路物件才能作爲 IBM 通道或手動通道的目標。
   - 路由器 - 一種主電腦，可在兩個或兩個以上的網路之間遞送傳輸的資料，其遮罩爲 255.255.255.255。
   - 介面 - 機器上的一種網路配接卡，其遮罩爲 255.255.255.255，並不一定是「防火牆」中的配接卡。
2. 填入物件名稱。
3. 填入說明。本欄位是選用性的。
4. 請鍵入本物件的帶點十進位數 IP 位址。

5. 請鍵入子網路遮罩，它指定位址中的位元來比較 IP 封包的位址。
6. 按一下 **OK**。

網路物件群組

代表網路物件集合的群組。群組用來作爲設定連線時的便利工具，可免除重複性作業。 例如，把以網路物件呈現的個別位址集合起來，成爲一個網路物件群組，來代表一個部門。 此部門可作爲連線的來源或目的位址。

若要定義一群組的網路物件，請從架構從屬站導覽樹狀結構選取「網路物件」， 即會出現**網路物件**對話框。 連按兩下**新增群組**，即顯示**新增網路物件**對話框。

1. 填入群組名稱。
2. 填入說明。本欄位是選用性的。
3. 按一下**選取**來選取群組的物件。
4. 按一下 **OK**。

秘訣: 建議您儘可能將連續的位址範圍包含在單一網路物件中。 如此可提高連線規則處理的效能。下面範例可說明此種情況。

```
      會計部門
Kevin 的機器  191.1.10.1
Susan 的機器  191.1.10.3
Helen 的機器  191.1.10.5
Peter 的機器  191.1.10.7
Bob 的機器    191.1.10.9
```

若要爲本會計部門建立網路物件，請輸入本群組的 IP 位址資訊如下： 191.1.10.0 with a Subnet Mask of: 255.255.255.0。本網路物件（會計部門）可作爲連線的來源或目的地。

備製您的 Firewall 架構

Firewall 會將其所有的架構檔存放在 ROOTDIR\config 中。若您想只要備製 Firewall 架構，而不要任何 Firewall 檔案的話，請備製 ROOTDIR\config 目錄的所有內容。

若您要復置已備份的 Firewall 架構，請將 ROOTDIR\config 目錄中所有的現存檔案，然後再復置該檔案的備份版本。您必須先重建並啓動過濾規則，所復置的架構才會生效。

主要防火牆架構檔列示如下。您 Firewall 上的 \config 目錄可能不會包含這裡所列的每個檔案。請注意：雖然大部份的防火牆架構檔都是可用文字編輯程式來檢視的純文字檔，但是，**您不能以手動的方式來編輯這些檔案**。

- carriers.cfg - 呼叫器的電訊公司的定義
- cfgfilt.output

- explode.cfg
- filters.active - 表示是否使用過濾處理
- fwadpt.cfg - 網路介面的定義
- fwconfig.map - 包含架構檔名稱
- fwconns.cfg - 過濾器連線定義
- fwfilters.cfg - 目前在使用中的過濾器
- fwhttp.cfg - HTTP proxy 架構
- fwmail.conf - SafMail 架構
- fwobjects.cfg - 網路物件定義
- fwpolicy.cfg - 安全性策略選項
- fwrules.cfg - 過濾規則模版定義
- fwservices.cfg - 服務程式定義
- fwsocks.cfg - 架構從屬站的 Socks 5 規則
- fwtdefn.conf - 警示定義
- fwtpproxy.cfg - 透通式 Proxy 定義
- fwusrdb.cfg - 「防火牆使用者」資料庫
- logmgmt.cfg - 儲存定義
- modems.cfg - 數據機定義
- pager.cfg - 呼叫器定義
- rcsfile.cfg - 架構服務程式參數
- Socks5.conf - 產生出來的 Socks 5 架構檔
- Socks5.header.cfg - 所產生之 Socks5.conf 的使用者提供部份
- syslog.conf - 日誌機能定義

第6章 處理領域名稱服務程式

本章將說明如何架構與 IBM Firewall 相關的「領域名稱服務程式 (DNS)」。 DNS 的目標是，提供完整領域名稱服務給安全網路內的主電腦使用，同時不提供任何資訊給安全網路外的主電腦。 此方式可讓安全性網路內的使用者存取 Internet 所提供的所有服務。 而且，透過拒絕洩露安全性網路的相關資訊，將使入侵者更難以找到可以下手攻擊的電腦。

若要完成此目標需有三個領域名稱伺服器：

1. 一個在 IBM Firewall 上
2. 一個在安全網路中
3. 一個在安全網路外

關於 DNS 如何使用 IBM Firewall 的資訊，請參閱第31頁的圖 10。

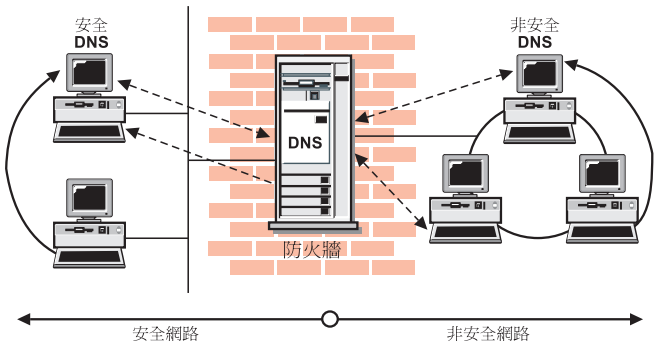

圖 10. DNS

Firewall 的架構方式，是要作爲安全性網路的名稱伺服器與提供服務給非安全性網路的名稱伺服器之間的閘道。 Firewall 所扮演角色的正式術語爲*僅快取名稱伺服器*，因爲 Firewall 的 DNS 本身不含任何資料庫檔案的緣故。

第31頁的圖 10 將說明 Firewall 的角色。每當 Firewall 必須解析某個名稱以進行其操作時，它便會詢問安全端名稱伺服器。每當查詢被轉送至 Firewall 時，它便會將查詢轉送至非安全名稱伺服器。

當安全性網路上的從屬站要求安全端資訊時，從屬站會將其要求傳送給安全端 DNS，並由 DNS 來答覆。當同一個從屬站要求非安全端資訊時，從屬站會將要求傳送給同一個安全端 DNS。由於所查詢的是非安全性資訊，因此安全端 DNS 無法進行答覆，而由 DNS 將該查詢轉送給 Firewall。在非安全性 DNS 將要求轉送給 Firewall 的情況下，該要求會轉送給非安全性 DNS 領域，因此具敏感性的資訊同樣不會被洩露。

使用架構從屬站架構 DNS

欲架構 DNS，請從架構從屬站導覽樹狀結構選取「系統管理」。 連按兩下檔案資料夾圖記以展開檢視畫面。 選取**領域名稱服務程式**。 「IBM Firewall」會顯示現行的 DNS 架構，您可以將它修改。

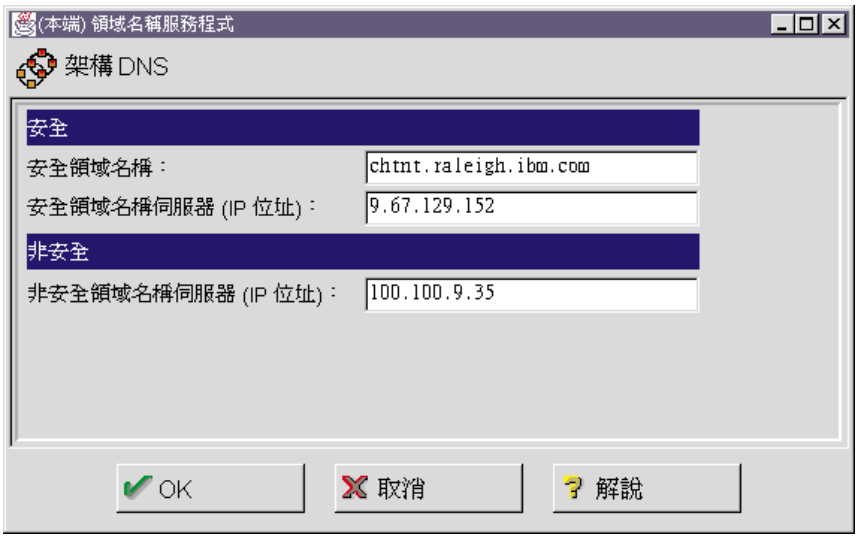

圖 11. 領域名稱服務程式

註: 新增 DNS 時，防火牆會儲存並將任何現有領域名稱服務程式架構檔更名。

1. **安全領域名稱**欄位可識別領域名稱， Firewall 會將該領域名稱附加至任何不完整的主電腦名稱。
2. **安全領域名稱伺服器**欄位表示，可分辨受 IBM Firewall 保護，防止 Internet 侵入的主電腦名稱和 IP 位址的名稱伺服器。 您可以輸入帶點十進位數的 IP 位址，並以空格加以區隔。
3. **非安全領域名稱伺服器**欄位意指由您的服務提供者所提供的伺服器，用於解析非安全性網路的相關資訊。 您可以輸入帶點十進位數的 IP 位址，並以空格加以區隔。

註: 當名稱伺服器起始設定時，它會送出查詢，以取得 Root 名稱伺服器的列示。 大部份的執行會將此列示保留在記憶體中。 不過， Mircosoft 的執行則會將此列示寫回到架構檔。 這時雖然不會修改名稱伺服器的行爲，但是會變更顯示在**非安全名稱伺服器**欄位中的值。 不過您不必特別留意這件事。

架構安全名稱伺服器

安全名稱伺服器必須架構爲能將未解析的查詢轉送給 Firewall。 如果您具有標準的 BIND 執行，請將 *forwarders* 陳述式及 *cache* 陳述式，新增至您安全名稱伺服器上的 *boot* 檔案中：

```
forwarders      aaa.bbb.ccc.ddd
cache           .               named.cache
```

建立 cache 檔 *named.cache*，以指向 Firewall：

```
. 99999999 IN NS firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

其中 *private.com* 是從安全端所用的領域名稱，而 *aaa.bbb.ccc.ddd* 則是 Firewall 的 IP 位址。

此外，您可能要將您 firewall 的主電腦名稱新增至 DNS 資料庫。 這時您的使用者便可利用 Firewall 的主電腦名稱來取代其 IP 位址，存取 Firewall 的 Socks 伺服器、HTTP proxy、Telnet proxy 及 FTP proxy。 不過這項操作需要執行兩個額外的步驟，詳細資料請參閱*第 4 章的 DNS 與 BIND*。 本書的明細請參閱*參考書目*。

首先，將一筆 A 記錄新增至領域資料庫檔案：

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

然後，再將一筆 PTR 記錄新增至反向尋找 (reverse-lookup) 檔案：

```
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

如果您沒有針對您的安全性網路使用 DNS，則您的防火牆必須仍舊能解析它自己的資訊。請按照一般情況所描述的步驟來架構防火牆，但是必須將防火牆的安全介面列示於**安全名稱伺服器**欄位中。 然後，將下列這一行新增至 `c:\winnt\system32\dns\boot`。

```
primary ccc.bbb.aaa.in-addr.arpa c:\winnt\system32\dns\fwnamed.rev
```

然後，再將 *fwnamed.rev* 建立成類似如下所示：

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9        ; Serial
                          86400    ; Refresh after 1 day
                          300      ; Retry after 5 minutes
                          654000   ; Expire after 1 week
                          3600  )  ; Minimum TTL of 1 day
ccc.bbb.aaa.in-addr.arpa.          IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.      IN PTR   firewall.private.com.
```

架構安全從屬站

安全性網路上的從屬站必須架構爲能將它們的查詢傳送給安全名稱伺服器，不是傳送給 Firewall。 這項操作的重要性在於，它能確保安全端資訊不會儲存在 Firewall 的記憶體內的快取記憶體中。 同時，它會減輕 Firewall 的工作量，這是因爲 Firewall 只有在某查詢關係到將查詢從安全端轉送到非安全端時，才會參與此作業。

如果您沒有針對您的安全性網路使用 DNS，您的從屬站便須指向 Firewall，作爲從屬站的名稱伺服器。

發佈服務作為公用

許多企業組織會想將某些特定服務發佈到 Internet 作爲公用項目。 通常，這些服務項目包括 E-mail 及 Web 伺服器，而事實上您可以使用任一種類型的 TCP/IP 伺服器。 若要使這類服務項目可供使用，您不僅要將伺服器置於可以被存取的網路上，還必須將該伺服器與公用 DNS 一起列示，如此使用者才能取得正確的資訊。

您可以採取兩種方法完成這項操作。方法之一是：您的服務提供者可將您的伺服器列示爲其領域的一部份 (而因此置於它們的名稱伺服器上)，或者您必須提供您自己的名稱伺服器，並且在 Internet 上登記該伺服器。 由您的 Internet 服務提供者 (ISP) 爲您提供這項服務，遠比第二種方式容易得多。 如果您可以選擇這個選項，您必須將所要列示的主電腦名稱及 IP 位址提供給服務提供者。例如，假設您的公用 Web 伺服器爲 *www.public.com*，而其 IP 位址爲 *50.100.150.200*，則您必須要求您的 ISP 爲您列示 *www.public.com at 50.100.150.200*。

此外，假如您想接收到 E-mail，則您必須要求您的 ISP 針對您的公用 E-mail 領域，將您的防火牆列示爲*郵件交換器*。 ISP 必須知道主電腦名稱 *(gateway.public.com)*、其 IP 位址 *(50.100.150.201)*，以及您希望由此接收郵件的領域名稱 *(public.com)*。

如果您的 ISP 不願意爲您提供這些服務，則您必須自行完成這項操作。 同樣的，您可以有兩個額外的選項。您可以將 DNS 伺服器置於您的 DMZ，或者您也可以將您的防火牆當作該名稱伺服器。使用防火牆並不會引發其他的安全風險，這是因爲您放置在該處的資料庫檔案，並沒有包含任何安全性網路的相關資訊。此處所儲存的資訊，只限於您選擇要提供的公用服務項目。

設定 DNS 伺服器的相關詳細資訊，請參閱*參考書目*所列之 *DNS and BIND* 的第四章。我們強力推薦您閱讀這一章，必要時，我們還會將它納入作爲書中的導讀章節。 設定 DNS 伺服器並不是一件容易的事，因此我們建議最好能由專家來執行。如果您可以找到這類專家，請愼重考慮好好借重他們的專業技術。

相關資訊，請參閱第35頁的『架構範例』。

安裝 Microsoft 的 DNS 伺服器

欲安裝 Microsoft 的 DNS 伺服器，請到「控制台」，按二下**網路**，按一下**「服務程式」標籤**，按一下**新增**，然後選取 **Microsoft DNS 伺服器**。您必須要有安裝作業的 CDROM。

DNS 疑難排解

IBM eNetwork Firewall 參考手冊 包含 Firewall 疑難排解章節。 其將以特定章節詳細描述 DNS 相關問題。 本節將提供您建議事項，方便您使用 *nslookup* 命令，來識別 DNS 系統的錯誤區段。

架構範例

這個部份將會以圖示說明一些防火牆可能會用到的架構範例。這些範例的大部份重點會放在 DNS 作業所需的架構上。它和說明網路的範例不一像，所以請多花點時間來了解每一個範例，並且將適當的概念運用在您的安裝作業上。

範例 1：在非安全介面上 DMZ 中的 DNS 伺服器

第一個範例說明當您要在非安全性網路上的 DMZ 中操作名稱伺服器時，所需用到的檔案，如第35頁的圖 12 所示。

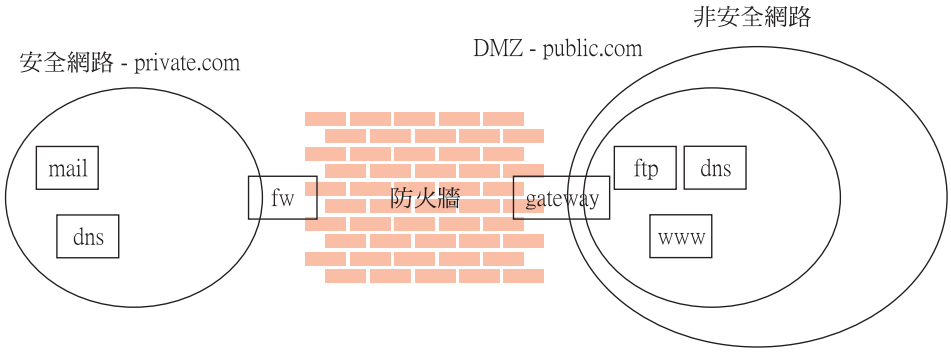

圖 12. 在非安全性網路上 DMZ 中的名稱伺服器

此圖示說明一 IBM Firewall 內的專用網路 *private.com*，該 IBM Firewall 的安全介面名稱爲 *fw.private.com*，而非安全介面的名稱爲 *gateway.public.com*。該公司的 DMZ 屬於非安全介面，並且包含名稱伺服器 *dns.public.com*、 FTP 伺服器 *ftp.public.com* 及 Web 伺服器 *www.public.com*。在 *dns.public.com* 上用來執行此計劃的檔案，如下所示：

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                   3600        ; retry after 1 hour
                  604800      ; expire after 1 week
                  86400  )    ; minimum TTL 1 day
;
; Nameservers
;
public.com           IN NS  dns.public.com.
;
; Hosts in the DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Mail-related entries
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                  3600        ; retry after 1 week
                  604800      ; expire after 1 week
                  86400  )    ; minimum TTL 1 day
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                  3600        ; retry after 1 week
                  604800      ; expire after 1 week
                  86400  )    ; minimum TTL 1 day
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

就此檔案而言，最好的做法是從 *ftp://ftp.rs.internic.net/domain/named.root* 用 FTP 來傳送現行的 root 名稱伺服器列示。

boot

```
primary public.com                  db.public
primary 150.100.50.in-addr.arpa     db.50.100.150
primary 0.0.127.in-addr.arpa        db.127.0.0
cache   .                           db.cache
```

欲設定資料傳輸過濾器來允許適當的 DNS 資料傳輸，請啓用**安全性策略**畫面上的*允許 DNS 查詢*。

範例 2：在專用介面上 DMZ 中的 DNS

在第二個範例中，DMZ 的 DNS 仍然是在專用的名稱伺服器上，但是這一次 DMZ 是屬於另一個介面，和非安全性網路的介面不同。

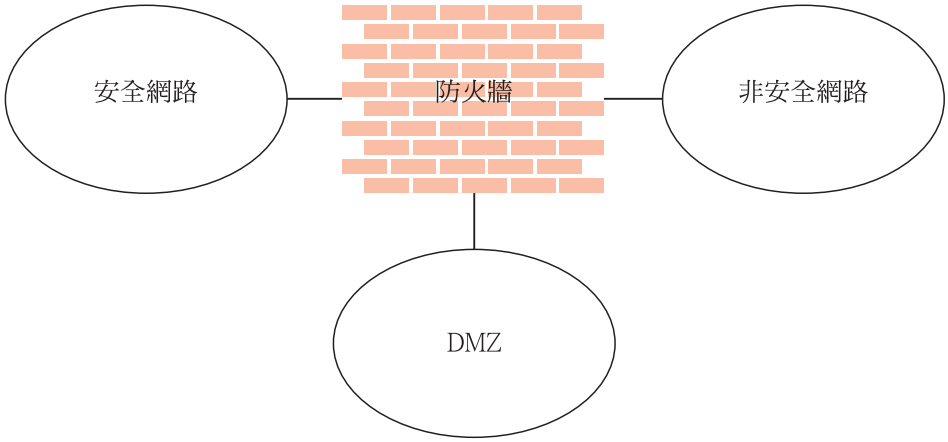

圖 13. 在專用介面上 DMZ 中的 DNS

dns.public.com 上的 DNS 資料檔案與前述範例中的檔案相同。但是爲了要使該名稱伺服器能夠讓公用網路存取，您必須開啓資料傳輸過濾器，或是執行區域轉送，將資料檔複製到「防火牆」。

欲開啓資料傳輸過濾器，請將名稱標題爲 *DNS 伺服器查詢*、 *DNS 回應* 及 *DNS 從屬站查詢* 的這三個規則模版複製。將每一個規則的遞送設定從*本端*變更爲*遞送*。然後將那三個新規則模版併入服務程式，並且設定下列的流程指示器：

- DNS 從屬站查詢：--->
- DNS 回應：<---
- DNS 伺服器查詢：--->
- DNS 伺服器查詢：<---

在使用 *The World* 爲來源物件，且以 *dns.public.com* 爲目的地物件的連線中，將此服務程式併入。

欲執行區域轉送，您必須設定資料傳輸過濾器，並指示名稱伺服器複製適當的檔案。欲設定資料傳輸過濾器，請執行下列步驟：

1. 在**安全性策略**畫面上，啓用*允許 DNS 查詢*。
2. 新增一個從 *dns.public.com* (來源物件) 到「防火牆」的 DMZ 介面 (目的地物件) 的連線，該連線包含「*DNS 轉送*」服務程式。

欲啓動區域轉送，請將下列字行加到「防火牆」`c:\winnt\system32\dns` 目錄下的 *boot* 檔中：

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

然後到「服務程式控制管理系統」中，關閉並重新啓動「DNS 伺服器」服務程式。

範例 3：用防火牆當作安全名稱伺服器

欲使用「防火牆」來當作安全名稱伺服器，請將資料庫檔案 (通常位於安全伺服器上) 放置在「防火牆」上。然後您的從屬站就可指向該「防火牆」來作爲它們的 DNS 伺服器。此方法所引發的相關風險有：DNS 伺服器無法分辨要求是來自安全端，還是來自非安全端。因此，它會將此安全端的資訊提供給任何提出要求的從屬站；您就再也無法隱藏您的安全 DNS 資訊了。

若要執行這個方法，請先用架構從屬站來架構「防火牆 DNS 機能」。在*安全領域名稱* 欄位中，列出您將會在您的安全網路上使用的領域名稱。在*安全名稱伺服器* 中，列出「防火牆」的安全介面。在*非安全名稱伺服器* 中，就如一般的情況，列出您的 ISP 所提供的名稱伺服器。然後，您必須在「防火牆」上建立一個反向尋找 (reverse-lookup) 檔，以增強此架構。

建立 `c:\winnt\system32\dns\fwnamed.rev` 這個檔案，內容如下列範例。

就此範例而言，「防火牆」的安全介面名稱爲 *fw.private.com*，而其 IP 位址爲 *10.100.100.1*。

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
1.100.100.10.in-addr.arpa.        IN NS fw.private.com.
1.100.100.10.in-addr.arpa.        IN A  fw.private.com.
```

然後將下面這一行加到 `c:\winnt\system32\dns\boot` 中：

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

在此範例中，從屬站的架構必須將「防火牆」(10.100.100.1) 指定爲該從屬站的 DNS 伺服器。您的「防火牆」將會幫助您解析外部資訊，但是沒有安全端資訊的解析。意即，若有任何安全端從屬站想要連線到架構伺服器或任何「防火牆」上的 proxy 伺服器，都必須用 IP 位址來參照「防火牆」，而不是用主電腦名稱。

第7章 SafeMail

IBM Firewall SafeMail 閘道提供 SMTP 資料傳輸的閘道。 它會將訊息從安全郵件伺服器傳遞至非安全的一方，並在傳遞過程中隱藏具敏感性的領域名稱。它會將訊息從非安全的一方傳遞至安全郵件領域，並保護安全性網路免於遭受侵害。

雖然 SafeMail 並不會執行內容掃描，不過 SafeMail 卻提供了使用者呼叫，而透過它便可執行內容掃描。相關資訊，請參閱第43頁的『SafeMail 使用者呼叫』。

SafeMail 會即時將訊息從送件者傳遞給接收者。這項操作可以避免因爲維護 Firewall 上的訊息佇列，而可能引發的風險和複雜性。在此情況下，相鄰的郵件領域便須具備特定的架構基本需求。在某些情況下，這些基本需求對特定的安裝作業而言，可能會顯得有點不切實際。若出現這類情形，您可以另行購買並安裝數種 SMTP 伺服器中的任一種，以取代 SafeMail。如果您選擇要安裝完整的 SMTP 伺服器，請在架構它時特別注意安全方面的問題。相關資訊，請參閱第43頁的『以 SMTP 伺服器取代 SafeMail』。

使用架構從屬站來架構 SafeMail

要架構 SafeMail 時，請從架構從屬站導覽樹狀結構中選取「系統管理」。 連按兩下檔案資料夾圖記以展開檢視畫面。選取 **SafeMail**。IBM Firewall 將顯示已架構郵件伺服器及領域的列示。您必須對已架構的每一個專用郵件領域，架構一個項目。

1. 要新增領域時，請選取**新增**，然後按一下**開啓**。**新增郵件伺服器**對話框即會出現。
2. **安全領域名稱**欄位包含讓防火牆安全端中之使用者知道其郵件領域的名稱。
3. **安全郵件伺服器**欄位包含此項目適用之郵件伺服器的主電腦名稱或帶點十進位數 IP 位址。此伺服器必須位於其中一個安全網路上。您只能列出指定領域的一個郵件伺服器。
4. **公用領域名稱**欄位所包含的郵件領域名稱，是防火牆非安全端之使用者所知道的郵件領域名稱。這個名稱將被安全領域名稱所取代，以將安全網路的內容隱藏起來。
5. 按一下 **OK**。

變更郵件架構項目

要變更郵件架構項目時，請從列示選取項目，然後按一下**開啓**。 **變更郵件伺服器架構**對話框即會出現。

安全領域名稱欄位已停用，但您可變更其它欄位，如第41頁的『使用架構從屬站來架構 SafeMail』中所示。

註:

1. 如果先前已架構 SafeMail，而您又在此指定另一個安全郵件伺服器的話，則新指定的安全郵件伺服器會取代先前架構的郵件伺服器。
2. 如果先前**未**架構 SafeMail，而且又在此指定另一個安全郵件伺服器，則後來指定的這個郵件伺服器會新增到該架構中。

刪除郵件架構項目

要刪除 SafeMail 架構項目時，請從列示選取項目，然後按一下**刪除**。畫面上即會顯示刪除警告。 按一下 **OK**，即可刪除；或者，如果您改變主意不要刪除，請按一下**取消**。

架構安全伺服器

您必須將您的安全郵件伺服器，架構爲能將 Firewall 列示爲其不明領域的閘道。這項操作將使原先要送至非安全性網路的郵件，被轉送至 Firewall。同時，每一個伺服器均須架構爲能接受傳送給其公用領域名稱以及其專用領域名稱的訊息。當 Firewall 從非安全性網路轉送訊息時，所有的接收者會與其公用領域名稱一起列示出來。

如果您的安全性網路中具有一個以上的不同郵件領域，您亦須架構每一個伺服器，使它能將原先要傳送至其它安全性領域的郵件直接轉送至該伺服器，而不透過 Firewall。這項操作可減輕 Firewall 不必要的工作負擔，並能使 Firewall 的即時遞送機制正常運作。

架構公用領域

非安全性網路中必須執行的唯一架構作業，是要將您的 Firewall 列示爲您網路的郵件交換器。請要求您的服務提供者，將必要的資訊新增至他們的 DNS 伺服器。請參閱第31頁的『第6章 處理領域名稱服務程式』，以取得相關機制的特定資訊。

該項操作的目標，是要將您的 Firewall 列示爲每個要接受郵件的公用領域名稱之*郵件交換器*。例如，假設您在您的安全性網路內使用領域名稱 *private.com*，而在您的安全性網路外則使用領域名稱 *public.com*，您可以將您的防火牆命名爲 *gateway.public.com*。在這種情況下，您可以要求您的服務提供者將 Firewall 的主電腦名稱及 IP 位址列示爲主電腦 (它通常會與 ″A″ 記錄和 ″PTR″ 記錄一起列示)。然後，由於您要接受傳送至 *user@public.com* 的郵件，您可以要求您的服務提供者，針對領域 *public.com* 新增一筆 MX 記錄，而 public.com 會爲該領域將 *gateway.public.com* 列示爲郵件交換器。如果您同時要接受傳送至 *user@somethingelse.com* 的郵件，您可以列示一筆額外的 MX 記錄 (它也指向 Firewall)。

SafeMail 使用者呼叫

SafeMail 將提供使用者呼叫，在進行安裝作業時便可藉此調整 SafeMail，以拒絕可能發生的惡意資料傳輸。欲取得針對此目的所提供的「軟體開發人員工具組」 (Software Developers Kit) 的詳細說明，請參閱 *IBM eNetwork Firewall 參考手冊*。

此特性可讓您建立一個函數 *UsrCheck()*，每當 SafeMail 接受來自送件者的封包時，便會呼叫它。此函數會接受傳遞給它的結構，該結構中含有數個與系統狀態有關聯的欄位。此結構中含有一個獨一無二的階段作業 ID、用於傳送與接收伺服器的 IP 位址、先前所接收命令的指示器，以及一個包含已經過分析的封包之純文字緩衝區。

以下是可在此函數中執行的檢查類型範例：

- *被禁止的*主電腦列示
- 掃描不被允許的字元順序，例如：不適當的語言或專案碼名稱
- 檢查內嵌的加引號字串
- 訊息長度限制

如果需要的話，使用者呼叫也可作爲與協力廠商內容審查 (content-screening) 產品間的介面。

如果使用者呼叫函數決定不處理某一則訊息，該函數會將原因碼傳回給 SafeMail。SafeMail 會立即拒絕與傳送中的 SMTP 伺服器之間的連線。同時，會有一則訊息被寫入防火牆日誌，包括由使用者呼叫所傳回的原因碼在內。

在編寫使用者呼叫時，請隨時注意當接收每一個封包時，均會呼叫此函數。請在編寫它時特別注意效率問題，避免對系統的效能造成負面的衝擊。另外，您也須注意此函數將在多執行緒的環境下執行，因此它的編寫方式也必須考慮執行緒安全問題。您可以用任一種編譯器來編寫使用者呼叫，只要該編譯器支援多執行緒作業，而且可以使用 *_cdecl* 鏈結慣例。IBM Visual Age C++ 與 Microsoft Visual C++ 中均提供 makefiles 範例。

以 SMTP 伺服器取代 SafeMail

停用 SafeMail

若要停用 SafeMail，以避免與其它 SMTP 伺服器產品發生衝突，請自**服務程式控制管理系統**中停用 SafeMail 服務程式。在 Windows **開始**功能表中，選取**設定，控制台，服務程式**。透過捲動來選取 *IBM Firewall SafeMail Server*。按一下**啓動**。在**啓動類型**欄位中，選取**停用**。按一下 **OK**。

架構 SMTP 伺服器

當您安裝完整的 SMTP 伺服器以取代 SafeMail 時，您必須先考慮數個層面。本節將說明 SafeMail 的安全性功能，讓您能將您的 SMTP 伺服器，架構成可以執行與其類似的功能。

不過，某些特定的 SMTP 伺服器產品可能會有無法執行某些作業的問題，因此請在購買產品之前，先仔細研究所有可用的選項以及您的需求。

您可能會碰到某些特定的攻擊，試圖爆掉或毀壞郵件佇列。雖然沒有一個功能完整的伺服器能在不使用郵件佇列下操作，但假如您事先指定一個專用的磁碟容體供該作業運用，便可降低郵件佇列的相關危機。這項操作可以將因爲爆滿的佇列而對防火牆的其它操作造成的衝擊降至最低。

另外一個重要事項是，您的郵件伺服器必須隱藏安全性網路的相關資訊。根據 SMTP 的規則，每一個可轉送郵件的伺服器均應該插入一個*接收：*表頭行。這些表頭行可能會被入侵者用來對映您的安全性網路。SafeMail 會在它處理郵件時除去所有的表頭；請將您的 SMTP 伺服器架構成具備相同的功能。同時， SafeMail 會將所有專用的主電腦名稱，重新編寫爲公用領域名稱。這項操作會進一步移除更多可用於對映您網路的資訊。

SafeMail 的記載輸出範例

以下是 SafeMail 的記載輸出範例。

```
Feb 03 13:46:11 1998 mr16n18: ICA2163i: safemaild started.

Feb 03 13:41:14 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e7a19
received from RACK3BD.
Feb 03 13:41:21 1998 mr16n18: ICA2179i: SafeMail has forwarded 215575
bytes for connection 0xd71e6118 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:21 1998 mr16n18: ICA2178i: SafeMail session 0xd71e7a19
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:23 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e831a
received from RACK3BD.
Feb 03 13:41:36 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e901b
received from RACK3BD.
Feb 03 13:41:56 1998 mr16n18: ICA2179i: SafeMail has forwarded 215567
bytes for connection 0xd71e7a19 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e831a
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e901b
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 346
bytes for connection 0xd71e901b from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 358
bytes for connection 0xd71e831a from 9.67.144.52 to 9.67.131.250.
```

日誌訊息指出下列資訊：

- ICA2177 - 指示新連線的開始。
- ICA2179 - 指示終止成功。
- ICA2178 - 指示已與接收訊息的 SMTP 伺服器建立連線。

- ICA2181 - 指示 SafeMail 拒絕了該階段作業。欲取得原因碼，請參閱 *BM eNetwork Firewall 參考手冊*。
- ICA2180 - 指示階段作業停止。
- ICA2182 - 指示使用者呼叫決定要拒絕階段作業。

第8章 透過防火牆控制資料傳輸

本章爲您解釋說明，如何使用架構從屬站來透過 Firewall 控制網路資料傳輸。 使用「專用過濾器」，防火牆會根據各種基準，如時間、IP 位址及子網路，來過濾階段作業層次上的封包。過濾器在安全及非安全性網路介面之間活動，它們不會影響防火牆路由表。

在預設的狀況下，Firewall 不允許在安全與非安全性網路之間傳遞任何資料。您必須建立連線，才能在安全與非安全性網路之間傳遞特定類型的資料。

使用架構從屬站建立連線

請使用第48頁的圖 14 中說明的架構從屬站元件，來建立網路物件、規則模版及連線。

連線 連結網路物件與服務程式及（或）socks 模版，來定義端點之間可容許的通信類型。每一個連線是定義來源與目的網路物件之間可容許或拒絕的特定 IP 資料傳輸類型。

服務程式

由一或數個模版建立而成。服務程式會定義允許或拒絕哪些類型的 IP 資料在來源及目的地物件之間傳輸。例如，您可以建構一個服務程式來允許 Telnet 或拒絕 Ping。 (FTP 服務程式中有一種是由 8 個規則模版所組成)。 IBM Firewall 有預設服務程式集。 您不能刪除這些預載的預設服務程式，但可以修改某些欄位。不過，若這些預先定義的服務程式不符合您的需求，您可以使用規則模版來建立新規則，以新增至服務程式。相關資訊，請參閱第68頁的『定義服務程式』。

規則模版

指示 Firewall，根據 IP 封包的各種屬性，允許或拒絕這些 IP 封包進入。

Socks 模版

指示防火牆 socks 常駐程式，根據 IP 封包的各種屬性，允許或拒絕這些 IP 封包進入。

網路物件

代表各種與 Firewall 互動的網路元件，如主電腦、使用者及子網路。它們是由 IP 位址及位址遮罩所定義，所以若要用一個物件來代表整個範圍的網路位址，也是有可能的。網路物件可組成群組。

網路物件群組

代表一或數個網路物件；可作爲設定連線時的便利工具，而且可避免重複性的工作。例如，將許多位址組成一個網路物件群組，來代表一個部門。然後，這個網路物件群組就可以用來當作連線的來源或目的地。

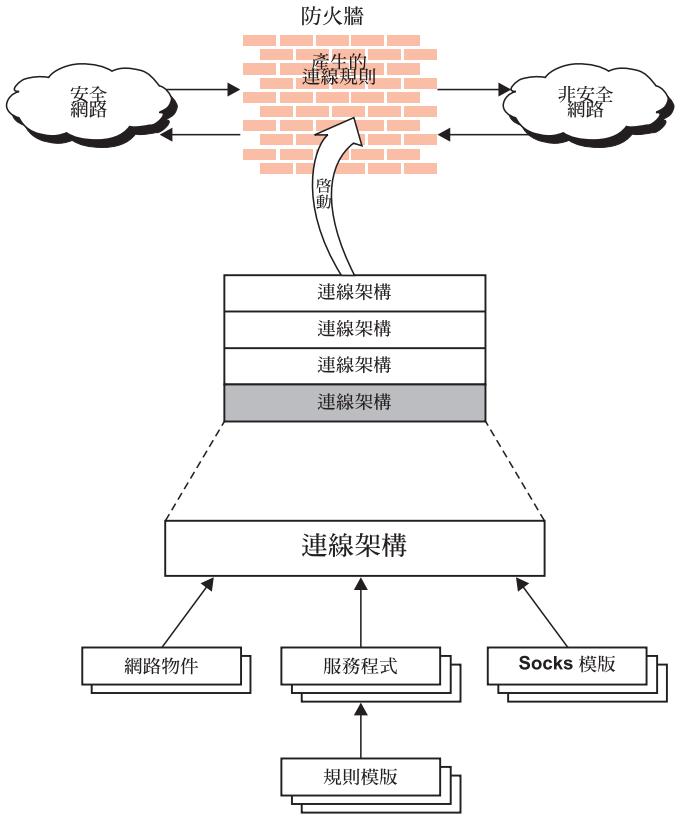

圖 14. 建立連線

使用預先定義的服務程式建立連線

若要以兩個網路物件或網路物件群組爲端點，允許或拒絕特定的通信類型，您需建立一個連線。

在定義網路物件之後，您就可以建立連線。若要通過 Firewall 來傳輸資料，請選取一個網路物件或群組作爲來源，並選取另一個網路物件或群組作爲目的地。

欲建立連線，請從架構從屬站導覽樹狀結構中選取「資料傳輸控制」，然後按兩下檔案資料夾圖記，將資料夾展開。 選取**連線設定**。**連線列示**對話框即會出現。選取**新增**，然後按一下**開啓**。即出現**新增連線**對話框，如第49頁的圖 15 中所示。

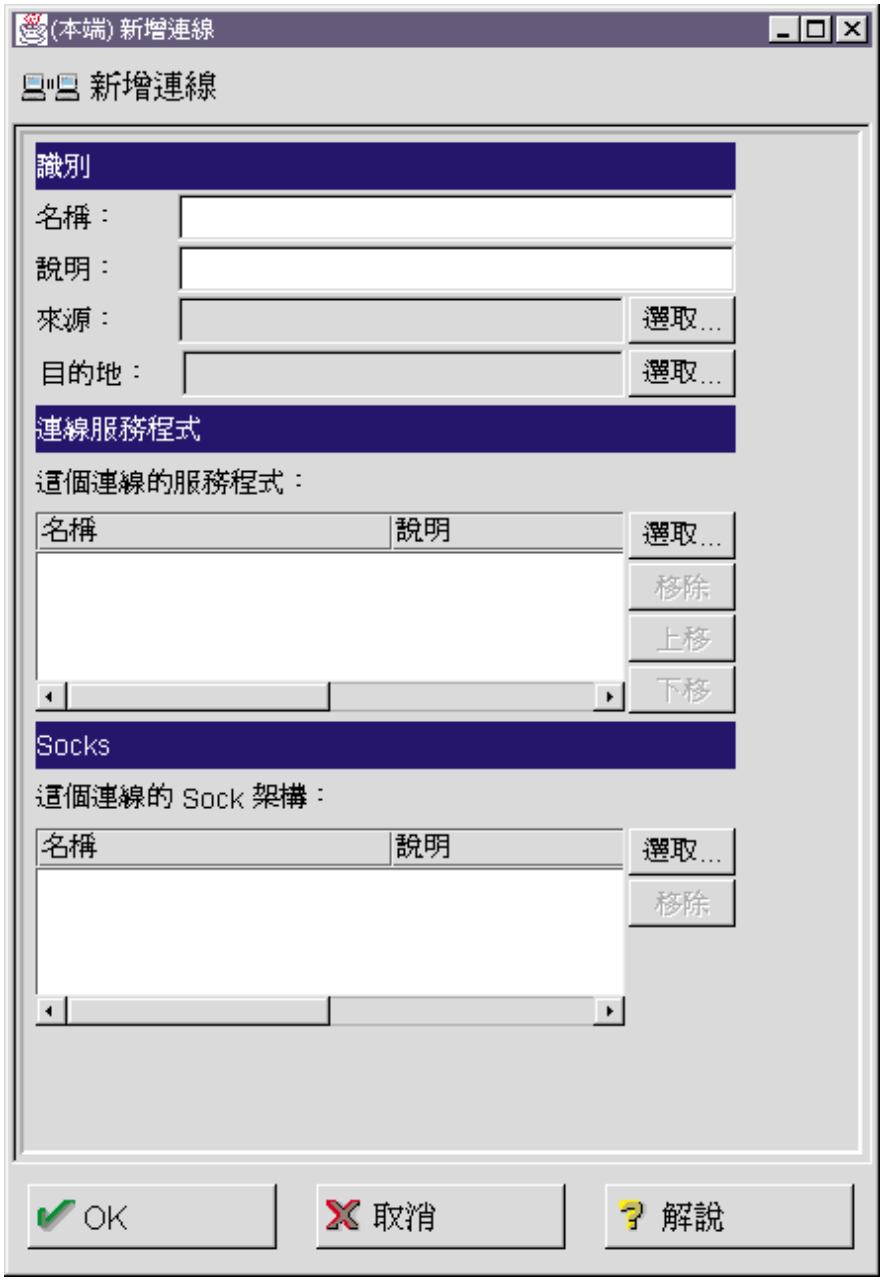

圖 15. 新增連線

1. 填入連線名稱。

2. 填入連線說明。
3. 在來源欄位中，按一下**選取**，從**網路物件**對話列示中選擇網路物件。
4. 在目的地欄位中，按一下**選取**，從**網路物件**對話列示中選擇網路物件。
5. 欲選擇此連線的務程式列示，按一下**選取**，並選擇您要在端點間控制的資料傳輸類型。
6. 從列示中選擇一個或多個服務程式，將服務程式新增到「連線」。
7. 您可以選取服務程式，然後按一下**往上移**或**往下移**，重新排列列示的順序。請參閱第50頁的『排列連線順序』。
8. 您可以選取服務程式，然後按一下**移除**，來移除服務程式。
9. 使用**此連線的 Socks 架構**。請遵循步驟 5-7，完成 Socks 的連線。
10. 在一切都已定義之後，按一下 **OK**。
11. 啓動您的所有連線。請參閱第50頁的『連線啓動』。

排列連線順序

大部份的 IBM Firewall 只有少於 1000 個的規則。愈多的規則，愈會影響效能。

在網路介面上接收封包時，無論是傳入或送出防火牆主電腦，都會從所產生的連線規則最上面那一條開始引用。如果封包的資訊完全符合規則中的資訊，就會執行該動作 (允許或拒絕)。若搜尋整個檔案後沒有發現任何符合情形，即拒絕要求。

秘訣: 可將較特定的連線放在靠近頂端的地方，較不特定的連線則放在靠近底端的地方。例如，您可能有一個位址爲 (1.1.10.X) 的「ABC 部門」，及一部位址爲 (1.1.10.7) 的機器，作爲「ABC 部門」內部的伺服器。若您要排除機器 1.1.10.7，因爲它是不應使用於 telnet 資料傳輸的伺服器，則您必須將「拒絕 Dept ABC 伺服器的 telnet」連線放在「允許 Dept ABC 的 telnet」連線之前。如果您倒轉了連線順序，就絕對不會碰到拒絕連線。

連線啓動

註: 在您啓動連線之前，請確定您已定義安全介面。

選取架構從屬站導覽樹狀結構中的**連線啓動**，可讓您執行下列作業：

重建並啓動連線規則
Firewall 會從連線架構，建立產生的連線規則，並啓動該規則集。

停止連線規則
Firewall 現在受預設規則保護。

列示現行的連線規則

您會看到最新產生的連線規則集。如果已停用規則的話，就不會使用它們。

確認規則產生

確認您所建立的規則是否有效。

啓用連線規則記載

Firewall 將所選取的資料傳輸記載至防火牆日誌機能中。

停用連線規則記載

停止 Firewall 記載功能。

出現**連線啓動**對話框，如第52頁的圖 16 中所示。

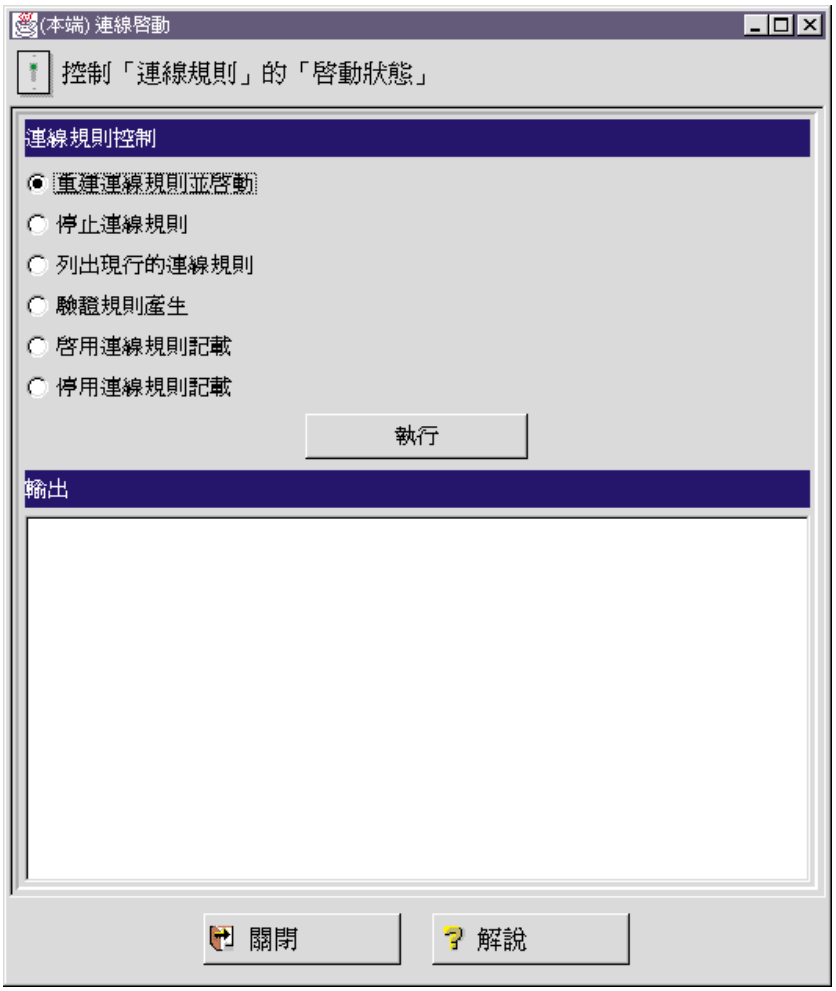

圖 16. 連線啓動

在完成選取之後，按一下**執行**。

重建與啓動連線規則時的記載輸出範例

以下是您重建與啓動連線規則時的記載輸出範例。

```
Feb 03 13:46:53 1998 mr16n18: ICA9037i: 防火牆介面將
於 Tue Feb  3 13:46:53 1998 自動更新

Feb 03 13:46:55 1998 mr16n18: ICA1032i: 過濾器規則將
於 Feb-03-1998 的 13:46:55 加以更新
```

```
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp gt  1023 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 gt  1023 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:4 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp     gt  1023 eq 25 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:5 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp/ack eq  25 gt 1023 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:6 permit 9.67.144.49 255.255.255.240
9.67.130.154 255.255.248.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:7 permit 9.67.130.154 255.255.248.
0 9.67.144.49 255.255.255.240 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:8 permit 9.67.144.49 255.255.255.240
9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:9 permit 9.67.131.250 255.255.255.255
9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:10 permit 9.67.131.250 255.255.255.
255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:11 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:12 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 secure local inbound
l=n f=y t=0 e=none a=none
.
.
.
Feb 03 13:46:58 1998 mr16n18: ICA1037i: #:100 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
all any 0 any 0 both both both l=y f=y t=0 e=none a=none
```

判斷規則狀態

IBM Firewall 規則可處於下列任何一種狀態：

1. 架構不在作用中。

   您尚未使用架構從屬站來啓動架構，或者您已停止架構。這是您第一次安裝 IBM Firewall 後，啓動系統時或停止過濾規則的架構狀態。當您第一次安裝 Firewall 時，預設過濾器會立即就位，保護您的網路以免被侵入。

   防火牆存取：

   - 預設的過濾器架構允許所有本端的入埠資料傳輸及所有的離埠資料傳輸。

2. 架構爲作用中，但有錯誤。

   您已啓動架構。可能是架構中有錯誤 (無有效規則) 或未在架構中設定任何規則。錯誤及警告會顯示在「啓動」輸出視窗中。

防火牆存取：

- 允許所有的本端入埠資料傳輸。
- 允許所有的離埠資料傳輸。

3. 架構爲使用中，而且有效。請注意：可能出現一些警告，其中最值得注意的是重覆的過濾規則。

   您已啓動使用架構從屬站資料傳輸控制區段所定義的架構。

   註: 此架構檔可以有效，但仍不含規則。 在此情形下，會採用隱含的『拒絕所有存取』規則。

   防火牆存取：

   - 由架構檔決定存取。

     由任何網路介面所接收或即將要傳送的每一個封包都要接受檢查，並根據所產生連線規則中的每一個規則來比較其內容。如果發現符合的規則，即執行該規則上的動作 (允許或拒絕存取)。
   - 如果沒有規則符合該封包，則會使用隱含的『全部拒絕』規則，拒絕存取。

第9章 服務程式範例

本章說明如何架構 Firewall，以執行某些一般作業。 列出的作業僅屬範例，但了解這些範例之後，您就可以架構防火牆來使用已提供的任何服務程式。

規劃考量

Firewall 的資料傳輸控制是根據「連線」組織而成，這些連線會定義二端點之間所容許或禁止的通信類型。 因此，您一定要根據這些端點來規劃您的連線。

如第47頁的『第8章 透過防火牆控制資料傳輸』中所描述，在 Firewall 上端點是以網路物件來代表。 如果您尚未以網路物件來代表，則應先完成第7頁的『第2章 規劃』中的網路規劃工作清單，然後建立必要的網路物件來代表您的網路。

本章中的範例是使用下列網路物件：

安全介面
Firewall 的安全介面。

非安全介面
Firewall 的非安全介面。

安全網路
可經由 Firewall 安全介面存取的位址範圍。 這可以是包含若干不同領域的網路物件群組，而每個領域都由其本身的網路物件代表。

The World
非安全性網路。

每一個所要的通信類型都必須以點對點通信的觀點來看待。在這個階段中，請考慮您的防火牆是要以 proxy 的形式來提供這些通信，或是 Firewall 要遞送這些通信。

如果防火牆充當 proxy，則防火牆將代表安全使用者執行必要工作，而非安全主電腦永遠不會知道有安全主電腦存在。如果用防火牆遞送資料，則安全主電腦及非安全主電腦會直接對談。

如果您將 Firewall 當作 proxy 使用，則您的通信端點會將防火牆併入，如第56頁的圖 17 中所示。

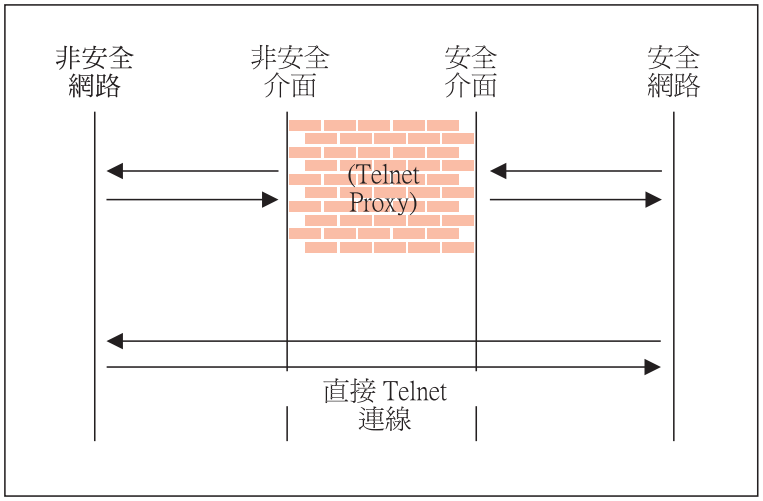

圖 17. Telnet Proxy 與直接 Telnet 連線

Telnet Proxy 範例

第一個範例是單純的離埠 telnet proxy 連線。在此範例中，安全網路上的使用者可使用防火牆 Telnet Proxy，來存取非安全網路中主電腦上的 telnet 服務程式。

如第56頁的圖 17 中所描述，此時將產生兩個連線：

1. 安全網路內的從屬站連接到防火牆的 Telnet Proxy。
2. 防火牆的 Telnet Proxy (代表安全使用者) 連接到非安全網路中的主電腦。

若要爲這個通信架構 Firewall 的資料傳輸控制，我們需要設定兩個連線：

表 1. Telnet Proxy

來源物件	目的地物件	必要的服務程式
安全網路	安全介面	Telnet Proxy 離埠 1/2
非安全介面	全球網路 (The World)	Telnet Proxy 離埠 2/2

已過濾的 Telnet 範例

用上面的範例來與簡單的過濾後的 telnet 連線做比較。在此情形下，安全端上的從屬站將直接與非安全端上的主電腦連接。

表 2. 已過濾的 Telnet

來源物件	目的地物件	必要的服務程式
安全網路	全球網路 (The World)	Telnet 直接離埠

如前所述，當安全從屬站連接到非安全主電腦時，此架構會暴露出這些從屬站的位址。

Proxy HTTP 的範例

大部份安裝的網路連線至少要容許一些安全從屬站來瀏覽 Web。 IBM Firewall 提供了預先定義的 HTTP 離埠方向服務程式 (HTTP outbound direct service)，來容許遞送的 HTTP (功能與已過濾的 Telnet 範例完全相同)。此外，Firewall 還提供 HTTP proxy。

HTTP 通訊協定不同於 Telnet，因爲它可以封裝其它通訊協定。即使是簡單的瀏覽，大部份使用者需要的不僅是 HTTP，也需要 FTP 服務程式。若要提供完整的 HTTP 功能，也應允許使用 Gopher 及 WAIS，不過這兩項的使用頻率較低。

但請注意，當使用這些額外通訊協定時，它們是包含在從屬站與 proxy 之間的 HTTP 中。因此通信會類似第57頁的圖 18 中的圖解。

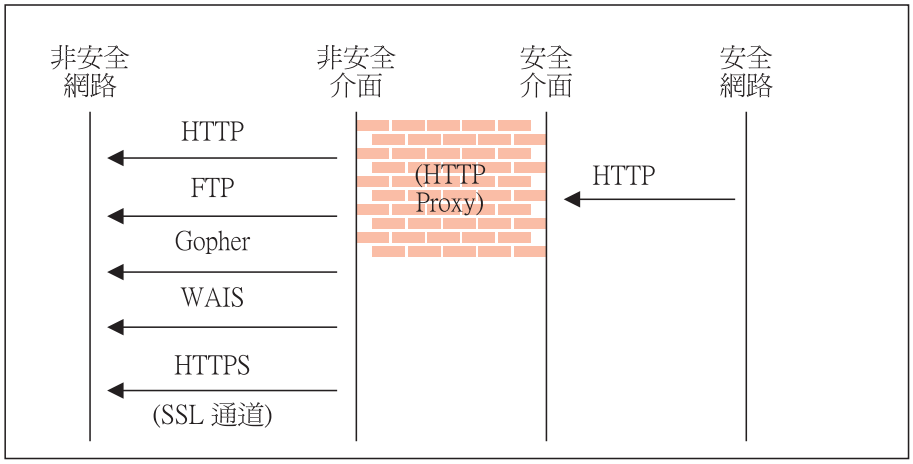

圖 18. Proxy HTTP

由於我們有兩組端點要參與作業，所以必須編寫兩個連線。

表 3. Proxy HTTP

來源物件	目的地物件	必要的服務程式
安全網路	安全介面	HTTP proxy 離埠 1/2
非安全介面	全球網路 (The World)	選取自... • HTTP proxy 離埠 2/2 • FTP proxy 離埠 2/2 • Gopher proxy 離埠 2/2 • WAIS proxy 離埠 2/2 • HTTPS proxy 離埠 2/2

關於 HTTP Proxy 的詳細資訊，請參閱第91頁的『第13章 架構 proxy 伺服器』。

Socks 的範例

Socks 會有類似 HTTP proxy 的問題，因爲 socks 常駐程式會處理許多不同的通訊協定，並且會將它們封裝到 Firewall 與從屬站之間的單一資料流中。 Socks 比 HTTP proxy 更有彈性，因爲它可以接受任何 TCP 或 UDP 導向的通訊協定，而且 Firewall 可以在過濾器外獨立架構，以進一步控制通信。

由於此項新增的彈性，所以架構 socks 除了以 HTTP proxy 中示範的連線之外，還需要第三個連線。兩個基本連線容許封包來回流動至 Firewall；而要有第三個連線才能在 socks 常駐程式收到封包時，通知它 proxy 要求。

表 4. Socks

來源物件	目的地物件	必要的服務程式
安全網路	安全介面	Socks 1/2
非安全介面	全球網路 (The World)	選取自... • HTTP proxy 離埠 2/2 • FTP proxy 離埠 2/2 • Telnet proxy 離埠 2/2 (您要提供支援的任何 2/2 proxy 服務程式)

表 4. Socks (繼續)

來源物件	目的地物件	必要的服務程式
安全網路	全球網路 (The World)	在「Socks 架構」視窗中，在下列選項中選取... • 允許 socks 化的 HTTP • 允許 socks 化的 FTP • 允許 socks 化的 Telnet

當然，您安全網路內的從屬站必須 socks 化，且必須架構爲以防火牆當作 socks 伺服器使用。

關於 Socks 的詳細資訊，請參閱第73頁的『第11章 架構 Socks 伺服器』。

DNS 提示

如果您未提供 DNS 解決方案，就很難有效率地進行通信。 請參閱第31頁的『第6章 處理領域名稱服務程式』，以取得有關架構 DNS 的明細。而且請務必記得啓用「安全性策略」中的「允許 DNS 查詢」。

非安全 Socks 從屬站的提示

「安全性策略」畫面包含**拒絕 Socks 到非安全介面**的勾選框。這個服務程式會拒絕從任何非安全介面遞送到您 socks 常駐程式的任何封包，這樣可使您的防火牆更加安全。

如果您要讓從屬站從非安全性網路進入您的網路，您*絕不能*選取此勾選框。

第10章 自行設定資料傳輸控制

本章協助您定義過濾規則及服務程式。 服務程式是一規則集合或一組指令集，可透過 Firewall 來允許或拒絕特定的資料傳輸類型，例如 telnet 階段作業。 您可以使用規則模版來建立新規則，以新增至服務程式。 您也可以刪除服務程式。 Socks 服務程式可引用至 socks 化的連線上。

IBM Firewall 附有預先載入的預設服務程式集。您可以修改任何預先定義的服務程式，以符合您的特定需求，或者建立新的服務程式。

使用架構從屬站建立規則模版

此程序可用來將新規則加入至可用規則模版的列示中。

1. 在架構從屬站導覽樹狀結構中選取「資料傳輸控制」，然後按兩下檔案資料夾圖記。選取**連線模版**後，再選**規則**。
2. 在**規則列示**對框話上，按兩下**新增**。

   「IBM Firewall」會顯示如第62頁的圖 19 所示的**新增 IP 規則**對話框，您可以用它來定義新的規則。

圖 19. 新增 IP 規則

3. 輸入「規則名稱」。
4. 輸入「規則說明」。本欄位是選用性的。
5. 按一下動作箭號，然後選擇允許或拒絕存取「防火牆」。
6. 按一下通訊協定箭號，然後從下列列示中選取：

all 任何通訊協定皆符合此規則。

tcp 封包通訊協定必須是傳輸控制通訊協定 (TCP)，才能符合此規則。

tcp/ack
封包通訊協定必須是經認可的 TCP，才能符合此規則。

udp 封包通訊協定必須是使用者封包通訊協定 (UDP)，才能符合此規則。

icmp 封包通訊協定必須是 Internet 控制訊息通訊協定 (ICMP)，才能符合此規則。

ospf 封包通訊協定必須是「開啓最短路徑的第一個通訊協定 (ospf)」，才能符合此規則。當 ospf 指定爲通訊協定時，則 ospf 記錄類型值會使用來源埠作業和來源埠值。ospf 類型上亦可進行過濾。您可以指定類型值 **any**，而目的埠欄位必須指定爲 **any 0**，其它任何值即予以忽略。

ipip 封包通訊協定必須是 IP-in-IP 通訊協定 (IPIP)，才能符合此規則。 指定 IPIP 時，連接埠欄位必須指定爲 **any 0**。

esp 封包通訊協定必須是虛擬專用網路用來傳送封裝 IP 封包的封裝安全通訊協定，才能符合此規則。

ah 鑑證表頭通訊協定係指虛擬專用網路用來傳送 IP 封包 (具有相關的鑑證記號) 的封包通訊協定。

7. 數值通訊協定可讓您利用其十進位值 (根據 RFC-1700 規定) 來指定通訊協定，有效值範圍爲 1 至 252。請注意：使用本選項時，此規則使用的連接埠欄位必須指定爲 0 (表示任何連接埠)。請參閱 RFC-1700，以取得所有通訊協定的列示。或者，您也可以直接用瀏覽器來存取 Internet Assigned Numbers Authority (IANA)。
8. 運算與埠號運算元是同時並用。來源及邏輯運算陳述封包所用的埠號 (目的地或來源) 與來源埠號和目的地埠號運算元之間的關聯。例如，如果封包目的埠爲埠 20，而且目的地運算和目的埠號都爲 『ge 15』，所以封包相符。(20 大於或等於 15)。

   如果您使用值爲 **any** 的來源或目的地運算，則過濾器會忽略埠號；任何連接埠都將符合。在此情形下，您不能變更埠號。

   以 ICMP 通訊協定而言，則不指定來源埠，而指定 ICMP 類型，且不指定目的地埠而指定 ICMP 碼。所指定的邏輯運算子會引用至該類型或字碼，若是埠，則 any 運算子表示任何類型及/或字碼值皆符合規則。在此情形下，您不能變更埠號。

   運算值爲：

   - 任何
   - 等於
   - 不等於
   - 小於
   - 大於
   - 小於或等於
   - 大於或等於

以下爲一些需要保護的重要埠。埠號值必須在 1 到 65536 的範圍內。

連接埠 **用途**

20 FTP 資料

21 FTP 控制

23 Telnet

25 郵件

53 領域名稱伺服器

70 Gopher

80 HTTP

111 RPC

161 SNMP

1080 socks

下面列出 ICMP 類型和字碼：

類型 **字碼和說明**

0 0 - Ping 回應

8 0 - Ping 要求

3 1 - 無法存取主電腦

3 3 - 無法存取連接埠

5 1 - 主電腦重新導向

9. 按一下**介面**箭號來選取介面 (配接卡) 類型。

   兩者 用於安全或非安全性介面上進入或送出的封包

   安全 用於安全性介面上進入或送出的封包

   非安全性
   用於非安全介面上進入或送出的封包

   特定 選取介面時，與介面名稱欄位一起使用 (如果您已指定名稱給介面)。

10. 如果您選擇特定介面類型，特定介面的名稱即出現在「名稱」欄位中。
11. 按一下所要的遞送路徑：

    兩者 適用所有的資料傳輸。

    本端 意指封包是在防火牆主電腦本端範圍內。這表示：

    - 所傳入的區域封包爲由介面接收且要傳送到此防火牆主電腦的封包；這些封包不會傳送到其他主電腦上，其目的地在本端。

- 送出的封包從該介面傳輸，但是由防火牆主電腦所發出。其來源爲本端。

遞送 意指封包是由防火牆主電腦傳送，這表示：

- 進入的區域封包是由介面接收且傳遞到其他主電腦的封包；封包不會保留在 Firewall 上。其目的地在遠端。
- 送出的封包是從介面傳輸，其來源是其他主電腦發起傳出。其來源在遠端。

12. 按一下所要的方向：

    兩者 所選定之介面所傳送或接收的封包。

    入埠 從網路傳送到所選定之介面的封包

    離埠 從所選定之介面傳送到網路上的封包

13. 如果您在「日誌控制」欄位選擇「是」，則符合該規則的每一個封包都會以優先順序層次 Error 記錄在防火牆日誌中。如果未指定這個參數，則預設值爲「否」。
14. 按一下**片段控制**箭號來選擇所要的片段控制。 爲了使 IP 封包資訊符合規則片段控制規格，此控制解譯如下：

    是 該規則將符合片段表頭、片段及非片段。若是片段，連接埠資訊將予以忽略並認定爲符合。

    唯一 僅片段和片段表頭可以符合。若是片段表頭，連接埠資訊必須符合；若是片段，連接埠資訊將予以忽略。

    否 僅非片段可以符合。片表頭和區片被此參數排除在外。

    表頭 僅非片段和片段表頭可以符合。片段被這個參數排除在外。

    如果未指定這個參數，則「允許」規則及「拒絕」規則的預設值皆爲「是」。

    註: 不管這個控制的設定為何，偏置為 1 的 IP 片段都會被捨棄。這個動作會消除以封包片段來覆蓋 TCP 表頭旗號的已知攻擊。

爲了使封包表頭符合已定義的 IP 規則，封包資訊必須符合編碼規則中指定的所有參數。若是封包片段，除了埠資訊以外，所有參數都可用來決定是否符合。

如果這些封包片段不被先前有「是」或「唯一」編碼的規則所允許，則封包片段將爲永遠附加在規則檔末端的最後一個規則所拒絕。

變更 IP 規則架構項目

欲修改您已建立的 IP 規則，請：

1. 請連按兩下**規則列示**中的現存規則，即出現**修改 IP 規則架構**對話框。
2. 修改適當的欄位，如第61頁的『第10章 自行設定資料傳輸控制』中所示，然後按一下 **OK** 來引用所作的變更。

刪除規則架構項目

欲刪除規則，請從**規則列示**中選取一規則，然後按一下**刪除**。

預先定義的服務程式

IBM Firewall 附有預先載入的預設服務程式集。 服務程式是一規則集合或一組指令集，可透過 Firewall 來允許或拒絕特定的資料傳輸類型，例如 telnet 階段作業。 您可以使用規則模版來建立新規則，以新增至服務程式。

預先載入的預設服務程式爲：

所有非安全
拒絕所有透過非安全介面的資料傳輸

全部允許
允許所有資料傳輸 (僅限用於偵錯)

全部允許，以單向方式
允許所有資料傳輸 (僅限用於偵錯)

所有安全
拒絕所有透過安全介面的資料傳輸 (以防止安全性違規)

全部關閉
拒絕所有封包 (關機或偵錯)

反詐騙 拒絕來源位址爲安全性的非安全性封包入埠

廣播 拒絕將訊息廣播到非安全介面

非安全性的架構從屬站
允許您從非安全性網路使用架構從屬站

架構從屬站安全
允許您從安全性網路使用架構從屬站

CU-SeeMe
CU-SeeMe Video 位於預設埠 7649 及 7648

DNS 查詢
(安全性策略) 允許 DNS 查詢

DNS 轉送
允許 DNS 區域轉送 (針對備用名稱伺服器)

領域控制器鑑證
允許您針對使用者鑑證使用「領域控制器」

FTP proxy 入埠 1/2
允許 FTP 從非安全網路入埠到「防火牆」

FTP proxy 入埠 2/2
允許 FTP 從「防火牆」入埠到安全網路

FTP proxy 離埠 1/2
允許 FTP 從安全網路離埠到「防火牆」

FTP proxy 離埠 2/2
允許 FTP 從「防火牆」離埠到非安全網路

Gopher proxy 入埠 2/2
允許 gopher 自 Firewall 離埠至安全網路

Gopher proxy 離埠 2/2
允許 gopher 從「防火牆」離埠到非安全網路

HTTP 拒絕非安全性
拒絕 HTTP 到非安全介面

HTTP 直接離埠
允許 HTTP 直接從安全網路離開至非安全網路

HTTP proxy 入埠 2/2
允許 HTTP 從「防火牆」入埠到安全網路

HTTP proxy 離埠 1/2
允許 HTTP (埠 8080) 從安全網路離埠到 Firewall

HTTP proxy 離埠 2/2
允許 HTTP 從「防火牆」離埠到非安全網路

HTTPS 直接離埠
允許 HTTPS (SSL) 自安全網路離開至非安全網路

HTTPS proxy 離埠 2/2
允許 HTTPS (SSL 通道) 從 Firewall 離埠到非安全網路

IDENTD
允許有 Socks 通訊協定的使用者 ID

郵件 (安全性策略) 允許「郵件」資料傳輸通過 Firewall

NetBT 名稱服務程式廣播
允許 NetBIOS over TCP/IP 名稱服務程式廣播

Ping 允許 Ping 離開安全網路至任何地方

SDI 鑑證
允許連線到安全網路中的 SecurID ACE 伺服器

Socks 1/2
允許使用從安全網路到 Firewall 的 Socks

Socks 拒絕非安全
拒絕來自非安全配接卡的 Socks

Socks 入埠 1/2
允許使用從非安全性網路到 Firewall 的 Socks

Telnet 直接離埠
允許 Telnet 從安全網路離埠到非安全網路

Telnet proxy 入埠 1/2
允許 Telnet 從非安全網路入埠到 Firewall

Telnet proxy 入埠 2/2
允許 Telnet 從 Firewall 入埠到安全網路

Telnet proxy 離埠 1/2
允許 Telnet 從安全網路離埠到「防火牆」

Telnet proxy 離埠 2/2
允許 Telnet 從「防火牆」離埠到非安全網路

VDOLIVE 直接入埠
允許非安全從屬站入埠到安全伺服器

請注意，使用者必須架構個別使用者 (player) 的性質，便於僅使用 UDP 埠 7001。

VDOLIVE 直接離埠
允許安全從屬站離埠到非安全伺服器

WAIS proxy 入埠 2/2
允許 WAIS (z39.50) 從 Firewall 離埠到安全網路

WAIS proxy 離埠 2/2
允許 WAIS (z39.50) 從「防火牆」離埠到安全網路

定義服務程式

定義規則之後，您必須將規則新增到服務程式中。從架構從屬站導覽樹狀結構中選取「資料傳輸控制」，然後按兩下「連線模版」，再選取「服務程式」，「服務程式列示」對話框即會出現。按兩下「新增」可取得「新增服務程式」對話框，如第69頁的圖 20 中所示。

圖 20. 新增服務程式

使用架構從屬站來建立服務程式

1. 輸入服務程式名稱。
2. 輸入說明。
3. **置換日誌控制**欄位提供一種方法，來置換已爲這個服務程式選取之規則模版中的日誌控制設定。例如，如果您併入一組規則模版其日誌控制一般設成「否」，則您可特別爲此服務程式，將該設定置換成「是」。此置換設定將會影響服務程式中的所有規則。請在**置換日誌控制**欄位中，輸入下列選項之一：
   - 不置換 - 置換已關閉，規則本身的設定仍然適用
   - 是 - 當服務程式中有任何規則符合時，寫入日誌記錄

- 否 - 當服務程式中有任何規則符合時，不寫入日誌記錄

當針對過濾規則寫入日誌記錄時，日誌記錄中顯示的值爲來自 IP 封包的實際值。符合過濾規則的記錄，可提供關於 Firewall 所看到之 IP 封包內容的重要資訊，例如實際通訊協定和埠號。

4. **置換片段 控制**欄位提供一種方法，來置換已爲這個服務程式選取之規則模版中的「片段控制」設定。例如，如果您併入一組規則模版其「片段控制」一般設成「否」，則您可特別爲此服務程式，將這個設定置換成「是」。此置換設定將會影響服務程式中的所有規則。請在「置換片段控制」欄位中，輸入下列之一：
   - 不置換 - 置換已關閉，規則本身的設定仍然適用
   - 是 - 符合任何 IP 封包，例如，非片段、片段表頭及不含表頭的片段
   - 否 - 僅符合非片段封包，不符合片段表頭或不含表頭的片段
   - 唯一 - 僅符合片段表頭及不含表頭的片段，不符合非片段
   - 表頭 - 僅符合非片段及片段表頭，不符合不含表頭的片段
5. 時間控制項可讓您連結時間範圍與每一個服務程式，因此，這個服務程式僅在指定的期間內有效。如果沒有爲服務程式指定時間，則該服務程式在所有時間都是有效的。

   由一天中時間控制

   如果您要根據當天的起始及結束時間，來啓動或停止這個服務程式，請選取此選項。 使用 24 小時格式。若未啓用此欄位，則「一天中時間」欄位會在一天 24 個小時中起作用。

   由日期控制

   如果您要根據以一週或一年日期排定的時程來啓動或停止服務程式，請選取此選項。請注意：服務程式是啓動或停止，視「時間控制動作」欄位中的值而定。

   時間控制動作

   如果您要服務程式在指定時間內啓動，請選擇**在指定時間內啓動服務程式**。此服務程式在這些指定時間之外會停止。

   如果您要服務程式在指定時間內停止，請選擇**在指定時間內停止服務程式**，此服務程式在這些指定時間之外會啓動。
6. 按一下**選取**來選擇構成此服務程式的規則。
7. 您可使用「流程」切換，來決定在將「連線」的「來源」及「目的地」值寫入「規則基本」檔時，如何將這些值指定給過濾器。

   ---> 「由左向右」表示「連線」的「來源」與「目的地」被寫入「規則基本檔」時，會直接寫入該規則。

   <--- 「由右向左」表示「連線」的「來源」與「目的地」被寫入「規則基本檔」時，會倒轉。

8. 當收到封包時，「IBM Firewall」會將封包內的資訊與「規則架構檔」中的規則從檔案頂端開始比較。 在發現第一個符合的資訊時即停止比較，並執行規則內所含的動作。

   在新增一串規則到服務程式後，您可以變更這些規則的順序。 從**服務程式物件**列示中選取規則，然後按一下**往上移**或**往下移** 按鈕來將規則重新定位。或者，您可以按一下**移除**來移除規則，架構從屬站會顯示復新的規則列示，按一下 **OK** 來儲存您的變更。

第11章 架構 Socks 伺服器

Socks 是電路閘道的 Internet 標準。 如果您的應用程式是使用 TCP (像是 Web 瀏覽器、FTP 或 Telnet 應用程式)，則您可以使用 Socks 伺服器來轉換位址。隱藏內部 IP 位址時，Socks 可以幫助您存取 Internet。

若是從安全從屬站到非安全伺服器的離埠要求，則 Socks 伺服器的作用與 Proxy 伺服器相同：是要中斷 Firewall 上的階段作業，並在保護內部網路定址及結構的同時，提供使用者可存取外部、非安全網路的安全門。 Socks 伺服器對使用者的優點是更容易使用，且只需用很少的額外管理工作。

Socks 伺服器可攔截所有通過您網路和 Internet 之間的離埠 TCP 要求。 Socks 伺服器提供遠端應用程式介面，因此從屬站程式在安全領域中執行的功能，都會在防火牆工作站上利用管道通過安全伺服器，而隱藏從屬站的 IP 位址。與 Socks 規則連結的過濾器會控制存取權。

Socks 伺服器類似 proxy 伺服器。但事實上 Proxy 伺服器是在 Firewall 上執行 TCP/IP 功能，而 Socks 伺服器只是識別使用者，並使該功能經由 Firewall 重新導向。實際的 TCP/IP 功能是在從屬站工作站上執行，而非防火牆。這樣可省去 Firewall 的處理程序。安全網路中的使用者可使用許多支援 Socks 標準的 TCP/IP 產品。 圖 21 說明 Socks 伺服器如何截取來自安全網路從屬站的 HTTP 要求。

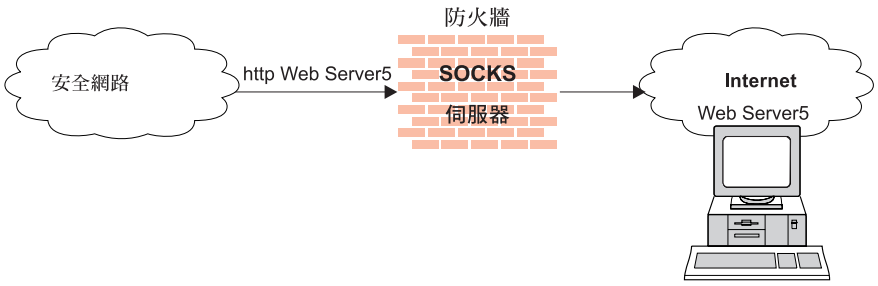

圖 21. Socks 伺服器

Socks 伺服器能有效地對外界隱藏的內部 IP 位址。

IBM Firewall 提供「Socks 通訊協定第 5 版」，可讓安全網路中的從屬站在存取非安全性網路中的應用程式之前，能夠通過鑑證階段。同時，它也提供聲音及影像通訊協定給經過鑑證的一般 proxy 及一些串流的 proxy。

Socks 常駐程式會在系統啓動時，以「Windows NT 服務程式」的型態自動啓動。此外，所提供的 Watch 代理程式 (Watch Agent) 可監督伺服器。您可以人工方式啓動 Watch 代理程式。

IBM Firewall 提供一簡單的移轉路徑，它是由三種鑑證設定檔組合而成，所以當 Socks 從屬站導入「Socks 通訊協定第 5 版」從屬站時，客戶還是可以繼續使用已安裝的「Socks 通訊協定第 4 版」從屬站。

1. 無論使用「Socks 通訊協定第 4 版」或「Socks 通訊協定第 5 版」的從屬站來連線，最寬大的設定檔都不會啓用離埠鑑證來認可任何使用者。在這種情況之下，會拒絕入埠連線。
2. 移轉設定檔可讓「Socks 通訊協定第 4 版」使用者通過而不需鑑證，但是會要求「Socks 通訊協定第 5 版」的使用者進行鑑證。入埠「Socks 通訊協定第 4 版」連線會遭拒絕；而入埠「Socks 通訊協定第 5 版」連線需經鑑證。此爲預設的設定檔。
3. 最安全的設定檔會要求所有使用者都使用「Socks 通訊協定第 5 版」從屬站，並需提供有效的鑑證資料。

當您安裝 Firewall 時，就已經啓用了 Socks 伺服器，但這個 Socks 架構檔中並沒有規則。若要 socks 從屬站使用「Socks 伺服器」，您必須使用架構從屬站來架構 socks。 關於如何設定 Socks 服務程式的範例，請參閱第58頁的『Socks 的範例』。

Socks 通訊協定第 5 版伺服器所支援的通訊協定

Socks 通訊協定第 5 版伺服器支援下列 TCP 及 UDP 通訊協定及其他：

- Archie
- Finger
- FTP
- Gopher
- HTTP
- HTTP Proxy
- News
- SNMP
- Telnet
- TFTP
- RealAudio
- RealPlayer
- Whois
- X-Windows

此外，也支援大部份的 E-mail 從屬站。這些通訊協定的支援端視它們的實際執行狀況而定。

使用架構從屬站來架構 Socks 伺服器

Socks 模版是控制 Socks 伺服器安全性的規則。 「Socks 模版」可讓您自行設定、新增、複製或刪除現存的「Socks 模版」。這些 Socks 模版可依序使用在防火牆的「連線」定義中，使用方式與「規則模版」相同。

新增 Socks 規則

欲使用由架構從屬站所提供的 Socks 模版來將規則新增至 Socks 架構檔中，請從架構從屬站導覽樹狀結構中，選取「資料傳輸控制」。按兩下檔案資料夾圖示來展開檢視畫面。選取「連線模版」。 按兩下檔案資料夾圖示來展開檢視畫面。選取 **Socks**， **Socks** 對話框即會出現。

1. 連按兩下**新增**來增加一個新的 socks 模版。

   即出現**新增 Socks 規則**對話框，如第75頁的圖 22 所示。

圖 22. 新增 Socks 規則

2. 請在**模版名稱**欄位中，輸入 socks 項目的名稱。這個名稱必須是唯一的，且不應包含直線符號 (|)、單引號 (') 字元或雙引號 (″) 字元，因爲這些字元爲檔案定界符號。若您使用這些字元，則會產生不可靠的資料。
3. 填入說明。
4. 按一下「動作」箭號，然後選擇允許或拒絕由來源至目的地之間的存取。

   當資料包進入 socks 伺服器時，伺服器會以資料包規格與架構檔中每一個規則進行比較，從第一個規則開始直到找到完全符合的規則爲止， 然後停止搜尋，並在該規則上執行相關動作 (允許或拒絕存取)。如果找不到符合的規則，存取會自動被拒絕。
5. 您可以在**使用者列示**欄位中，輸入一個使用者 ID 或一個列示的使用者 ID。如果您輸入一列使用者，請以逗點隔開其中的項目。請勿在使用者列示中，使用空格、欄標、直線符號 (|) 或雙引號 (″)。
   - 使用者列示最多爲 396 個字元。
   - 使用者 ID 必須是要求主電腦上的使用者 ID，而非目的地主電腦或 Socks 伺服器主電腦上的使用者 ID。
   - 使用者 ID 可由 1 至 8 個字元組成，包括：
     - a 到 z
     - A 到 Z
     - 0 到 9
     - _ (底線)
6. 使用者 ID 不可包含下列字元：直線符號 (|) 或雙引號字元 (″)。
7. 如果使用檔名，則必須是完整檔名 (使用前置符號 ″/″ 來避免檔名被解譯爲使用者 ID)。每一個檔案可包含一份使用者 ID 列示，每一行有一個以上的使用者 ID，以逗點隔開，並可選擇納入以 # 字元定界的備註，也支援完整備註行 - 以 # 字元開頭的行。檔案中每一行最長爲 1023 個字元，且必須以 ″newline″ 字元終止。
8. 在**作業**欄位中，輸入埠號上要執行的邏輯作業：

   eq 等於

   neq 不等於

   lt 小於

   gt 大於

   le 小於或等於

   ge 大於或等於

   當與「埠號」一起使用時，邏輯運算會建立一種必須符合的關聯。例如，如果您輸入「作業 gt」及「埠號 23」，則該埠號必須大於 23 才能呼叫此規則。

9. 在**埠號**欄位中，輸入埠號。「作業」與「埠號」一起使用，來建立一種必須符合的關聯。例如，如果您輸入「作業 gt」及「埠號 23」，則該埠號必須大於 23 才能呼叫此規則。如果省略作業及埠號的話，則規則適用於所有的目的埠號。

您可使用此**新增 Socks 規則**對話框，根據 IP 位址來允許或拒絕防火牆對網路主電腦的存取。

修改 Socks 規則

1. 連按兩下 **Socks** 對話框上的項目，

   即出現**修改 Socks 規則**對話框。
2. 變更適當的欄位，如第75頁的『新增 Socks 規則』中所述，然後按一下 **OK**。

刪除 Socks 規則

從 **Socks** 對話框中選取項目，然後按一下**刪除**。 此時系統會詢問您，是否眞的要刪除這個 Socks 規則，按一下 **OK** 即刪除該規則。

啓動連線規則

如同使用過濾規則一樣，您必須啓動 socks 規則。 按一下架構從屬站導覽樹狀結構中的**連線啓動**，選取**重建連線規則及啓動**，然後按一下**執行**。

Firewall 將一些規則從 socks 架構檔複製到防火牆規則，然後啓動這些規則。 啓動這些規則時，新規則即記錄在防火牆日誌檔中。

Socks 的記載輸出範例

以下是 Socks 的記載輸出範例。

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Sockd 伺服器啓動
Feb 03 13:47:31 1998 mr16n18: ICA3010i: 階段作業啓動
Feb 03 13:47:31 1998 mr16n18: ICA3011i: 階段作業啓動
Feb 03 13:49:15 1998 mr16n18: ICA3007i: 太多緒
Feb 03 13:58:31 1998 mr16n18: ICA3015i: 階段作業終止
```

使用 Socks 伺服器時的從屬站考量

大部份 Web 瀏覽器都已 Socks 化，您可以從大多數平台上，取得 Socks 化的堆疊。其他 TCP/IP 應用程式的 Socks 化從屬站可從許多來源取得。 Socks 所執行之特定從屬站的相關資訊，請參閱從屬站文件說明。詳細相關資訊，請參閱：

http://www.raleigh.ibm.com/sng/sng-socks.html

http://www.socks.nec.com

Socks 伺服器的連結

「Socks 伺服器的連結」功能可將一個 Socks 伺服器放在另一個 Socks 伺服器後面，但是裡面的 Socks 伺服器仍可越過最外面的 Socks 伺服器來存取網路。 (您也可以把它當作將 Socks 伺服器 Socks 化。) 這是一種很有用的內部網路計劃。

若要用 Socks 伺服器來設定「Socks 與伺服器的連結」，請編輯 `socks5.header.cfg` 檔案。此檔位於「防火牆」的 `config` 子目錄中。新增下列動作：

- *no proxy* 指引 - 表示「防火牆」直接存取的子網路
- *socks4* 指引 - 表示可透過「SOCKS 通訊協定第 4 版伺服器」來存取的子網路
- *socks5* 指引 - 表示可透過「SOCKS 通訊協定第 5 版伺服器」來存取的子網路

以下面這個網路爲例。「研究」部門在自己的防火牆後面有一個小的專用網路：*q.private.com*。「研究」部門的子網路爲 10.007.007.0/255.255.255.0。公司的專用網路 *private.com* 包含整個 10.0.0.0/255.0.0.0 網路。而公司的「SOCKS 通訊協定第 4 版伺服器」*socks.private.com* 提供 Internet 的存取權。

在「研究」部門的 Socks 伺服器 *socks.q.private.com* 上，將以下二行新增至 `socks5.header.cfg` 中。

```
no proxy 10.0.0.0/255.0.0.0 - - -
socks4      0/0   - socks.private.com 1080
```

最後，加入「資料傳輸控制」連線，讓 *socks.q.private.com* 與 *socks.private.com* 通信。較常用的「服務程式」可能就已經完成這個程序了。新增一「連線」：來源爲 *q.private.com*「防火牆」的非安全介面，目的地爲 *socks.private.com*，並且包含 *Socks Proxy-Chaining* 服務程式。然後重新啓動您的「資料傳輸控制」規則。

第12章 管理防火牆的使用者

本章說明如何以「IBM Firewall」來執行每日管理作業，包含：

- 將使用者新增至 IBM Firewall，以便讓使用者存取受保護網路之外的主電腦
- 變更存取防火牆的使用者之屬性
- 刪除不再需要在您網路外進行存取作業的使用者

請勿直接編輯架構檔；如果您直接編輯，則您的 IBM Firewall 使用者屬性將無法正確設定。使用架構從屬站對話框或命令行來執行所有的「IBM Firewall」管理作業。

將使用者新增至 IBM Firewall

IBM Firewall 定義了三種類型的使用者，並將有關它們的資訊儲存在兩個不同的使用者資料庫中。

使用者類型

IBM Firewall 將使用者分爲三大種類：

Proxy 使用者

在法人組織的網路中，利用防火牆服務程式 (如 HTTP proxy 服務程式) 來存取 Internet 上的 Web 站台。 Proxy 使用者可以透過防火牆來使用服務程式，但是沒有防火牆機器的存取權，也不能執行本端登入至 Firewall 機器。

防火牆管理者

可以使用 Firewall proxy 服務程式，而且可以使用架構從屬站，及從遠端主電腦登入 Firewall 來架構 Firewall。 防火牆管理者和 proxy 使用者一樣，都不能執行本端登入至 Firewall 機器。

防火牆管理者可以建立及修改 proxy 使用者的定義，但是卻無法建立或修改其他防火牆管理者的定義。

主要防火牆管理者

具有與防火牆管理者相同的能力。但他們可以執行本端登入至 Firewall 機器。 主要防火牆管理者可以建立及修改其他防火牆管理者的定義。

資料庫類型

共有兩種資料庫類型。

防火牆使用者資料庫

包含每一個 proxy 使用者及管理者的防火牆相關屬性。包含使用者的防火牆通行碼及通行碼規則等屬性，以及應該使用何種鑑證方法來鑑證每一個服務程式的使用者。

如果 proxy 使用者沒有定義在防火牆使用者資料庫中，而該使用者試著使用防火牆 proxy 服務程式的話，就會使用預設的使用者記錄 `fwdfusr` 來定義屬性及鑑證計劃以用來驗證該使用者。

主要防火牆使用者不能定義在防火牆使用者管理者中。使用預設的防火牆管理者記錄 `fwdfadm` 來指定管理者的屬性。

防火牆管理者和 proxy 使用者一樣，如果他們在 Windows NT 使用者資料庫中也有定義的話，當使用者要求任何必須用 NT 登入通行碼來鑑證的服務程式時，就會使用該使用者的 NT 登入通行碼。

Windows NT 使用者資料庫

包含使用者的 NT 登入通行碼。一般而言， proxy 使用者可以不必定義在 NT 使用者資料庫中，除非他們要使用他們的 NT 登入通行碼來進行鑑證。

如果要使用其他鑑證方法來鑑證 proxy 使用者的話，則他們可以不必定義在 Windows NT 使用者資料庫中。

主要防火牆管理者與 Windows NT 使用者相似，都一樣是 NT 管理者群組的成員，因此必須定義在 Windows NT 資料庫中。

使用「架構從屬站」來新增使用者

將使用者新增至 IBM Firewall，讓使用者存取外部網路。

1. 在架構從屬站導覽樹狀結構中，選取「使用者」。**使用者管理**對話框即會出現。
2. 選取**使用者管理**對話框中的**新增**，然後按一下**開啓**。 即出現**新增使用者**對話框，如第81頁的圖 23 所示。

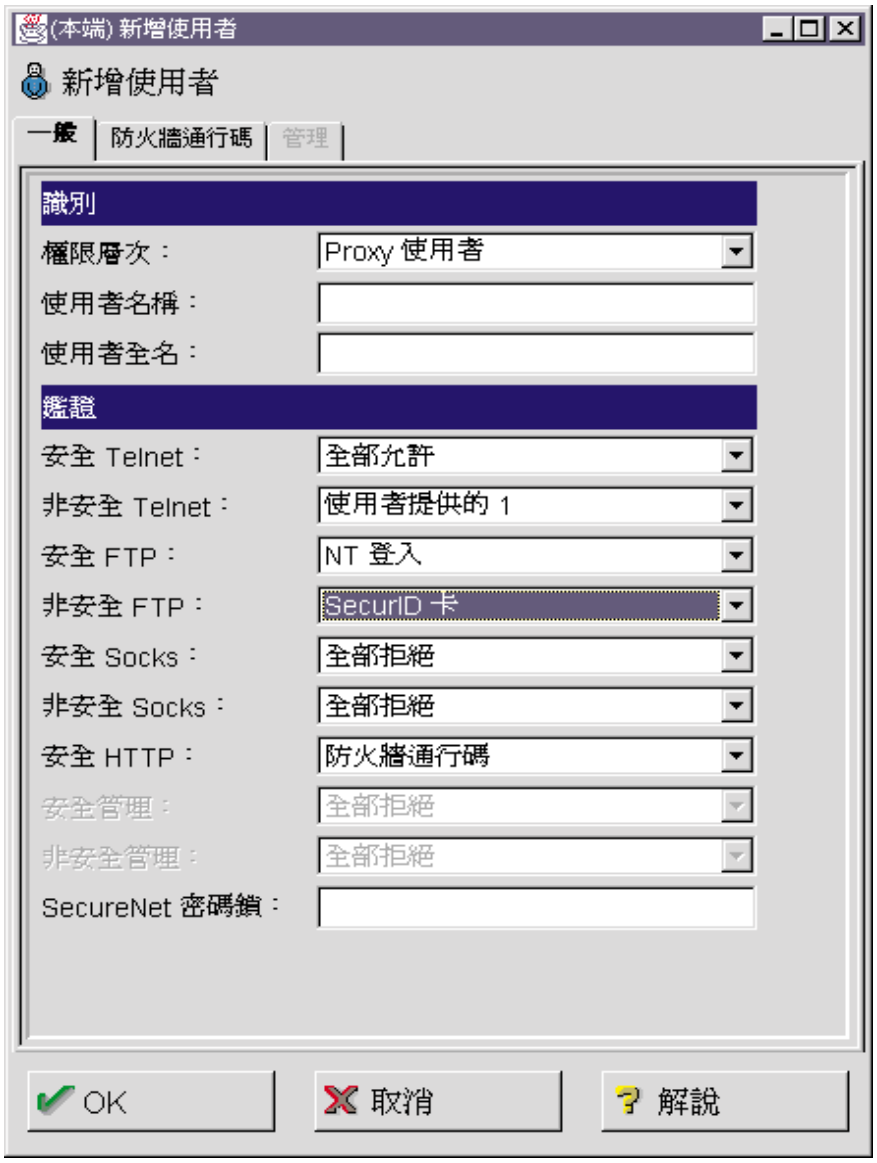

圖 23. 新增使用者

3. 提供下列資訊：

   權限層次

   爲這個使用者指定權限層次。按一下**權限層次**箭號來選取使用者類型。

Socks/Proxy 使用者

所定義的使用者將用於 Socks 伺服器的存取與 proxy 的存取。此使用者不具管理權限。此爲預設值。

防火牆管理者

管理者擁有使用者的所有屬性，而且可以登入 Firewall 並執行管理作業。管理者還擁有其他屬性，可以定義該管理者所能執行的管理功能。防火牆管理者可以建立防火牆使用者，但是無法建立其他防火牆管理者。防火牆管理者不能以區域登入的方式來登入 Firewall 機器。他們必須從遠端機器來存取架構伺服器。

主要防火牆管理者

主要防火牆管理者可以區域登入的方式來登入 Firewall 機器。他們擁有完整的存取權，可以存取所有管理功能。而且也可以建立其他「防火牆管理者」，但不能建立其他「主要防火牆管理者」。

在 NT 資料庫中建立使用者，並使該使用者成爲 NT 管理者群組的一員，則該使用者即可定義爲「主要防火牆管理者」。修改 `fwdfadm` 記錄，來定義主要防火牆管理者的屬性。

使用者名稱

爲這個使用者指定名稱。這是使用者在IBM Firewall上，用來登入 telnet 或 FTP 伺服器的使用者名稱，而並不一定是使用者的 TCP/IP 使用者名稱或主電腦名稱，但這些名稱可以是相同的。

使用者名稱可以由 1 至 20 個字元組成，包括：

a 到 z

A 到 Z

0 到 9

_ (底線)

使用者名稱並不會區分大小寫。

Firewall 中附有兩個預先安裝的使用者：

a. 預設使用者或 `fwdfuser`。若使用者沒有定義在防火牆資料庫中，就會使用 `fwdfuser` 來決定使用者的防火牆屬性，例如要用何種鑑證方法來鑑證該使用者。

   在安裝時，若建立 `fwdfuser`，所有鑑證方法都會設定爲「全部拒絕」。`fwdfuser` 的許可權可控制，防火牆如何處理未定義的使用者名稱。

   管理者可使用架構從屬站或命令行來檢視 `fwdfuser` 或變更已指定的鑑證方法。不過，您不能刪除 `fwdfuser`，且必須永遠將它保存在防火牆上。此外，對 `fwdfuser` 而言，防火牆通行碼及 SNK 都是無效的鑑證類型。相關資訊，請參閱 *IBM eNetwork Firewall 參考手冊*。

b. 預設的「主要防火牆管理者」fwdfadm 可定義所有主要防火牆管理者的防火牆屬性。 因爲「主要防火牆管理者」在防火牆資料庫中沒有他們自己的使用者記錄，所以就會用這個記錄來定義要用來鑑證「主要防火牆管理者」的鑑證方法。

   安裝時，fwdfadm 的所有鑑證方法都會設定爲全*部拒絕*，但安全及非安全管理鑑證方法除外，因爲它們的設定是「NT 登入通行碼」。「主要防火牆管理者」可以檢視及修改這個記錄，但是不能將它刪除。此外，對 fwdfadm 而言，防火牆通行碼及 SNK 都是無效的鑑證類型。

完整使用者名稱

指定用來描述使用者的一個名稱。

下列欄位參照鑑證方法。按一下箭號，從鑑證方法列示中選取。在第84頁的『使用者鑑證方法』中會加以說明這些選項。

安全 Telnet

指出當使用者從安全網路上登入時，其身份是否必須以某種方法來鑑證。

非安全 Telnet

指出當使用者從非安全網路上登入時，其身份是否必須以某種方法來鑑證。

安全 FTP

指定使用者使用 FTP，從安全網路存取 Firewall 時，所需要的鑑證層次。

非安全 FTP

指定使用者使用 FTP，從非安全網路存取 Firewall 時，所需要的鑑證層次。

安全 Socks

指定用 Socks V5 鑑證方法來鑑證來自防火牆安全端的 Socks 從屬站連線。按一下箭號，從選項列示中選取。詳細資訊請參閱第84頁的『使用者鑑證方法』。

非安全 Socks

指定用 Socks V5 鑑證方法來鑑證來自防火牆非安全端的 Socks 從屬站連線。按一下箭號，從選項列示中選取。詳細資訊請參閱第84頁的『使用者鑑證方法』。

安全 HTTP

指定用使用者 ID/通行碼類型的鑑證方法來鑑證離埠的 HTTP proxy 要求。按一下箭號，從選項列示中選取。詳細資訊請參閱第84頁的『使用者鑑證方法』。

瀏覽器會提示使用者輸入使用者 ID 及通行碼，所以如果您是使用 SDI，請在通行碼提示時填寫通行碼。

使用者提供的鑑證方法必須了解 Socks/通行碼無法支援交談式對話，因而無法視情況作用。

安全管理

指定透過安全介面從架構從屬站登入時，所用的鑑證方法。請注意：當您進行本地登入 (亦即在登入畫面上選擇本地) 時，您一直都處於安全環境中，所以您使用的就是這種鑑證方法。

非安全管理

指定透過非安全介面，從架構從屬站登入時，所用的鑑證方法。

SecureNet 密碼鎖

指定要由具有「AssureNet Pathways 安全網路密碼鎖」卡之遠端使用者輸入的字元順序。請鍵入您用來起動密碼鎖卡的密碼。 請參閱「SecureNet 密碼鎖」資訊，以取得關於選取和安裝通行碼的指示說明。

註:

a. 這個欄位不適用於 SecurID 卡。

b. 您必須爲每一位使用者建立唯一的隨機密碼鎖。

c. 當您在 SecureNet 密碼鎖卡中安裝密碼時，請使用 AssureNet Pathways 安裝程序，然後選取**模式 5**。

詳細相關資訊，請參閱第88頁的『鑑證方法』。

使用者鑑證方法

使用者鑑證的選項如下：

全部拒絕

使用者被拒絕存取。

全部允許

不需要鑑證。

NT 登入通行碼

NT 登入通行碼比防火牆通行碼的安全性低。但是，如果使用者已在 Windows NT 領域中定義的話，您就可以用 Windows NT 登入通行碼，所以使用者並不需要各種不同的通行碼。

若您選擇這個鑑證方法，則會用區域 Windows NT 使用者資料庫的資料，來驗證您的使用者 ID 及通行碼。如果將「防火牆」架構爲信任其他 Windows NT 伺服器，則會搜尋這些受信任的可靠伺服器，以尋找使用者的定義。

您必須先在 Windows NT Firewall 及可靠的 Windows NT 伺服器之間設定連線，讓 TCP/IP 通信能夠在這二台機器之間傳輸，之後才能設定二者之間的信任關係。

請使用下列預先定義的服務程式來設定這個連線：

1. 領域控制器的鑑證 - 可使用使用者鑑證的領域控制器
2. NetBT 名稱服務程式廣播 - 准許 NetBIOS over TCP/IP 名稱服務程式廣播

並使用 Windows NT 架構公用程式來定義信任關係。

SecureNet 密碼鎖

使用「AssureNet Pathways SecureNet 密碼鎖」完成鑑證。

請在「SecureNet 密碼鎖」欄位中鍵入通行碼，該通行碼亦可用於起動「SecureNet 密碼鎖」卡。

註:

1. 您必須爲每一位使用者建立唯一的隨機密碼鎖。
2. 隨機密碼鎖每一個八進位值的範圍須在 1-377 內
3. 當您在 SecureNet 密碼鎖卡中安裝密碼時，請使用 AssureNet Pathways 安裝程序，然後選取**模式 5**。

詳細相關資訊，請參閱第88頁的『鑑證方法』。

SecurID 卡

使用 Security Dynamics SecurID 安全卡或 pinpad 卡來完成鑑證。*請勿*使用「安全網路密碼鎖」欄位。 以 IBM Firewall 使用此鑑證方法之前，必須先設定 PIN。

在 FTP 下，不支援 SDI 新 PIN 模態及下一個記號模態。

詳細相關資訊，請參閱第88頁的『鑑證方法』。

使用者提供的鑑證 1、2 及 3

由使用者提供鑑證。您最多可以在 Firewall 上安裝 3 個使用者提供的鑑證方法。關於如何爲使用者提供的鑑證建立及編譯次常式的詳細資訊，請參閱 *IBM eNetwork Firewall 參考手冊*。

防火牆通行碼

必須提示使用者鍵入有效的通行碼。完成這個畫面後，「IBM Firewall」會提示您爲新使用者指定通行碼。

「防火牆通行碼」所允許的安全通行碼及通行碼規則比「Windows NT 登入通行碼」多，因此，建議您選擇這個通行碼。

要求使用者變更

請按「是」或「否」，以指定使用者在下次鑑證時，是否需要變更通行碼。

鎖定通行碼

按一下「是」或「否」，指出是否要鎖定通行碼。當登入失敗的次數超過限制，或是未使用通行碼的週數達到「停工前的時間上限」所指定的週數時，就會將這個設定設爲「是」。

管理者可以將這個欄位設定爲「是」，以防止使用者使用通行碼鑑證。

註:

1. 通行碼有大小寫的區分。若您以大小寫混合的方式輸入使用者通行碼，則使用者必須輸入大小寫完全相同的通行碼。如果您的工作站僅接受大寫，請以大寫鍵入使用者的通行碼。
2. 該作業系統可讓您定義通行碼規則。當使用者變更他或她的通行碼時，便可引用通行碼規則，但若是管理者變更了通行碼，則不能引用通行碼規則。通行碼規則如下：

   到期前的警告日數 (日數)
   通行碼到期之前的日數，Firewall 會提供使用者變更通行碼的選項。

   到期前的最大週數
   要求使用者變更通行碼前的週數。

   停工前的最大週數
   通行碼停工前，未使用該通行碼的週數。

   最大允許登入重試數
   通行碼鎖定之前，登入失敗時重試的次數上限。

   重新使用前的通行碼
   存放在「通行碼歷程列示」中的通行碼個數。您不能將通行碼變更爲任何目前在歷程列示中的通行碼。 只有在「可重用通行碼之前的週數」爲 0 的情況下，這個參數才有效。

   可重用通行碼之前的週數
   將通行碼保留在「通行碼歷程列示」中的週數。您不能將通行碼變更爲任何目前在歷程列示中的通行碼。

   最小長度
   通行碼的最少字元限制。

   文字字元數下限
   通行碼的最少文字字元限制。

   其它字元數下限
   通行碼中的非文字字元數下限。

   重複字元數上限
   通行碼中任何單一字元可以重複的次數上限。

   相異字元數下限
   通行碼中不同字元數的下限。

按一下 **Firewall 通行碼**標籤，自行設定每一個使用者的值，如第87頁的圖 24 中所示。

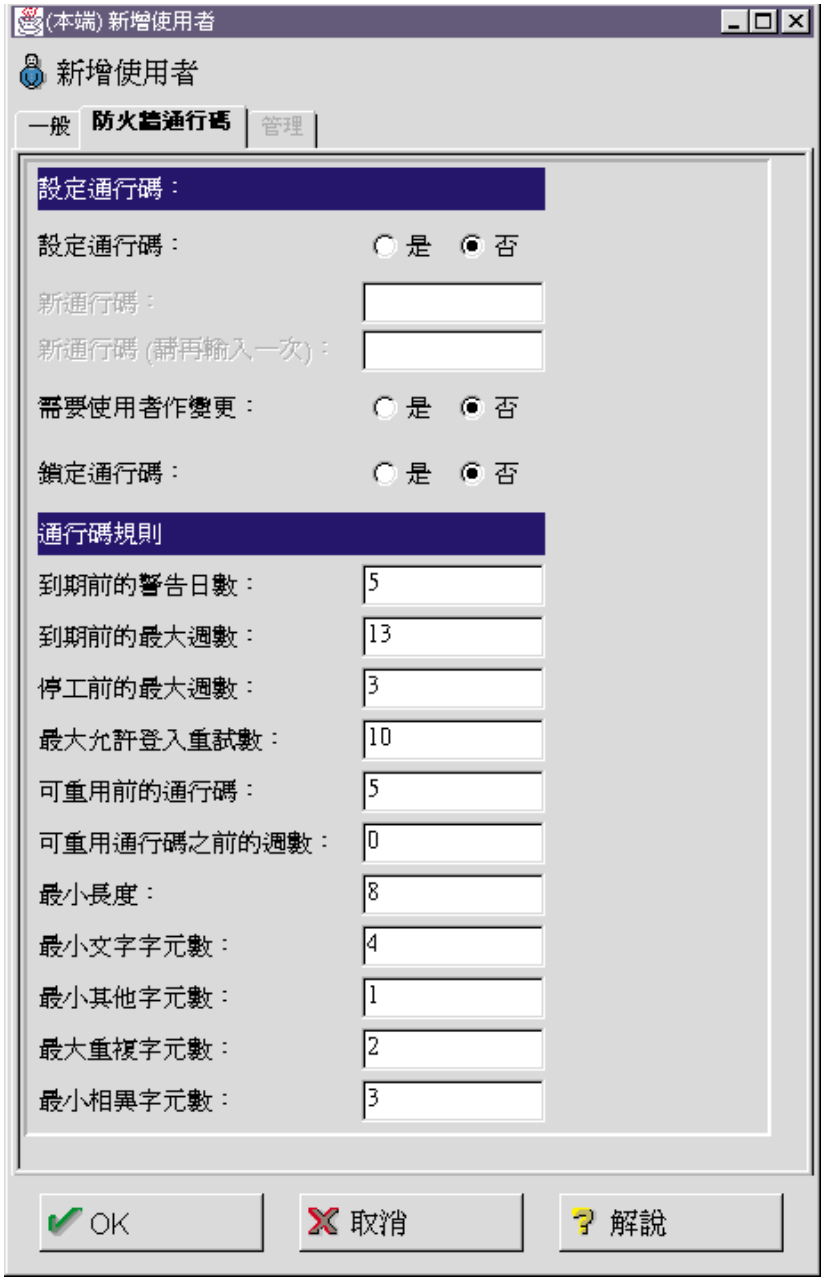

圖 24. 防火牆通行碼標籤

變更使用者存取權

將使用者新增至 Firewall 後，您可以在**修改使用者**對話框上變更該使用者的安全屬性。

1. 從**使用者**對話框中，選取您要變更的使用者，然後按一下**開啓**。
2. 當出現**修改使用者**對話框時，請變更適當的欄位。關於您可變更的使用者屬性列示，請參閱第79頁的『將使用者新增至 IBM Firewall』。
3. 完成所有變更後，按一下 **OK**。

從「IBM Firewall」刪除使用者

註: 請勿刪除使用者 `fwdfuser` 或 `fwdfadm`。

要刪除使用者時，請按一下**使用者列示**畫面上的**刪除**。

根據功能區分的管理者權限層次

只有*主要的防火牆管理者*可以建立及修改管理者，並決定管理者有權使用的防火牆功能。例如，您可將特定管理者的權限設定爲只能執行「使用者」及「日誌監督程式」功能。

請在**新增使用者**對話框上，爲**權限層次**欄位選取「防火牆管理者」。關於完成**新增使用者**對話框的詳細資訊，請參閱第79頁的『將使用者新增至 IBM Firewall』。

然後選取**新增使用者**對話框頂端的**管理者**標籤。選取您要授權予管理者的功能。

鑑證方法

下列爲各種使用者鑑證方法。

全部拒絕

「IBM Firewall」禁止存取伺服器。

全部允許

不需要鑑證。伺服器並不會鑑證您的身份；但接著會出現命令提示，您可以藉由這個命令提示來存取外來主電腦。

防火牆通行碼

伺服器會要求您先輸入防火牆通行碼（不會顯示出來），然後才會讓您繼續。

```
Password:
```

請輸入您的防火牆通行碼。這是當初新增使用者名稱到「防火牆」時所使用的通行碼。

SecurID 卡鑑證

如果您有 SecurID 卡，且您的網路使用 Security Dynamics ACE/Server 的話，您可以使用這個方法。

Proxy 伺服器要求輸入您的 PASSCODE（不會顯示出來）之後才會讓您繼續。

```
Enter PASSCODE:
```

此時，請輸入 4 位數的 SecurID PIN 碼並在後面加上逗點，然後鍵入您的 SecurID 卡碼。例如，當您的 SecurID 卡顯示字碼 179091 時，若要以指定 1234 PIN 的使用者 NEWUSER 身份登入，則必須輸入：

```
login: NEWUSER
Enter PASSCODE: 1234,179091
```

如果使用者一開始便使用 FTP，便會因爲 FTP 沒有提供允許變更通行碼的選項，而導致 SecurID 卡的鑑證失敗。使用者必須在第一次嘗試進行 SecurID 卡鑑證以建立 PIN 時，使用 telnet。使用者隨後可將該 PIN 用於稍後進行的鑑證操作，如 FTP、HTTP 等等。

如果 SecurID 卡是處於新的 PIN 模式，則在對「IBM Firewall」使用此鑑證方法之前必須設定 PIN。

SecureNet 密碼鎖鑑證

如果有「Assurenet Pathways 安全網路密碼鎖」卡，請使用本方法。 當您起始設定 SNK 卡時，請使用下列項目：

- 顯示格式 (十六進位)
- 「消除」功能 (開或關)
- 單一數字的盤問功能 (關)

Proxy 伺服器會要求等待您的「SecureNet 密碼鎖」卡提供回應之後才讓您繼續。

```
Use SNK for challenge
######## for user user_id
Ed:
```

challenge `########` 是一個您輸入到「SecureNet 密碼鎖」卡的 8 位數數字。

1. 當接收到這個提示時，請啓動「SecureNet 密碼鎖」卡並輸入 PIN 碼。 PIN 碼隨此卡提供給您。
2. 請輸入伺服器提供的盤問 (challenge)。

   例如：您登入伺服器，伺服器會提示:

   ```
   Use SNK for challenge
      78987648 for user NEWUSER
   Ed:
   ```

   請將值 78987648 輸入「SecureNet 密碼鎖」卡。然後此卡會顯示回應，您要將此回應提供給 Proxy 伺服器。
3. 請對伺服器輸入這個回應。

   如果「SecureNet 密碼鎖」卡顯示 8AE222A9 來回應您的詢問，請對伺服器輸入 8AE222A9：

   ```
   logon: NEWUSER
      Use SNK for challenge 78987648 for user NEWUSER
   Ed:8AE222A9
   ```

SecurNetKey (SNK) 已經由「AXENT** Technologies」更名爲 Defender Handheld Token** (DHT)。

NT 登入通行碼

若您選擇這個鑑證方法，則會用區域 Windows NT 使用者資料庫的資料，來驗證您的使用者 ID 及通行碼。如果將「防火牆」架構爲信任其他 Windows NT 伺服器，則會搜尋這些受信任的可靠伺服器，以尋找使用者的定義。

使用者提供的鑑證 1、2 及 3

您可以將「使用者提供的鑑證」方法用在 FTP 及 Telnet 上。 相關資訊，請參閱 *IBM eNetwork Firewall 參考手冊*。

第13章 架構 proxy 伺服器

本章包含關於如何從安全網路內外的工作站架構及使用 proxy 伺服器的一般資訊。

HTTP Proxy

HTTP proxy 會在不必使用 Socks 伺服器來瀏覽 Web 的情況下，有效率地處理透過 IBM Firewall 的瀏覽器要求。 使用者可在 Internet 中存取有用資訊，不會危及他們內部網路安全，也不必改變他們的從屬站環境來實施 HTTP Proxy。

HTTP Proxy 不是伺服器。一般使用者無法從 Proxy 中載出檔案或在其中放入檔案。此外，它不是快取 proxy。不會有任何東西是代表 HTTP 要求儲存在防火牆上。

持續性階段作業

持續性連線允許從屬站及伺服器針對 TCP 連線的關閉發出訊號。這種發出訊號的操作須使用一個連線表頭欄位。

IBM Firewall proxy 支援從屬站與 proxy 之間的持續性連線。*最大持續性要求數*條件及*持續性連線逾時*條件可控制該連線的持續時間。如果這些條件之一出現，則 proxy 與從屬站之間的 socket 連線將會關閉。如果*最大持續性要求數*條件及*持續性連線逾時*條件不符，則連線將維持開啓狀態，並交由從屬站負責決定要求何時完成。

如果決定錯誤，便可能導致顯示畫面上指出仍在連線上進行資料傳輸，但實際上並非如此的情況。例如，瀏覽器的動畫圖記在已載入完整頁面之後，卻仍在繼續執行。按一下**停止**，即可停止動畫。請參閱第94頁的『最大持續性要求數』及第94頁的『持續性連線逾時』，以取得這些參數的相關資訊。

使用架構從屬站架構 HTTP Proxy

要架構 HTTP Proxy 時，請執行下列步驟：

1. 您必須准許 DNS 查詢才能適當地運作 HTTP Proxy。要達成此目的很簡單，只要在架構從屬站導覽樹狀結構中的「系統管理」資料夾上按一下「安全性策略」，然後按一下「允許 DNS 查詢」即可。
2. 啓動過濾器
3. 新增連線。關於如何在網路的非安全端設定連線的範例，請參閱第57頁的『Proxy HTTP 的範例』。

4. 若要架構 HTTP Proxy，請從架構從屬站導覽樹狀結構中選取 HTTP。 IBM Firewall 會顯示 **HTTP Proxy** 對話框，如第92頁的圖 25 中所示。

圖 25. HTTP

5. 欲停止 proxy，請選取 `my computer/control panel/services`。請選擇 IBM Firewall HTTP Proxy，然後按一下 *STOP*。

   可執行的 phttpd 是設定爲啓動系統時自動啓動的系統服務程式。

請架構 **HTTP Proxy** 對話框上的參數。如果您變更了任一個參數，則 Firewall HTTP proxy 服務將會停止，然後再重新啓動。現行的 proxy 使用者將發現他們的要求被終止，直到 proxy 重新啓動 (數秒之後)。

Proxy 埠號

使用此參數來指定此 Proxy 應該傾聽要求的埠號。如果變更埠號，則必須架構過濾器來准許或禁止通過連接埠。小於 1024 的埠號會保留給「TCP/IP」應用程式。一般 proxy Web 伺服器所使用的連接埠爲 8080 及 8088。

預設過濾規則設定成禁止連接埠 8080 有入埠的非安全性資料傳輸，但准許相同連接埠有安全資料傳輸。proxy 只拒絕非安全 proxy 要求。預設值是 8080。如果變更預設值，則也必須在針對此架構而設定的「服務程式」中變更埠號。如果變更任何這些設定，則必須重新啓動 phttpd 處理。

內容緩衝區長度上限

您可使用此參數來爲伺服器所產生的動態資料設定緩衝區的大小。從 CGI 程式、伺服器端併入以及 API 程式輸出動態資料。它不是來自 Proxy 的資料。

請以千位元組 (K) 爲單位來指定這個值。預設值爲 50K。

緒儲存池大小

此參數是用來設定同時作用中的最大緒數。 Proxy 會保留新的要求，直到另一個要求已完成且可使用緒爲止。一般而言，機器的功能愈強，此參數所使用的值就應該愈大。如果機器一開始就在經常作業（如交換記憶體）上用掉太多時間，請降低此值。 請指定整數，例如 60。預設值爲 200。

使用者層次

此參數會告訴 proxy 所要鑑證的使用者層次。您可指定參數值爲 all、new 或 none。預設值爲 none。參數值意義爲：

all 這個參數會使所有的瀏覽器傳送 proxy 鑑證回應，以指示瀏覽器提示使用者輸入使用者 ID 及通行碼。如果瀏覽器不支援這個 proxy 鑑證回應，就會出現錯誤頁面來指出錯誤。如果瀏覽器有支援這個回應，就會顯示使用者 ID 及通行碼提示。

new 這個參數可幫助您執行移轉的動作。它只會傳回一個 407 proxy 鑑證回應給將自己識別爲 HTTP/1.1 瀏覽器的從屬站瀏覽器，這個鑑證回應會要求瀏覽器發出輸入使用者 ID/通行碼的提示。您可以在 Internet Explorer 4.0 中設定切換，這樣它就會用 HTTP/1.1 識別碼來廣播要求。 Netscape 及其他瀏覽器都會將它們自己識別爲 HTTP/1.0 要求。

none 不檢查瀏覽器要求。也不提示輸入任何使用者 ID/通行碼。

逾時

這個參數會告訴 proxy 在要求使用者自我重新鑑證之前，要等待從屬站要求的時間。使用者是由特定的 IP 位址及使用者 ID 來鑑證，所謂的特定 IP 位址及使用者 ID，就是在這段閒置期間，給予原始鑑證的資料。請以分鐘爲單位來指定時間。預設值爲 60 分鐘。

只要使用者是處於正在瀏覽的狀態，這個時間視窗就會一直存在。

最大持續性要求數

這個參數可指定 proxy 在 HTTP/1.1 持續性連線上所能接收的要求數上限。這是一個直接影響鑑證逾時的效能工具。在持續性階段作業中，除非持續性階段作業結束，否則不會完成任何的使用者鑑證測試。請以整數指定該值，例如 25。預設值爲 5。

持續性連線逾時

本參數是以秒爲單位，指示在符合 HTTP/1.1 標準的瀏覽器啓動與 proxy 的階段作業時，保留 HTTP/1.1 與從屬站瀏覽器持續連線的時間。這是一個直接影響鑑證逾時的效能工具。在持續性階段作業中，除非持續性階段作業結束，否則不會完成任何的使用者鑑證測試。請以秒爲單位來指定時間。預設值爲 60。

HTTP 記載管理

此參數會告訴 Proxy 將啓動/關閉及所有 proxy 要求記錄到防火牆日誌中。它是使用 LOG_NOTICE 層次來記載。如果想要監督 HTTP 要求活動，請將它設定爲開啓。事件會記載在防火牆日誌機能中。

瀏覽器架構

您必須架構從屬站瀏覽器，來與 HTTP proxy 傾聽的連接埠連線。

如果使用 HTTPS 的話，也請爲安全性 proxy 指向 IBM Firewall 上的 HTTP proxy。

若您想讓您的 Internet Explorer 瀏覽器以 HTTP/1.1 瀏覽器呈現給 proxy，請執行下列步驟：

- 開啓*檢視* 下拉功能表。
- 選取 *Internet 選項*。
- 選取*進階標籤*。
- 向下捲動 HTTP 1.1 設定，並將設定切換爲「開 (on)」。

SSL 連線

支援 HTTP Secure Connection 到其它伺服器的 SSL 通道。在此情況中 IBM Firewall 是作爲閘道。通道自從屬站經過防火牆到伺服器。如下面範例所示，對 HTTP Secure Connection 使用標準連接埠 443：

```
https://www.ibm.com:443
```

另外，請使用預先定義的服務程式 HTTPS proxy 離埠 2/2。

如果使用 HTTPS 的話，也請爲安全性 proxy 指向 IBM Firewall 上的 HTTP proxy。

詳細相關資訊，請參閱第57頁的『Proxy HTTP 的範例』。

支援方法

HTTP Proxy 支援下列方法，這些是瀏覽 Internet 的一些不同方法：

- FTP
- Gopher
- HTTP
- HTTPS
- WAIS

HTTP Proxy 的記載輸出範例

下面這個範例是 HTTP Proxy 經鑑證的 get 要求的記載輸出。

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication UNSUCCESSFUL
for user <Unknown>, on 9.67.140.162, thru secure network ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> Status: 407 from client
9.67.140.162, who requested "GET http://9.67.128.69/ HTTP/1.1" for 0 bytes.
Mar 06 14:05:05 1998 fire3: ICA2024i: User fred successfully authenticated
using NT authentication from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2169i: User fred successfully authenticated
for HTTP Server using NT from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:05 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/HTTP/1.1" for 2693 bytes.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:06 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgsplash.gif HTTP/1.1"
for 211 bytes.
Mar 06 14:05:10 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
```

```
SUCCESSFUL for user fred, on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:10 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgmast.gif HTTP/1.1"
for 211 bytes.
```

記載活動的解釋如下：

- ICA2099i - 顯示回覆碼 407，意思是該 get 要求的鑑證失敗。

  然後瀏覽器會要求使用者進行鑑證，它會要求您提供使用者 ID 及通行碼。
- ICA2140i - 使用者 fred 的鑑證成功。

每當您提出 get 要求來取得該網頁上的任何元素時，就會出現此鑑證。

FTP

1. 使用 FTP proxy 來存取防火牆主電腦。 (我們將使用 ftp_gw.domain.net.com 作爲防火牆的主電腦名稱)。

   ```
   ftp ftp_gw.domain.net.com
   ```

   Proxy 伺服器會要求輸入您的使用者名稱：

   ```
   login:
   ```
2. 請輸入授權的使用者名稱來使用 Firewall：

   ```
   login: jane_doe
   ```

伺服器根據當初您的使用者名稱新增至 Firewall 時所選取的鑑證計劃，來驗證您的身份（請參閱第79頁的『將使用者新增至 IBM Firewall』）。關於 Proxy 伺服器如何鑑證使用者的資訊，請參閱第88頁的『鑑證方法』。

鑑證之後，Proxy 伺服器會顯示 FTP 命令提示。

```
ftp>
```

使用 quote 和 site FTP 命令來連線至外來主電腦：

```
ftp> quote site forhost.network.outside.com
```

現在，外來主電腦會要求您鍵入用於連線的使用者名稱和通行碼。 這多半與用於 Firewall 的 FTP 的使用者名稱與通行碼不同。

預設的登入逾時值爲 60 秒，而閒置的 proxy 逾時值爲 7200 秒。欲變更預設逾時值，請參閱第99頁的『置換 FTP 及 Telnet Proxy 的逾時值』。

透通式 FTP

您可以 ftp 方式通過「防火牆」。透通式 Proxy 不需要防火牆鑑證，因此透通式 Proxy 的使用者不須定義成防火牆 Proxy 使用者。 透通式 Proxy 只能從防火牆的安全端離開到防火牆的非安全端。爲了使透通式 Proxy 能夠運作，必須在「安全性策略」架構從屬站畫面中選取它。

1. 使用 ftp 來存取防火牆主電腦。(我們將使用 ftp_gw.domain.net.com 作爲防火牆的主電腦名稱。)

   ```
   ftp ftp_gw.domain.net.com
   ```

2. Proxy 伺服器會要求輸入您的使用者名稱：

   ```
   USER:
   ```

3. 請在非安全網路中輸入您的使用者名稱：

   ```
   USER: username@remote_site_host_name
   ```

4. 然後，目標主電腦會提示您輸入在上一個步驟中輸入之使用者名稱 的通行碼。

   ```
   password:
   ```

5. 請輸入您的通行碼。

登入的預設逾時值是 60 秒，而閒置 proxy 的預設逾時值爲 7200 秒 (兩個小時)。欲變更預設逾時值，請參閱第99頁的『置換 FTP 及 Telnet Proxy 的逾時值』。

Telnet

使用 telnet proxy 來登入防火牆 Proxy 伺服器。 您可以使用主電腦名稱或 Internet 位址。然後，在鑑證過您的資格後，請在 Firewall 上使用 telnet 命令來登入目的地主電腦。 例如，從安全網路內使用 telnet，以主電腦名稱 telnet_gw 通過 Firewall 來存取最終目的地 forhost.network.outside.com。

1. 若要啓動處理，必須使用 telnet 來存取防火牆主電腦。 (我們將使用 telnet_gw.domain.net.com 作爲 Firewall 的主電腦名稱。)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. Proxy 伺服器會要求輸入您的使用者名稱：

   ```
   login:
   ```

3. 請輸入授權的使用者名稱來使用 Firewall：

   ```
   login: jane_doe
   ```

伺服器根據當初您的使用者名稱新增至 Firewall 時所選取的鑑證計劃，來驗證您的身份（請參閱第79頁的『將使用者新增至 IBM Firewall』）。關於 Proxy 伺服器如何鑑證使用者的資訊，請參閱第88頁的『鑑證方法』。

您將會使用 oneact shell。有了 IBM Firewall proxy telnet 常駐程式，所有的通信都會透過防火牆傳遞。

若您使用 oneact shell，則在鑑證之後，Proxy 伺服器會顯示：

```
ENTER DESIRED HOST:
```

輸入

```
telnet forhost.network.outside.com
```

外來主電腦會要求您鍵入使用者名稱和通行碼，因爲您的身份已登記在該主電腦上了。這些可能與您在防火牆 Proxy 伺服器中使用的使用者名稱與通行碼不同。

預設的登入逾時值爲 60 秒，而閒置的 proxy 逾時值爲 7200 秒。欲變更預設逾時值，請參閱第99頁的『置換 FTP 及 Telnet Proxy 的逾時值』。

透通式 Telnet

您可以 telnet 方式通過「防火牆」。透通式 Proxy 不需要防火牆鑑證，因此透通式 Proxy 的使用者不須定義成防火牆 Proxy 使用者。 透通式 Proxy 只能從 Firewall 的安全端離開到 Firewall 的非安全端。爲了使透通式 Proxy 能夠運作，必須在「安全性策略」架構從屬站畫面中選取它。

1. 使用 telnet 來存取防火牆主電腦。（我們將使用 `ftp_gw.domain.net.com` 作爲主電腦名稱。）

   ```
   telnet telnet_gw.domain.net.com
   ```

2. Proxy 伺服器會要求輸入您的使用者名稱：

   ```
   Login:
   ```

3. 請在非安全網路中輸入您的使用者名稱：

   ```
   Login@remote_host
   ```

外來主電腦會要求您鍵入使用者名稱和通行碼，因爲您的身份已登記在該主電腦上了。這些可能與您在防火牆 Proxy 伺服器中使用的使用者名稱與通行碼不同。

預設的登入逾時值爲 60 秒，而閒置的 proxy 逾時值爲 7200 秒。欲變更預設逾時值，請參閱第99頁的『置換 FTP 及 Telnet Proxy 的逾時值』。

置換 FTP 及 Telnet Proxy 的逾時值

FTP 及 Telnet 都有「登入」及「等候閒置」的逾時值。預設的狀況下，在登入及鑑證使用者期間，每 60 秒內必須至少有一個階段作業活動。這就是所謂的 loginTimeout。

登入成功後，至少在 7200 秒內階段作業必須有活動，否則就會切斷階段作業的連線。

在 ROOTDIR\config 目錄中建立 fwTimeout.cfg 檔案，並以秒爲單位來指定新的逾時值，即可置換這些預設值。 fwTimeout.cfg 檔案應有下列格式。

```
telnet
proxyTimeout=7200
loginTimeout=60

ftp
proxyTimeout=7200
loginTimeout=60
```

第14章 監督防火牆記載

本章說明即時監督記載警示的方法。違反架構臨界值時會產生警示。

IBM Firewall 會根據使用者定義的臨界值，來監督送到防火牆日誌的訊息，看看是否有潛在的危急狀況。違反臨界值時，Firewall 會以防火牆管理者所指定的方式來遞送警示。

臨界值定義

臨界值由計數與時間參數組成 -- 如果在指定時間（以分鐘爲單位）內超過某個計數（特定事件數量），臨界值則遭違反，這時會產生警示訊息。日誌監督程式辨識四種臨界值：

1. 鑑證失敗總數
2. 特定使用者 ID 的身份驗證失敗
3. 產生自任何特定主電腦的身份驗證失敗
4. 日誌中訊息標籤的出現

架構從屬站或命令行介面可以用來架構全部的臨界值。 IBM Firewall 會自動收到任何對臨界值定義所做的變更。

警示訊息

到達某臨界值之後，IBM Firewall 會產生警示訊息。 警示訊息的傳送可能是採用下列 4 種形式的任何一種：

1. 記錄到下列日誌檔中：
   - 透過警示日誌機能，可藉由架構從屬站或命令行架構。
   - 在防火牆日誌中
2. 將 E-mail 郵件傳送到一整列的使用者
3. 透過所設定的呼叫器。請參閱第103頁的『呼叫器通報支援』。
4. 執行使用者定義的命令行，並以警示訊息作爲第一個參數

警示訊息包含與特定臨界值違規有關的資訊。例如：

```
ICA0001e: ALERT -- 20 authentication failures.
ICA0002e: ALERT -- 10 authentication failures for user root.
ICA0003e: ALERT -- 15 authentication failures from host 56.67.78.89
ICA0004e: ALERT -- Tag ICA1234e with 3 log entries.
```

不會監督由「日誌監督程式」產生的警示訊息及其它訊息。

使用架構從屬站來架構日誌監督程式

本節說明如何使用架構從屬站來架構即時日誌監督程式。 從架構從屬站導覽樹狀結構之中選取「系統日誌」。連按兩下檔案資料夾圖記以展開檢視畫面。 按一下**日誌監督臨界值**。

從**日誌監督臨界值管理**對話框中，您可新增、變更或刪除臨界值定義。

新增日誌監督程式

要新增臨界值定義時，請從**日誌監督臨界值管理**對話框中選取**新增**，然後按一下**開啓**。**新增日誌監督程式**對話框即會出現。請在下列欄位填入資料：

1. 要從等級類型列示中選擇，按一下**等級類型**箭號。類別類型如下：
   - 郵件通報
   - 執行命令
   - 個別使用者鑑證失敗臨界值
   - 鑑證失敗臨界值總數
   - 個別主電腦鑑證失敗臨界值
   - 訊息臨界值
2. 如果選取的類別類型爲「郵件通知」，請鍵入電子郵件位址。您可定義多重通報類別。

   將全部的臨界值違規訊息傳送至指定的電子郵件位址。
3. 如果選取的類別類型爲「執行命令」，請填入命令檔名。

   日誌監督程式執行本命令時會以警示訊息作爲它的第一個參數。您只能定義一個執行命令類別。
4. 如果選取的類別類型是「訊息臨界值」，請填入訊息標籤，這是來自您要監督的 IBM Firewall 日誌訊息的標準標籤。
5. 如果選取其中一個臨界值類別，請填入臨界值計數欄位。

   臨界值計數是指定期間內所容許的最大失敗事件數。
6. 如果選取其中一個臨界值類別，請填入臨界值時間欄位。

   臨界值時間是指從某事件第一次出現開始的分鐘數。
7. 如果選取其中一個臨界值類別，請按一下「是」或「否」來指示是否要使用呼叫器通報。
8. 填入備註，這是屬於選用性動作。
9. 按一下 **OK**。

變更臨界值定義

要變更臨界值定義時，請從**日誌監督臨界值管理**對話框中選取想要變更的項目，然後按一下**開啓**。**變更日誌監督程式**對話框即會出現。

1. 請鍵入您要對臨界值計數和臨界值時間欄位所做的變更。

   臨界值計數是在指定期間內所偵測到的最多失敗鑑證訊息數。臨界值時間是指從某訊息第一次出現開始的分鐘數。

2. 按一下 **OK**。

刪除臨界值定義

要刪除臨界值定義時，請從**日誌監督臨界值**對話框中選取想要刪除的項目，然後按一下**刪除**。系統會要求您確認刪除。 請按一下**是**以確認。請注意：刪除不表示從日誌檔中刪除。它表示刪除此定義。

呼叫器通報支援

Firewall 有侵入警示時，Firewall 可以將訊息送到管理者的傳呼器，來呼叫系統管理者。要設定呼叫器通報支援時，必須架構下列 3 種呼叫器元件。

1. 命令自行設定 - 此元件必須使用架構從屬站來建立與修改。它會爲日誌監督程式所使用的呼叫器命令 (可從命令行使用)，設定預設值。本元件包含定義呼叫器環境的唯一項目。定義及自行設定此元件的相關資訊，請參閱第104頁的『命令自行設定』。

2. 電訊公司管理 - 您必須在數據機連線之前定義適當的電訊公司。本元件包含美國境內所使用的預設電訊公司列示。如果您使用的電訊公司不是其中之一，請在本元件中新增您的電訊公司。相關資訊，請參閱第106頁的『電訊公司管理』。

   請向您的電訊公司取得電話號碼，以驗證電訊公司的現行電話號碼。與電訊公司交談時，請確定取得電訊公司的數據機號碼及其它適用於已購買之特定服務程式的設定。

3. 數據機管理 - 數據機連線之前，必須建立適合的數據機定義。這些定義包含呼叫器通報支援所需使用的數據機所有相關資訊。本元件包含您可從中選取的數據機列示。然而，某些數據機可能與您的電訊公司支援的不相容，雖然您可以將它們新增到列示中。維護數據機定義的相關資訊，請參閱第108頁的『數據機管理』。

註: IBM Firewall 支援可用於呼叫器通報支援的 Tele-AlphaNumeric Protocol (TAP) 通訊協定。

支援的電訊公司和數據機

電訊公司資料庫檔包含電訊公司的列示，以及相關的傳輸參數。 您可以新增其它電訊公司。電訊公司名稱及數據機電話號碼以外的其他參數：

- 文字型呼叫器的訊息長度上限，以及數字型呼叫器的數字位數上限
- 傳輸速率、同位檢查、資料和停止位元長度

使用特定電訊公司之前，請確定該電訊公司是使用 TAP 通訊協定。

呼叫器碼包含預設的數據機定義，分別是：

- IBM MOD 448 14400 bps
- IBM 5853 2400 bps
- IBM 7852 28800 bps
- IBM 7855 2400 bps
- Generic Hayes 相容性
- US Robotics Courier 9600 bps
- Zoom V.34

架構呼叫器通報支援

「呼叫器設定」是用來架構命令自行設定檔以及維護電訊公司和數據機。如果您是使用呼叫器，您必須先使用「呼叫器設定」來自行設定呼叫器環境，再使用「日誌監督程式」。

開始之前，您必須先從電訊公司取得正確的數據機電話號碼、呼叫器 ID，以及數據機參數。

欲架構「呼叫器通報支援」，請從架構從屬站導覽樹狀結構選取「系統管理」。 連按兩下檔案資料夾圖記以展開檢視畫面。 選取**系統日誌**。連按兩下檔案資料夾圖記以展開檢視畫面。選取**呼叫器設定**。

命令自行設定

選取**呼叫器設定**時，您可選取要使用的電訊公司及數據機，並寫入呼叫器訊息。

命令自行設定

從導覽樹狀結構中選取**呼叫器設定**時，即會顯示具有「命令自行設定」的**呼叫器設定**對話框，類似 第105頁的圖 26 中所顯示的對話框。

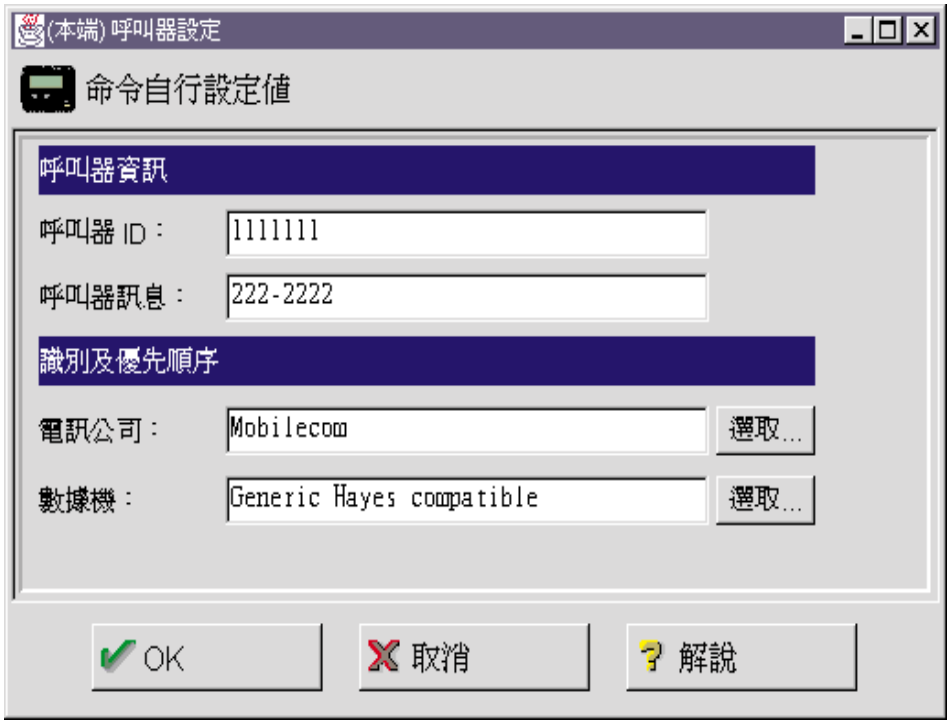

圖 26. 呼叫器設定

在要新增的輸入欄位中鍵入或選取一些值：

1. 請鍵入呼叫器 ID。這通常是電訊公司指定給您呼叫器的唯一 PIN。
2. 請鍵入呼叫器訊息。此字串包含使用者所要傳送的預設訊息。傳送給數字型呼叫器的訊息必須只能是數字。傳送給文字型呼叫器的訊息可以是文字訊息。請勿超出電訊公司設定中所指定的訊息長度上限，否則訊息可能會被截斷。不可使用冒號 (:)。如果您使用冒號的話，空白字元會取代冒號。
3. 如果沒有電訊公司名稱，請按一下**選取**來定義電訊公司。**呼叫器的電訊公司管理**對話框即會顯示出來。請參閱第106頁的『電訊公司管理』，以取得如何填寫此畫面的相關明細。
4. 如果沒有數據機名稱，請按一下**選取**來定義數據機。 **呼叫器數據機管理**對話框即會顯示出來。請參閱第108頁的『數據機管理』，以取得如何填寫此畫面的相關明細。
5. 按一下 **OK**。

變更命令自行設定

從導覽樹狀結構中選取「呼叫器設定」時，即會顯示具有「命令自行設定」的**呼叫器設定**對話框。

1. 在輸入欄位中鍵入或選取一些值，來修改現有自行設定輸入欄位中的值。
2. 按一下 **OK**。

刪除命令自行設定

1. 從列示中選取項目，然後按兩下**刪除**，即可刪除**呼叫器的電訊公司管理**對話框或**呼叫器數據機管理**對話框上的項目。

   系統會要求您確認刪除。
2. 按一下**是**，確認刪除；或按一下**否**，返回**呼叫器設定**對話框。

如果沒有自行設定項目，則呼叫器通報支援無法傳送呼叫。

電訊公司管理

從**呼叫器設定**對話框中跳至電訊公司名稱欄位，然後按一下**選取**。**呼叫器的電訊公司管理**對話框即會顯示出來，如第107頁的圖 27 中所示。

圖 27. 呼叫器的電訊公司管理

新增電訊公司

要增加新的電訊公司時，請在**呼叫器的電訊公司管理**對話框上選取**新增**，然後按一下**開啓**。在適當輸入欄位中鍵入或選取一些值：

1. 請鍵入電訊公司名稱。任何名稱都可以，只要它是唯一的名稱，且提供足夠的資訊可讓您分辨它是哪一個載波即可。
2. 請輸入載波電話號碼 (載波公司的數據機電話號碼)，該電話號碼與其語音呼叫或其他服務號碼不同。當呼叫裝置及您所使用的服務程式要求您輸入數據機號碼時，您所提供的號碼必須是正確的，您必須分辨它的範圍是區域性或全國性的，而呼叫器是數字型的或文字型的。
3. 請輸入 TAP 以取得呼叫方法；這是所允許的唯一值。
4. 如果載波允許或要求通行碼，則請輸入通行碼。
5. 請輸入「文字型呼叫器」的訊息最長長度限制，以及「數字型呼叫器」的數字最長長度限制。
6. 請鍵入傳輸速率。按一下箭號，然後從列示之中選取一值。
7. 針對同位檢查欄位按一下**偶數**、**奇數**或**無**。
8. 選擇預設資料位元數；按一下 **7** 或 **8**。
9. 選擇預設的停止位元；請按一下 **1** 或 **2**。

10. 按一下 **OK**。

變更電訊公司

1. 從**呼叫器的電訊公司管理**對話框中選取要變更的電訊公司，然後按一下**開啓**。
2. 可變更欄位的相關說明，請參閱第107頁的『新增電訊公司』。電訊公司名稱本身無法變更。本欄位將被停用。
3. 進行想要的變更。
4. 按一下 **OK**。

刪除電訊公司

1. 從**呼叫器的電訊公司管理**對話框中選取要刪除的電訊公司，然後按一下**刪除**。
2. 系統會要求您確認刪除。請按一下**是**以確認。

註: 電訊公司資料庫檔中至少要有一個電訊公司。如果未定義任何電訊公司，則呼叫器通報支援會失效。

數據機管理

您的數據機手冊中會記載有關如何起始設定數據機的資訊。您可能需要調整電訊公司的數據機設定。一般而言，只會支援使用標準數據機命令的 Hayes 相容數據機。

從**呼叫器設定**對話框中跳至數據機名稱欄位，然後按一下**選取**。**呼叫器數據機管理**對話框即會顯示出來，如第109頁的圖 28 中所示。

圖 28. 呼叫器數據機管理

您可使用本對話框來新增、變更或刪除各種不同的數據機。

新增數據機

要增加新的數據機定義檔時，請從**呼叫器數據機管理**對話框中選取**新增**，然後按一下**開啓**。在**新增數據機**對話框中，請在輸入欄位中鍵入或選取一些值。

1. 請鍵入數據機名稱。任何名稱都可以，只要和其他定義不同，且提供足夠的資訊可讓您分辨它是哪一個數據機即可。
2. 請輸入「COM 連接埠」的號碼，以定義數據機所要連接的序列 COM 連接埠號。請輸入小於 10 的數字。數據機必須是硬體架構給此連接埠時，則它不能定義給 Windows NT，否則會造成該埠拒絕存取呼叫器功能。如果數據機不符合硬體設定，則呼叫器字碼會在重試一段時間後失效。
3. 請輸入起始設定字串，它可以將數據機定義爲資料數據機，擁有 X level4 的回應，以及由區域站台所定義的固定傳輸速率。請勿包含 AT 命令，因爲呼叫器功能會將它放在起始設定字串開始的地方。

4. 請輸入外線前置符號。此號碼爲您要從公司撥接外線時所需的數字。
5. 按一下 **OK**。

變更數據機

1. 要變更數據機定義檔時，請從**呼叫器數據機管理**對話框中選取數據機名稱，然後按一下**開啓**。

   在**變更數據機**對話框上，您會看到可爲數據機定義變更的欄位列示。 關於這些欄位的說明，請參閱第109頁的『新增數據機』。

2. 按一下 **OK**。

刪除數據機

1. 要刪除數據機定義檔時，請從**呼叫器數據機管理**對話框中選取數據機名稱，然後按一下**刪除**。
2. 系統會要求您確認刪除。請按一下**是**以確認。

呼叫器通報記載功能

呼叫器通報處理會使用防火牆日誌公用程式來撰寫輸出日誌。所有的呼叫器訊息及錯誤都會寫在一般防火牆系統日誌機能中。 欲取得如何設定及使用防火牆日誌檔的相關資訊，請參閱第113頁的『第15章 管理日誌與保存檔』。

測試呼叫器設定

您可以使用呼叫器命令來驗證呼叫器設定。相關詳細資訊，請參閱 *IBM eNetwork Firewall 參考手冊*。建議您在每一次定義或變更設定時，都務必使用呼叫器命令，以確保您的系統、數據機、電訊公司及呼叫裝置都能夠正確地彼此通信，而且您都能夠確實地傳送或接收呼叫。

執行命令

您可以指定一個程式，在每次到達警示臨界值時即會呼叫它。若要指定程式：

1. 按一下**日誌管理**，然後連按兩下**新增**。

   新增日誌監督程式對話框即會出現。

2. 在**等級類型**下拉方框中，選取**執行命令**。這時會啓用畫面上的**命令檔案名稱**欄位。
3. 在**命令檔案名稱**欄位中，鍵入到達警示臨界值時，您所要呼叫的程式之完全合格路徑名稱。

   日誌監督程式所執行之命令的工作目錄爲 `\winnt\system32`。因爲命令 Shell 是從系統程序起動的，所以只設定系統環境變數。並沒有設定使用者環境變數。一般而言，已起

動的程式應使用完整的檔案名稱，而不應倚賴路徑變數。

「防火牆」會將完整「警示」訊息傳送爲程式的第一個參數，如下所示：

鑑證失敗總數警示：ICA0001e
每個使用者鑑證失敗警示：ICA0002e
每個主電腦鑑證失敗警示：ICA0003e
訊息臨界值警示：ICA0004e

請參閱 *IBM eNetwork Firewall 參考手冊*，即可取得這些訊息的完整說明。

第15章 管理日誌與保存檔

本章將說明如何透過「架構從屬站」來使用日誌機能。 當使用者試圖透過不同的 IBM Firewall 伺服器來存取主電腦時， IBM Firewall 會將項目寫入由 IBM Firewall 記載服務程式所維護的日誌檔中。

IBM Firewall 會根據防火牆的架構方法來產生大量記載資訊。日誌項目可來自許多地方，如 socks 和專門過濾器。另外，也可以不同的嚴重性層次來寫入日誌檔；例如，*偵錯*、*資訊*或*錯誤*。 本章也說明如何使用日誌管理與日誌保存管理機能，來管理日誌與保存檔的大小。

使用架構從屬站來建立與保存日誌檔

架構從屬站可以用於日誌管理與日誌保存管理。 假設您的可用磁碟空間足夠容納全部日誌資訊。 Firewall 會將產生的例行偵錯及錯誤資訊，記載到防火牆日誌機能。只有主要防火牆管理者才能存取防火牆日誌機能。警示訊息會記載到警示日誌機能中。 管理審核日誌資訊會記載到審核日誌機能中。

爲了讓報告公用程式可以正常運作，必須只能讓防火牆日誌訊息出現在它們的輸入檔中。 不可將其它機能導向到與防火牆日誌相同的檔案中，所以請視情況設定防火牆記載功能。

如果要在主要架構從屬站畫面上查看警示，則必須將警示導向到指定爲警示日誌機能的檔案中。不可爲該檔案指定其它項目。

下列優先順序層次是以擷取大部份資訊的*偵錯*所累計的。「嚴重的 (Critical)」只擷取最嚴重的防火牆事件。

- 偵錯
- 資料
- 警告
- 錯誤
- 嚴重的

建議您從*資訊*層次開始，除非防火牆程序穩定。然後，您可以變更爲*警告*或*錯誤*，以減少記載的活動並縮小系統日誌的規模。

優先順序層次與訊息標籤字尾 *(i,e,w,s..)* 並不完全吻合。您可能需要測試，才能判定要如何*關閉 (shut off)* 那些訊息。

新增日誌機能

從架構從屬站導覽樹狀結構中，連按兩下「系統管理」檔案資料夾圖記，以展開檢視畫面。連按兩下「系統日誌」檔案資料夾圖記以展開檢視畫面。 選取「日誌機能」。**日誌機能**對話框即會出現，並顯示目前啓用一組的日誌機能。

1. 請從**日誌機能**對話框中選取**新增**，然後按一下**開啓**，即可將系統日誌 (syslog) 項目新增到那些目前已啓用的日誌機能。

   顯示**新增日誌機能**對話框，如第114頁的圖 29 所示。

圖 29. 新增日誌機能

2. 按一下**類型**箭頭，來選取類型。類型爲「檔案名稱」。
3. 日誌機能會判斷已記載的資訊之類型與來源。按一下**機能**來選取下列其中一種日誌機能：

- 防火牆日誌 - 一般防火牆日誌，包括過濾記載
- 警示日誌 - 日誌監督常駐程式狀態，以及用來輸入「警示顯示畫面」的臨界值違規警告
- 郵件日誌

4. 按一下**優先順序**箭頭，來選擇優先順序。記載優先順序會依遞增嚴重性的次序來列示。您將選取的優先順序爲日誌記載的最低層次。
5. 填入日誌檔名。該日誌檔名稱必須有絕對路徑 (以磁碟機及正斜線 / 開始)，而且該檔案的路徑必須存在。
6. 保存管理只可與*檔名*類型日誌功能一起使用。啓動之後，可以定期地縮小日誌檔。啓用保存管理表示您會根據 `fwlogmgmt` 命令來設定參數。 請參閱第116頁的『保存日誌』。您可啓動或停用保存管理參數。
7. 選取已保存現行日誌中的記錄之全天數。此值必須是零或大於零。當 `fwlogmgmt -l` 命令找到現行日誌記錄符合此基準時，便會執行保存操作。日誌管理並不包括計算保留日誌記錄天數的當天。
8. 請輸入保存檔名及完整的路徑。 IBM Firewall 提供一個使用目錄的預設保存功能。然而，您可以使用附加功能 (如果有需要的話)。
9. 選取應該從保存資料中刪除所保存日誌檔的等候全天數。此值必須是零或大於零。當 `fwlogmgmt -a` 命令找到保存的檔案符合此基準時，便會執行去除操作。日誌管理並不包括計算保留保存檔案天數的當天。
10. 按一下 **OK**。

變更日誌機能

1. 請從**日誌機能**對話框中選取您要變更的防火牆日誌項目，然後按一下**開啓**。

   變更日誌機能對話框即會出現。
2. 變更想要的欄位。關於欄位的說明，請參閱第114頁的『新增日誌機能』。
3. 按一下 **OK**。

刪除日誌機能

1. 請從**日誌機能**對話框上目前已啓用的日誌機能中選取防火牆日誌項目，然後按一下**刪除**。

   顯示**刪除警告**畫面。
2. 如果要繼續刪除，請按一下 **OK**。 如果不要繼續刪除，請按一下**取消**。 此動作不會刪除眞正的日誌檔。

保存日誌

保存程序如下：

- 從現行日誌中移除合格的記錄
- 將它們置於其它檔案中
- 緊密結合結果檔
- 將新檔案放入保存目錄中

若您要啓動日誌管理程式來保存已累積的日誌記錄，有二種做法可供您選用：

1. 偶而從命令行執行 `fwlogmgmt -l` ，或是
2. 將 `fwlogmgmt -l` 命令設定爲 NT Scheduled Service。

去除日誌保存是由刪除保存目錄中的合格保存檔所組成。

要去除保存的檔案時，您有兩個選項：

1. 偶而從命令行上執行 `fwlogmgmt -a` 命令
2. 將 `fwlogmgmt -a` 命令設定爲 NT Scheduled Service。

合格的記錄及檔案是由日誌機能定義中所指定的值來決定，如第114頁的『新增日誌機能』中所述。

執行日誌管理處理最有效或最便利的方法就是，將它設定爲 NT Scheduled Service。您可以用「控制台」上的「服務程式」物件來啓動它。

例如，如果要設定在每日 3:00 AM 執行日誌管理保存處理，請鍵入

```
at 3:00 /every:M,T,W,Th,F,S,Su fwlogmgmt -l
```

附加的 DLL

請參閱 *IBM eNetwork Firewall 參考手冊*，以取得可用來取代 Firewall 預設 DLL 的日誌保存程式附加的 DLL 相關資訊。

日誌管理輸出

進行任何日誌管理活動之前，日誌管理機能會執行一些初步的完整性檢查。如果發現任何問題，則在命令行下執行 `fwlogmgmt` 命令時，會將偵錯送到防火牆日誌機能。

郵件或管理審核 (local0) 日誌機能是受不同的保存規則所支配，而不是受其他機能支配。所有的日誌機能都必須啓用保存功能，才能進行保存。然而，都只有在其日期超過基準 (執行保存處理時，在機能定義中指定基準) 時，才會保存防火牆 (local4) 及警示 (local1) 日誌記錄；但是每一次都會把*整個* 郵件或審核日誌檔案保存起來。同時，郵件日誌中的資訊被認爲

是針對偵錯目的而使用的，而且一般而言，只有用些許參數值來保存。另外，通常更有用的郵件資訊會記載在防火牆 (local4) 日誌中。

報告公用程式

您可以使用「報告公用程式功能」來幫助您從現行的或保存的日誌檔產生報告。 「報告公用程式」產生一些經組織與格式化的管理資訊檔，便於輕易地對映到關連式資料庫表格。 這些表格可協助防火牆管理者分析：

- 防火牆的一般用法
- 防火牆處理中的錯誤
- 在未經授權情況下嘗試存取安全網路

管理者可使用公用程式和防火牆日誌來建立訊息的一般文字檔。接著，會產生表列化檔案，並匯入關聯式資料庫系統（像是 DB2 系列的產品）的表格中。然後，管理者就可使用「結構化查詢語言」(SQL)，來查詢資料並產生報告。

安裝「報告公用程式」作爲 Firewall 安裝的組件。您也可以將它們個別安裝，並且在非防火牆主電腦上執行。您可以在防火牆上使用架構從屬站來執行「報告公用程式」。在非防火牆機器上，請使用命令行。

爲了讓報告公用程式可以正常運作，必須只能讓防火牆日誌訊息出現在它們的輸入檔中。不可將其它機能導向到與防火牆日誌相同的檔案中，所以請視情況設定防火牆記載功能。

請勿在任何比 IBM Firewall for AIX V3R1 舊的日誌檔上使用「報告公用程式」。但是，您可以使用報告公用程式來處理 IBM Firewall for AIX V3R1 或更新版本的日誌檔。您也可以用它們來處理 AIX su 日誌。關於報告公用程式的詳細資訊，請參閱 *IBM eNetwork Firewall 參考手冊*。

使用架構從屬站來執行報告公用程式

從架構從屬站導覽樹狀結構中，連按兩下「系統管理」檔案資料夾圖記，以展開檢視畫面。連按兩下「系統日誌」檔案資料夾圖記以展開檢視畫面。選取**報告公用程式**。顯示**報告公用程式**對話框，如第118頁的圖 30 所示。

圖 30. 報告公用程式

1. 針對 IBM Firewall 提供的預設保存器，日誌保存路徑名稱是包含壓縮日誌檔的目錄。在日誌保存路徑名稱欄位中，請輸入您在**日誌機能**對話框之保存目錄欄位中所指定的目錄。請輸入保存目錄的明確路徑名稱。若要檢視未經保存的日誌檔，本欄位請保留空白。
2. 選取**報告類型**。要產生展開的日誌訊息文字時，請選取**文字日誌**。若要建立 DB2 所使用的表列化的檔案，請選取**表格日誌**。如果將所產生的檔案匯入 DB2，則可在日誌資料上執行 SQL 查詢。相關資訊，請參閱 *BM eNetwork Firewall 參考手冊*。
3. 日誌檔名可能是任何一個壓縮保存日誌檔或其它有效防火牆日誌 或 AIX su 日誌檔的名稱。如果在日誌保存目錄欄位中輸入項目，則可按一下**日誌檔名**箭號，來選擇要使用的日誌。如果在步驟 1 中未輸入日誌保存，此處輸入的日誌檔名稱則必須是有效的解壓縮防火牆日誌檔或 AIX su 日誌檔的名稱。您必須指定完整路徑。
4. 選取**防火牆**或 **AIX su** 其中一種**日誌類型**。
5. 請輸入**輸出文字的路徑和檔名**。
6. 選取**是**，將表格日誌要求的結果附加至現有製表檔，或選取**否**來取代現有檔案。
7. 此欄位可讓您選取特定的訊息類型，以便置於輸出文字檔中。此欄位的內容會被視爲是放入標準 Windows NT `Find` 命令中的參數。例如，假設您在該欄位中鍵入 ″ICA0″ (必須包含引號)，就如同您在執行下列命令：

```
fwlogtxt < my.log | find "ICA0"
```

以下是一些您可以放入此欄位的項目範例及其結果：

過濾器	結果
"ICA0"	列出日誌監督臨界值警示訊息
"ICA3"	列出與 Socks 相關的訊息 (#ICA3000 - 3999)
"ICA2010"	僅列出 ICA2010 訊息的出現次數
/V "ICA3"	列出除 Socks 訊息之外的所有訊息
/C "ICA001"	計算 ICA0001 訊息的數目

8. 按一下 **OK**，防火牆機器上指定輸出目錄中所會產生要求的檔案。
9. 「報告公用程式結果」區域會顯示任何來自已執行報告公用程式的錯誤訊息。要檢視來自「文字日誌」報告類型的日誌文字結果，請按一下主「防火牆架構從屬站」畫面上的**日誌檢視器**，並鍵入完整的輸出檔名。由表格日誌取得的 .tbl 檔案可以載入資料庫，請參閱 *IBM eNetwork Firewall 參考手冊*。

第16章 轉換網路位址

由於 Internet 的急速發展，突顯出 IP 位址殆盡的問題。「網路位址轉換」(NAT) 提供一個解決方案，以位址的重新使用爲基礎，來解決 IP 位址殆盡的問題。

專用網路中的位址可以自龐大位址空間當中 (一般爲 10.0.0.0 等級 A 的位址空間) 來指定。這些位址爲專用的，而且不會顯露在 Internet 上。因此，其它 IP 網路也可以重複使用這些位址。單一的 IP 登記位址會被用來隱藏許多專用網路位址。 NAT 會將未登記的位址及埠號轉換爲有效的 Internet 登記位址及埠號。在入埠方向的 NAT 會將已登記的 Internet 位址及埠號轉換回復爲未登記的位址及埠號。 NAT 的好處是，透通式容許使用專用或非法位址的網路與 Internet 上的主電腦通信；如此可以有效率地讓專用網路擁有寬廣的位址空間。此外，若使用 NAT，則專用網路中的位址就會被隱藏起來，不會被外界看到，進而提供多一層的安全性。

第121頁的圖 31 以圖示說明 IBM Firewall 環境中的基本 NAT 作業。

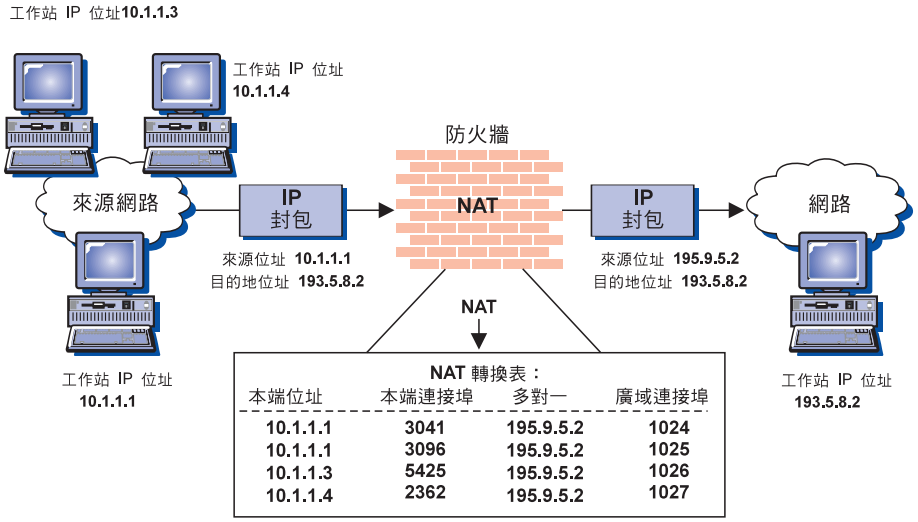

圖 31. 網路位址轉換

安全主電腦所產生的 TCP/UDP 封包會將其來源位址替換爲已登記的 Internet 位址。安全主電腦的連接埠會被轉換爲專有的埠號。所有離埠的封包都會有相同的來源位址，但是有專有的埠號。這種形式的轉換稱爲 Many-to-one 轉換，可讓許多安全主電腦隱藏在單一的位址後面。 IP 表頭及 TCP/UDP pseudo 表頭中之封包的總數都已更新。並行連線的最大限制數爲 64536 (實際爲 64512)，因爲已保留連接埠 0-1023。入埠連線是由靜態 (而不是動態)

轉換表格項目所支援。例如，只有當靜態項目存在於 NAT 轉換表格 (195.9.5.2 對映至 10.1.1.1) 時，主電腦 193.5.8.2 才可以用主電腦 10.1.1.1 (使用全球位址 195.9.5.2) 來起始 TCP 連線。

所有由 TCP/UDP 應用程式所產生的封包都可以被轉換。如果 IP 封包所包含的應用程式資料包含 IP 位址的話，就會發生困難。位址轉換其中一種麻煩的應用程式，就是 FTP。 FTP 控制連線會發出 ″PORT″ 命令或 ″PASV″ 回應，會將以 ascii 編碼的 IP 位址包含在郵件中。在此案例中，NAT 不只需要修改 IP 表頭中的位址，而且也要修改資料欄中的 ascii 位址及埠號。

在即將出版的 APAR 版次中， NAT 的 Many-to-one 及 MAP 轉換選項將可讓入埠及離埠的 ICMP 封包接受轉換。只有當現存的轉換表格項目發生重新導向的異常狀況時，入埠的 ICMP 回應封包 (ping、時間標記、位址遮罩) 及所有錯誤封包 (無法連繫的目的地、來源抑制、重新導向、超出時限及錯誤的封包訊息) 才能被轉換。 ICMP 重新導向會通過 NAT，而不被轉換。它會根據您的過濾規則來決定要允許或拒絕 ICMP 重新導向。

離埠的查詢/回應 ICMP 封包 (ping 查詢/回應、時間標記查詢/回應、位址遮罩要求回應) 是經由轉換封包的安全位址及 ICMP 查詢識別碼而支援的，如此一來，來自不同安全主電腦的 ICMP 封包就可以共用單一的已登記位址。

當「管理者」讓某些 ICMP 封包 (尤其是位址遮罩/回應及重新導向) 在安全及非安全性網路之間傳輸時，必須非常小心。讓 ICMP 資料傳輸通過 Firewall 時的安全性威脅相關資訊，請參閱下面的紅冊子 (列在參考書目中)，書名爲： *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*。

IBM eNetwork Firewall NAT 執行

IBM Firewall NAT 執行支援基本的位址轉換 (如上述說明)，請注意下列警告事項：

- 在資料欄中有包含 IP 位址資訊的 TCP/UDP 應用程式 (以下所描述的 FTP 除外) 只會讓封包表頭欄位轉換爲上述的情形。意即，UDP 應用程式 (如 DNS 或 SNMP) 將不會轉換資料欄所包含的位址資訊。
- FTP PORT 命令整個都被轉換了，但是並沒有轉換 PASV 回應封包中所包含的位址。
- ICMP 要求/回應及加密訊息都會被轉換。例如，這樣可以讓離埠的 ping 及 TCP 路徑 MTU 偵測正確地操作。
- NAT 不會偵測 TCP 的斷線狀況，但是在將動態轉換表格移除，並且將已登記的 IP 位址插回可用位址的儲存區之前，會較依賴可架構的閒置逾時設定。

NAT、過濾器及通道之間的互動範例

第123頁的圖 32 以圖例說明 NAT、過濾器及通道之間的互動範例。

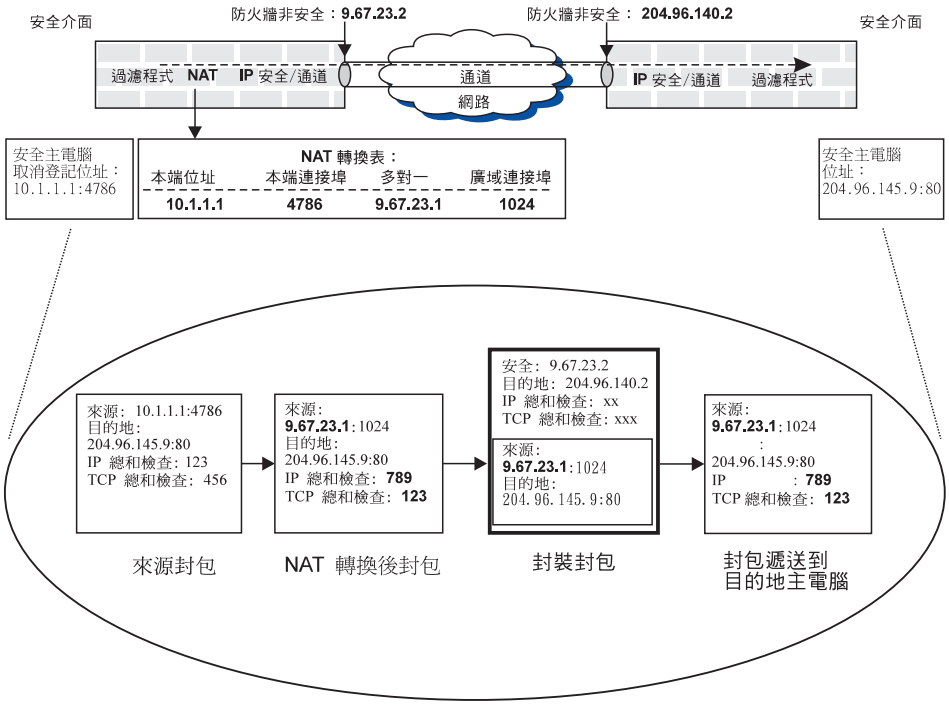

圖 32. NAT、過濾器及通道之間的互動範例

假設您是在防火牆 9.67.23.2 及 204.96.140.2 之間以手動的方式建立 IPSec ESP 通道。則 NAT 只能在 9.67.23.2 防火牆作用，因爲這個安全網路是使用專用位址。而通道另一端的安全網路並不是使用 NAT。除了以圖例說明基本的 NAT 轉換 (左邊第二個封包中的粗體欄位是在離埠位址轉換期間，封包中已修改的欄位) 之外， 第123頁的圖 32 也以圖例表示從主電腦轉換過來的封包裝入*尚未*轉換之 IP 封包中的例子。

一般而言，過濾處理會先應用在離埠封包，然後才用在 NAT，並且會在 NAT 轉換之後才應用到入埠封包。因此，過濾規則是以未轉換的位址爲依據。當牽涉到 NAT 及通道時，已啓用 NAT 之防火牆上的過濾規則也是以未轉換的位址爲依據。在通道的另一端 (假設 NAT 不在此防火牆上作用的情況下)，入埠封包的過濾規則是以已轉換過的來源及目的地位址爲依據 (針對入埠及離埠而有所分別)。如果通道兩端都有啓用 NAT 的話，則上述的說明即可同時應用在二個方向上。

使用第123頁的圖 32 的設計爲範例，並且假設其目的是要讓安全主電腦 10.1.1.1 透過通道來與安全主電腦 204.96.145.9 進行通信，則與 10.1.1.1 連接的防火牆就必須要有一個過濾規則，以讓 10.1.1.1 能夠透過通道來與 204.96.145.9 通信。在另一個與目的地主電腦連線的防火牆上，必須要有一個過濾規則，以透過通道在 9.67.23.1 及 204.96.145.9 之間進行通信。

NAT 的其它資訊

若您想允許下列作業，請使用 NAT：

- 在保護該安全機器的位址的情況下，允許防火牆後的機器的直接存取非安全站台。
- 讓某些沒有登記位址的機器能夠共用已登記的位址，以讓這些機器能夠連線到 Internet 上的站台。
- 讓其它來自非安全位置的機器能夠存取防火牆後的伺服器。

向您的 ISP 取得 NAT 所要使用的登記位址。所有供 NAT 使用的位址都不能供其它用途使用。

NAT 的選項有四：

Many-to-one
透過轉換封包的安全位址及埠號，可以讓許多 (最多 65536) 內部位址共用一個已登記的 IP 位址。這個供多者共用的已登記 IP 位址會將本端位址隱藏起來，但除了此 IP 位址之外，您必須要有另一個 Internet 登記位址，以供 Firewall 的非安全位址使用。 NAT 架構會利用 Many-to-one 項目來識別用以從事連接埠轉換的 Internet 登記位址。

轉換 用來建立要轉換之安全位址的列示。

排除 用來建立不要轉換之安全位址的列示。

對映 用來保留特定安全位址的特定登記位址。

使用「架構從屬站」來架構「網路位址轉換」

1. 從架構從屬站導覽樹狀結構中，連按兩下「位址轉換」檔案資料夾圖記，以展開檢視畫面。連按兩下 NAT 檔案資料夾圖記以展開檢視畫面。
2. 選取 **NAT 設定**來架構「網路位址轉換」模組。

   網路位址轉換列示出現，如第125頁的圖 33 所示。

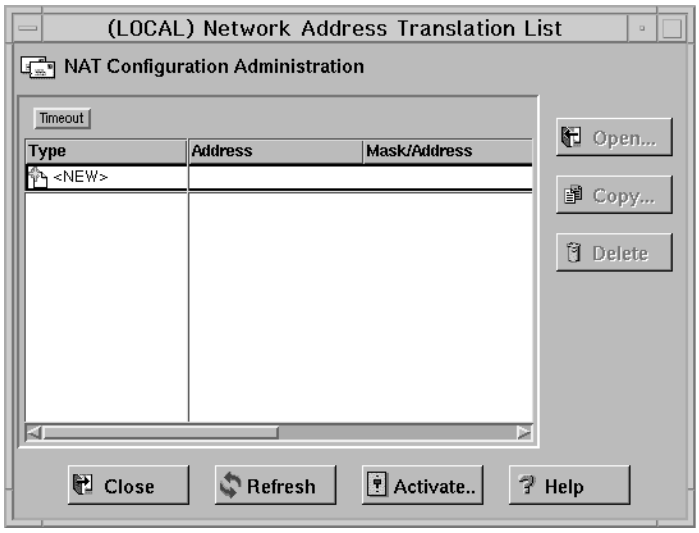

圖 33. 網路位址轉換列示

3. NAT 架構檔中所包含的「網路位址轉換」項目都顯示在此對話框上。您也可以新增、變更或刪除 NAT 項目。

新增 NAT 項目

1. 從**網路位址轉換列示**選取**新增**，並按一下**開啓**，以將新的項目新增至 NAT 架構檔。

   新增 NAT 對話框即出現。
2. 在**新增 NAT** 對話框中，按一下「NAT 類型」欄位中的箭號，並從下列項目中選取：
   - Many-to-one 網路登記位址：將所指定的 IP 位址新增至保留的 IP 位址。參數爲保留的 IP 位址及與轉換表格相關的逾時設定。
   - 轉換安全網路位址：指定一個需要網路位址轉換的安全 IP 位址範圍。
   - 排除安全網路位址：指定一個要從網路位址轉換排除的安全 IP 位址範圍。
   - 對映安全網路位址：定義一對一的安全對登記 IP 位址靜態轉換。

Many-to-one 網路登記位址

Many-to-one 登記位址項目可轉換封包的安全位址及埠號，可以讓許多 (最多 65536) 內部位址共用一個已登記的 IP 位址。 此功能可讓您用一個已登記的 IP 位址來隱藏許多本端位址。 (您必須要有另一個 Internet 登記位址來供防火牆的非安全位址使用。)

當一個安全主電腦將封包傳送到非安全性網路時，就會配置一個 IP 登記位址。此獨一的 IP 登記位址是用來在 IBM Firewall 及安全網路外的機器之間傳輸 IP 框架。

如果您從「新增 NAT」畫面選取 Many-to-one，請輸入下列值：

已登記的 IP 位址

向您的 ISP 取得此位址。此位址將會是帶點十進位數的 IP 位址，而此 IP 位址的所有安全位址都會被隱藏起來。

按一下**選取**來取得**選取網路物件**對話框，即可選擇網路物件。選取一個網路物件，並按一下**確定**。網路物件會新增至**新增 NAT 架構**對話框上的「網路物件」欄位中。或者，如果您先前沒有建立網路物件，您可以直接將值鍵入該欄位。

逾時值 輸入分鐘數 (在 NAT 能夠釋放 IP 登記位址之前，位址轉換可以維持在閒置狀態的分鐘數)。此逾時值只能應用在位址轉換，此位址轉換使用這個項目所指定之 IP 位址範圍中的 IP 登記位址。

預設值爲 15 分鐘。逾時值的範圍爲 5 至 45。

轉換安全網路位址

轉換安全 IP 位址項目可定義需要用 NAT 來執行 IP 位址轉換的一組安全網路位址。 在預設的狀況下，NAT 會在轉換安全 IP 位址組中的所有安全 IP 位址上執行位址轉換。

如果您從「新增 NAT」畫面選取「轉換」，請輸入下列值：

安全 IP 位址

指定一個可識別需要網路位址轉換之安全 IP 位址範圍的帶點十進位數 IP 位址。

按一下**選取**來取得**選取網路物件**對話框，即可選擇網路物件。選取一個網路物件，並按一下**確定**。網路物件會新增至**新增 NAT 架構**對話框上的「網路物件」欄位中。或者，如果您先前沒有建立網路物件，您可以直接將值鍵入該欄位。

安全 IP 位址遮罩

指定一個遮罩，例如子網路遮罩，可指定用來識別 IP 位址範圍的安全 IP 位址中的位元。在這些遮罩中，若將位元設定爲 0，表示有 0 或 1 的位元位置都包含在 IP 位址的範圍中。因此，在遮罩中指定 255.255.255.255 即表示此轉換項目中只包含一個安全 IP 位址，而 255.255.255.0 的遮罩即表示類別 C IP 位址需要位址轉換。

排除安全網路位址

排除安全 IP 位址項目可定義不須用 NAT 來執行 IP 位址轉換的一組安全網路位址。 在預設的狀況下，NAT 會在轉換安全 IP 位址組中的所有安全 IP 位址上執行位址轉換。

如果您是從**新增 NAT** 對話螢幕來選取「排除」的話，請輸入下列值：

安全 IP 位址

指定一個可識別應排除在網路位址轉換外之安全 IP 位址範圍的帶點十進位數 IP 位址。

按一下**選取**來取得**選取網路物件**對話框，即可選擇網路物件。選取一個網路物件，並按一下**確定**。網路物件會新增至**新增 NAT 架構**對話框上的「網路物件」欄位中。或者，如果您先前沒有建立網路物件，您可以直接將值鍵入該欄位。

安全 IP 位址遮罩
指定一個遮罩，例如子網路遮罩，可指定用來識別 IP 位址範圍的安全 IP 位址中的位元。在這些遮罩中，若將位元設定爲 0，表示有 0 或 1 的位元位置都包含在 IP 位址的範圍中。因此，在遮罩中指定 255.255.255.255 即表示此項目中只有指定一個安全 IP 位址，而 255.255.255.0 的遮罩則表示將類別 C IP 位址排除在位址轉換之外。

對映安全網路位址

對映安全 IP 位址項目可定義從安全 IP 位址到 IP 登記位址的一對一對映。 此一對一 IP 位址對映可讓外部應用程式從屬站 (如：FTP 或 telnet 從屬站) 用位在安全網路中的伺服器機器來設定 TCP 階段作業。在對映安全 IP 位址項目中的 IP 登記位址，可與由保留的 IP 登記位址項目所指定的 IP 位址空間一致。

如果您已從**新增 NAT 架構**對話框中選取「對映」，請輸入下列值：

安全 IP 位址
應轉換爲所指定之 IP 登記位址的帶點十進位數 IP 位址。

按一下**選取**來取得**選取網路物件**對話框，即可選擇網路物件。選取一個網路物件，並按一下**確定**。網路物件會新增至**新增 NAT 架構**對話框上的「網路物件」欄位中。 或者，如果您先前沒有建立網路物件，您可以直接將值鍵入該欄位。

「IP 登記位址」欄位
指定的安全 IP 位址所應轉換而成的帶點十進位數 IP 位址。

您可以按一下**選取**來取得**選取網路物件**對話框，即可選擇網路物件。選取一個網路物件，並按一下**確定**。網路物件會新增至**新增 NAT 架構**對話框上的「網路物件」欄位中。

變更 NAT 項目

從 **NAT 架構**對話框選取現存的 NAT 項目，按一下**開啓**來變更 NAT 架構檔中的「網路轉換」項目。

刪除 NAT 項目

1. 從 **NAT 架構**對話框選取現存的 NAT 項目，按一下**刪除**，從 NAT 架構檔移除「網路轉換」項目。

   出現確認對話框。

2. 選取「是」或「否」。

NAT 啓動

1. 從架構從屬站導覽樹狀結構中，連按兩下「位址轉換」檔案資料夾圖記，以展開檢視畫面。連按兩下 NAT 檔案資料夾圖記以展開檢視畫面。
2. 選取 **NAT 啓動**，即出現一個類似第128頁的圖 34 中所顯示的對話框。

圖 34. NAT 啓動

3. 您可以選取下列任一項，然後再按一下**執行**：
   - 驗證所指定之 NAT 架構檔中所包含的網路位址轉換項目。

- 啓動/更新架構，以顯示 NAT 模組目前所使用的「網路位址轉換」項目。
- 停止 NAT 以停用網路位址轉換。
- 啓用「記載」來啓用網路位址轉換記載。
- 停用「記載」來停用網路位址轉換記載。

記載

在 NAT 記載及過濾處理記載都已啓用的情況下，NAT 會記載各種錯誤狀況。 NAT 記載是透過 **NAT 啓動**畫面或是用 **fwnat** 命令來啓用的。過濾處理記載是藉由**日誌機能**畫面或是用 **fwlog** 命令來啓用的。

下列活動都將記載在防火牆日誌機能：

- 由「管理者」更新 NAT 表格 (例如，靜態或 MAP 項目)
- 動態更新 NAT 轉換表格
- 錯誤訊息
- 失敗的轉換嘗試，導致封包被捨棄。
- 啓動及停止 NAT 的每個時間

建立 NAT 的過濾規則

在您完成 NAT 架構後，您必須爲即將使用 NAT 的連線建立過濾規則。檢閱第47頁的『第8章 透過防火牆控制資料傳輸』及使用要用來直接連線的預先定義的服務程式。要用來直接連線之預先定義的服務程式的範例，如下所示：

- HTTP 直接離埠
- Telnet 直接離埠

相關資訊，請參閱第48頁的『使用預先定義的服務程式建立連線』。

如果您要讓服務程式直接進入您的網路，您就必須建立一個服務程式。如何做的相關資訊，請參閱第69頁的『使用架構從屬站來建立服務程式』。

附錄. 注意事項

本書在提及一些 IBM 產品、程式或服務時，不暗示 IBM 會在有業務營運的所有國家發行這些產品、程式或服務。在提及 IBM 產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。只要不侵害到 IBM 智慧財產權或其他受到法律保護的權利，凡是功能相等的產品、程式或服務程式，都可以代替 IBM 產品、程式或服務程式。其他產品在運作上的評價與驗證，除非 IBM 特別指示，其責任屬於使用者。

本文件所涵蓋的主要項目，IBM 已有專利或正在申請專利。使用者不享有本書內容之專利權。 關於軟體授權若有任何問題，請以書面方式寄到：

台北市基隆路一段 206 號

台灣國際商業機器股份有限公司

法務部

本程式的合法使用者若想要 (i) 在獨立建立的程式和其它程式 (包括本程式) 之間交換資訊，以及 (ii) 共同使用交換的資訊，請連絡：

台北市基隆路一段 206 號
台灣國際商業機器股份有限公司

上述資訊需要在適當的條件和狀況下才可取得，包括可能需要付費。

本文件所描述的特許程式及其所有可用的特許資料，是由 IBM 根據「IBM 客戶契約」的條款規定而提供的。

本文件不專供生產使用且不提供任何保證，包括銷售性保證及特定用途的適用性。

這個產品包含由加洲大學柏克萊分校及其贊助者共同發展的軟體。

登記商標

下列詞彙是 IBM 公司在美國或其它國家，或兩者所使用的登記商標：

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Microsoft、Windows、Windows NT 以及 Windows 95 標誌是 Microsoft Corporation 的商標或登記商標。

Java 和 HotJava 是 Sun Microsystems, Inc. 的商標。

用雙星號 (**) 表示的其它公司、產品及服務程式名稱，可能是其它公司的商標或服務標記。

參考書目

請造訪 IBM eNetwork Firewall 首頁，以取得 Internet 安全性的相關資訊：
http://www.software.ibm.com.enetwork/firewall。

IBM 出版品中的資訊

有關防火牆、Internet 安全性及一般安全性主題的其它 IBM 資訊來源都列在這裡。

防火牆主題

下列文件可在 IBM Firewall CD-ROM 及 IBM eNetwork Firewall 首頁上取得。

- *IBM eNetwork Firewall 使用指南*, GC40-0213
- *IBM eNetwork Firewall 參考手冊*, SC40-0214
- *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*, SG24-5209

Internet 及全球通訊網 (World Wide Web) 主題

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

一般安全性主題

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

企業出版品中的資訊

這些企業出版品均與 TCP/IP 及 UNIX 有關：

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

這些企業出版品是有關防火牆及 Internet 安全性方面的資訊：

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

名詞解釋

您可以在下列網址上存取 IBM Software 名詞解釋：
http://www.networking.ibm.com/nsg/nsgmain.htm。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔十劃〕

〔十一劃〕

〔十二劃〕

〔十三劃〕

〔十四劃〕

〔十五劃〕

〔十六劃〕

〔十七劃〕

讀者意見表

IBM eNetwork Firewall for Windows NT
使用指南
版本 3 版次 2.1.1

GC40-0213-01

名稱

地址

公司或組織

電話號碼

讀者意見表
GC40-0213-01

撕開或折起
沿線

折疊並封上　　**請勿用釘書針釘上**　　折疊並封上

將
郵
票
貼在此

IBM Corporation
Information Development
Department CGMD / Bldg 500
P.O. Box 12195
Research Triangle Park, NC
27709-9990

折疊並封上　　**請勿用釘書針釘上**　　折疊並封上

GC40-0213-01

撕開或折起
沿線

Printed in Australia

GC40-0213-01