IBM SecureWay® Boundary Server for Windows NT® and AIX

啓動與執行

版本 2.0

IBM SecureWay® Boundary Server for Windows NT® and AIX

啓動與執行

版本 2.0

備註

使用本資訊及其支援的產品之前，請先閱讀第41頁的『附錄B. 注意事項』下的一般資訊。

本修訂版適用於 IBM SecureWay Boundary Server 產品版本 2 版次 0 修訂層次 0，與所有後續版次，直到新修訂版中另有指示爲止。

第二版 （1999 年 10 月）

目錄

關於本書 v
本書的適用對象 v
2000 年的因應. v
服務與支援. v
本書的結構. v
慣例. vi
Web 資訊 vi
有何新功能？. vi
與 SecureWay Policy Director 整合. . . . vi
遞送效率 vii
侵入封鎖 vii
IBM SecureWay Firewall 4.1 版 vii
MIMEsweeper 2.0 for SecureWay ix
SurfinGate 4.05 x

第1章 SecureWay Boundary Server 概觀 . 1
典型的 SecureWay Boundary Server 範例 . . . 1

第2章 IBM SecureWay Boundary Server 簡介. 5
什麼是 SecureWay Boundary Server？ 5
爲何我需要 SecureWay Boundary Server？ . . 5
SecureWay Boundary Server 如何整合到 FirstSecure？ 6
SecureWay Boundary Server 有哪些元件？ . . 6
IBM SecureWay Boundary Server 概觀. . . 6
IBM SecureWay Policy Director 概觀 . . . 7
IBM SecureWay Firewall 概觀 7
MIMEsweeper 概觀 7
SurfinGate 概觀 8

第3章 在安裝 SecureWay Boundary Server 之前 11
如何準備？ 11
與 SecureWay Policy Director 整合 . . . 11
SecureWay Firewall 11
SecureWay Boundary Server 13
SurfinGate 13
MIMEsweeper. 14

第4章 IBM SecureWay Boundary Server （SBS） 基本要求 15
SecureWay Boundary Server 硬體基本條件 . . 15
SecureWay Boundary Server 軟體基本要求 . . 16

第5章 安裝及架構 SecureWay Boundary Server. 19
安裝 SecureWay Boundary Server 元件 . . . 19
安裝 SecureWay Firewall 19
安裝 SecureWay Directory 19
安裝 SecureWay Policy Director. 19
安裝 SecureWay Boundary Server 19
安裝 SurfinGate 20
安裝 MIMEsweeper. 20
架構 SecureWay Boundary Server 元件 . . . 21
架構 SecureWay Firewall 21
架構 SecureWay Firewall 進行 Policy Director 整合. 22
架構 SecureWay Firewall 使用 SurfinGate Plugin（僅限 Windows NT） 23
架構 SecureWay Firewall 使用 MAILsweeper. 24
架構 SecureWay Policy Director. 24
架構 SecureWay Directory 25
架構 SecureWay Boundary Server 進行 Policy Director 整合 25
架構 SecureWay Boundary Server 啓用 SurfinGate Plugin （僅限 Windows NT） . 26
架構 SurfinGate 26
架構 MIMEsweeper. 28
侵入封鎖 29
測試您的配置. 32

第6章 相關的文件 33
IBM SecureWay FirstSecure 33
IBM SecureWay Firewall 33
MIMEsweeper. 33
MAILsweeper. 33
WEBsweeper 34
WEBsweeper HTTPS Proxy 34
SurfinGate 34

附錄A. 疑難排解 35

解決 IBM SecureWay Firewall 的一般問題 . . 35
遞送問題 35
DNS 失效. 37
解決一般問題-MIMEsweeper 37
WEBsweeper 及 MAILsweeper 好像無法在相同的機器上使用 37
WEBsweeper 速度很慢. 38
WEBsweeper 授權問題. 38
WEBsweeper 下載大型檔案時發生問題 . . 38
解決一般問題--SurfinGate 38
SurfinConsole 在開啓 Microsoft Internet Explorer 後停止回應 38
SurfinGate Plugin 速度緩慢 39

附錄B. 注意事項 41
商標. 42

名詞解釋 43

讀者意見表 47

關於本書

本書說明如何規劃 IBM SecureWay®Boundary Server for Windows NT® and AIX 的安裝、配置、使用與疑難排解。

極重要的一件事是，在開始安裝及架構 SecureWay Boundary Server 之前，您需要具備有關防火牆、虛擬專用網路、內容安全及網路管理方面的充分知識。因爲將要設定及架構用來控制網路進出存取的防火牆，您必須先瞭解網路如何運作。您尤其需要瞭解有關 IP 位址、完整的名稱及子網路遮罩的基本知識。

本書的適用對象

本書旨在針對負責安裝、管理及使用 IBM SecureWay Boundary Sever 的網路或系統安全管理者提供參考。

2000 年的因應

這些產品皆已做好 2000 年的因應。當您根據這些產品的相關文件來使用它們，只要這些產品的相關產品（例如，硬體、軟體與韌體）與它們之間能適當交換精確的日期資料，則在 20 世紀與 21 世紀間，這些產品亦能正確處理、提供與接收日期資料。

服務與支援

如要取得 IBM SecureWay FirstSecure 產品中所有產品的服務與支援，請聯絡 IBM。 這些產品中有些可能會參照非 IBM 支援。 如果您是從 FirstSecure 售品中取得這些產品，相關服務與支援請聯絡 IBM。

本書的結構

本書包含以下各章：

- 第1頁的『第1章 SecureWay Boundary Server 概觀』提供 SecureWay Boundary Server 及其元件的概觀。
- 第5頁的『第2章 IBM SecureWay Boundary Server 簡介』提供有關爲何需要使用 SecureWay Boundary Server 的資訊。
- 第19頁的『第5章 安裝及架構 SecureWay Boundary Server』說明在 Windows NT 及 AIX 作業系統上安裝及配置 SecureWay Boundary Server。

- 第11頁的『第3章 在安裝 SecureWay Boundary Server 之前』提供有關如何規劃 SecureWay Boundary Server 的資訊。
- 第15頁的『第4章 IBM SecureWay Boundary Server （SBS） 基本要求』提供有關 SecureWay Boundary Server 的最基本要求資訊。
- 第33頁的『第6章 相關的文件』說明到哪裡取得 SecureWay Boundary Server 的其它文件及相關產品的文件。

慣例

本書使用下列慣例：

慣例	意義
粗體	使用者介面元素，如勾選框、按鈕及指令
等寬字體	與 SecureWay Boundary Server 相關的語法及目錄預設值
->	顯示功能表中一系列的選項。例如：選取**檔案-> 執行**表示按一下**檔案**，然後按一下**執行**

Web 資訊

有關 SecureWay Boundary Server 的最新更新資訊可在以下網址取得：

http://www.ibm.com/software/security/boundary/library

有關其它 IBM SecureWay FirstSecure 產品的更新資訊，請造訪下列網址：

http: //www.ibm.com/software/security/firstsecure/library

有何新功能？

SecureWay Boundary Server 版本 2.0 包含一些新的特性。最有意義的新特性列出如下。

與 SecureWay Policy Director 整合

如果 Firewall 啓用 SecureWay Boundary Server，則 SecureWay Policy Director 可管理 Firewall Proxy 使用者。下列 Firewall 服務來定義 Firewall Proxy 使用者：

- Telnet
- FTP
- HTTP

- Socks

使用者及其相關的政策都儲存在「輕裝備目錄存取通訊協定」（LDAP）資料庫中。

SecureWay Directory 提供 LDAP 方法，可在一個集中位置維護目錄資訊，以便執行儲存、更新、擷取及交換作業。 SecureWay Policy Director 會管理在 LDAP 資料庫中的 Firewall proxy 使用者。

遞送效率

遞送效率使用 Finjan SurfinGate plugin，以縮減內容過濾的電路網路流量。

侵入封鎖

指令行程式，用來在 Firewall 上建立動態 DENY 規則。入侵封鎖可以整合至自動化的 script 中。

IBM SecureWay Firewall 4.1 版

IBM SecureWay Firewall for Windows NT 版提供：

遠端存取服務

Windows NT Remote Access Service（RAS）使用點對點通信協定（PPP）透過撥號式、ISDN 或 X.25 媒體提供網路連接。 NDISWAN 是網路驅動程式，提供作爲 RAS 的一部份，可將基礎 PPP 資料轉換爲類似乙太區域網路資料。

IBM SecureWay Firewall Enhancements for AIX 4.1 版

IBM SecureWay Firewall for AIX 提供：

強化的 IPSec 支援

IBM SecureWay Firewall 4.1 版包括已強化的 IPSec 支援，涵蓋三重 DES 加密，及支援新標頭。它也支援和多種 IBM 伺服器及路由器，及許多支援新標頭的非 IBM VPN 產品之間的交互作業能力。

對稱多重處理器 （SMP）

防火牆的使用者可以運用 RS/6000 的多重處理器特性，增進調整能力與效能。

增強過濾程式

已經加強過濾程式，以便透過配置提供更好的效能。您可以選擇要從哪裡尋找不同的過濾規則類型，藉此調整 Firewall 的效能。此外，也會記錄使用連接的次數。

安裝精靈

精靈會輔助進行 IBM SecureWay Firewall 的起始配置。此安裝精靈讓新使用者在安裝好 IBM Firewall 之後，即可快速設定一套基本的 Firewall 配置並開始執行。

網路安全稽核程式

「網路安全稽核程式」（NSA） 會檢查您的網路伺服器及 Firewall，察看有無安全漏洞或配置錯誤。此功能已強化，變得更快速並且更強大。

德文國際語言支援

國際語言支援現在增加了德文，原有的語言包括：巴西葡萄牙文、葡萄牙文、英文、法文、義大利文、日文、韓文、簡體中文、西班牙文及繁體中文。

網址轉換

網址轉換 （NAT） 已強化爲支援多對一位址映射。這些映射是從多個內部未登錄或專用位址，對映至已登錄的合法位址，它使用埠號建立唯一的映射。

AIX 及 Windows NT 版支援的共同功能

Security Dynamics ACE/Server

Security Dynamics ACE/Server 提供兩種鑑別因素。此特性已經過強化，並且可保護您的網路與資料資源免於遭受可能會造成破壞的意外或惡意入侵。

增強 Secure Mail Proxy

IBM Firewall Secure Mail Proxy 已經過強化，目前包括下列新功能：

- 防止 SPAM 演算法，包括封鎖來自已知散播 SPAM 者的訊息（除外清單）、針對訊息有效性與可靠度的驗證檢查（封鎖不受歡迎訊息的已知方法）、可配置每則郵件訊息的接收人數限制、可配置每則訊息的大小限制
- 反詐騙支援，包括與強大的鑑別機制整合
- SNMP 設陷支援及支援 MADMAN MIB
- 訊息追蹤，包括密切追蹤防火牆及 Domino 之間的訊息

增強 Socks Protocol Version 5

Socks Protocol Version 5 已經升級爲包括使用者 ID-密碼鑑別（UNPW）、檢核回應鑑別 （CRAM） 及鑑別 plug-in。

日誌記載已強化，提供使用者進一步控制，使用者可以將日誌訊息分類及指定日誌記載層次。

HTTP Proxy

IBM SecureWay Firewall 以 IBM Web Traffic Express （WTE）產品爲基礎，提供一套功能完整的 HTTP proxy 施行方法。 HTTP proxy 透過 IBM Firewall 有效率地處理瀏覽器要求，而不必在 Web 瀏覽作業中使用 socks 伺服器。使用者可以存取網際網路上的有用資訊，而不需要在其內部網路的安全上妥協。瀏覽器必須架構爲使用 HTTP proxy。

MIMEsweeper 2.0 for SecureWay

MIMEsweeper 具有三個主要元件：**MAILsweeper 4.1_2**、**WEBsweeper 3.2_5** 及 **WEBsweeper 1.0_2**。其中的某些增強項目包括：

MAILsweeper

MAILsweeper 4.1_2 for SMTP 是對 Content Technologies 旗艦 MIMEsweeper 產品的一大升級技術。它提供下列新特性：

- 容易使用的階層式政策架構，能彈性地將適當組織層級的政策架構套用到個別的使用者。
- 備有業界標準的圖形式使用者介面 （GUI），簡化軟體配置、政策建立及管理等程序。
- 新的「分割遞送」特性是版本 4 的階層式政策施行功能之一，對於具有多位接收者的訊息，可針對每一個接受者引用不同政策。獲授權的接收者可接收到訊息，未獲授權的接收者則被拒絕。
- 多執行緒訊息處理程序改進產量並增進強韌性，其方法是，如果有一或多個執行緒發生錯誤時，則使用剩餘的執行緒，讓訊息處理程序繼續進行。
- 和其它供應商的防毒產品連結，MAILsweeper 提供針對訊息與附件進行病毒偵測及清除。
- 使用 NEAR、AND、NOT 及 OR 表示式的先進文字分析方法，在根據訊息語法或在架構上建立有效廣泛的情節上，提供了極大彈性。
- 已強化的審核工具，可以傳送資料至任何 ODBC 相容資料庫
- 支援「即時黑名單」（RBL） 伺服器，列出已知會傳送垃圾電子郵件的網站。MAILsweeper 可以拒絕與此清單上的任何主電腦的連線
- 透過吸引人的電子郵件流量報告/圖形/圖表形式，使內容安全性更容易管理
- 與 LDAP 目錄整合
- 「遞送服務通知」（DSN） 現在可支援 SNMP 及 NT 警示器

WEBsweeper

- 附加的效能增強，改進資料處理速度。
- 使用 HTTP 及 FTP 流量的「病毒掃描器」

WEBsweeper HTTPS

- WEBsweeper 現在透過新的 HTTPS proxy 解決方案，完整支援 web 型電子商務應用程式

SurfinGate 4.05

SurfinGate 的增強功能包括：

JavaScript 內容檢驗

SurfinGate 4.05 會尋找潛在的問題 JavaScript 作業，並會停止和企業安全政策相衝突的 JavaScript。 SurfinGate 4.05 讓管理者可集中設定及實施對 JavaScript、Java 及 ActiveX 的政策，以智慧型過濾程序過濾 VisualBasic Script 與 cookies。

攸關任務的效能監督程式

SurfinGate 4.05 包括一個自動工具，可偵測不正常的行爲（如執行時間錯誤），並可在失效時重新啓動 SurfinGate。此爲攸關任務領域的必備安全特性。

改進政策管理

SurfinGate 會將無法分辨的 applet 設定檔輸入資料庫，以進行自動封鎖。管理者可以編輯 applet/control 清單。

支援 FTP 及 SSL 通信協定

SurfinGate 4.05 會監視檔案轉送通信協定 （FTP） 通道中的機動程式碼，持續查看可能會從網際網路潛入的程式碼。除了 FTP 外，SurfinGate 也監視 HTTP 流量中的機動程式碼，並傳遞 HTTPS 流量至附加的裝置。

Plugin 與防火牆 HTTP proxy 整合

SurfinGate 會擔任 proxy 鏈結中的一個 proxy ，或透過 Firewall for Windows NT 上 Web Traffic Express 中的 plugin來運作。

第1章 SecureWay Boundary Server 概觀

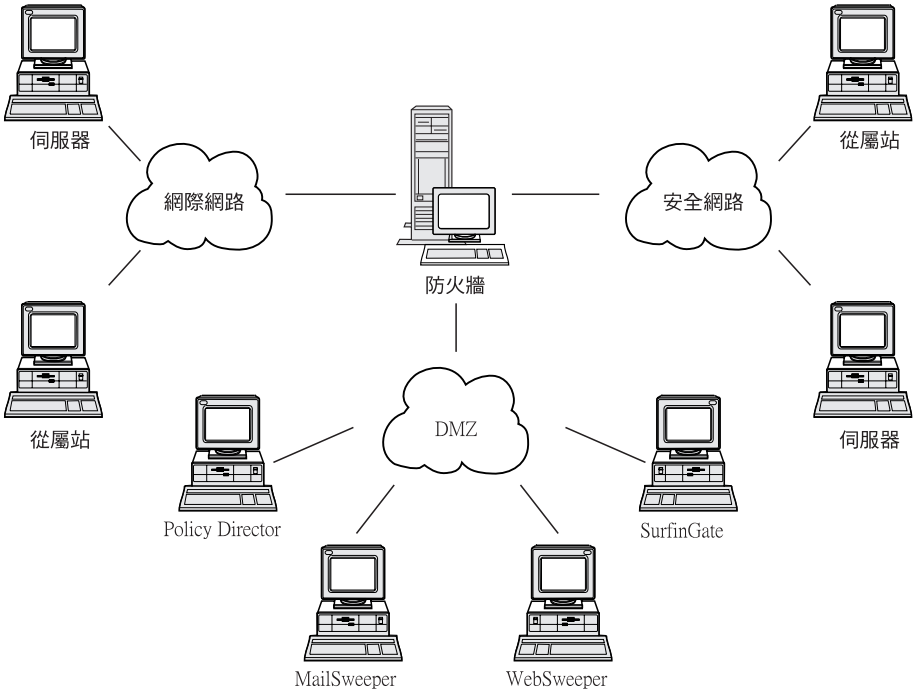

圖 1. IBM SecureWay Boundary Server 配置範例

此範例圖解表示 5 台工作站，它們分別使用 MAILsweeper、WEBsweeper、 Policy Director 及 SurfinGate 元件，利用 Firewall 監視及遞送從屬站與伺服器之間的 web 流量與郵件。在此範例中，我們會使用 5 部實際上分開的工作站。

典型的 SecureWay Boundary Server 範例

我們建議您使用下列機器作爲基本設定：

表 1. Boundary Server 元件產品硬體基本條件

產品	機器
IBM Firewall	Windows NT 或 AIX
MAILsweeper	Windows NT

表 1. Boundary Server 元件產品硬體基本條件 (繼續)

WEBsweeper	Windows NT
SurfinGate	Windows NT

如果您希望充分運用 SecureWay Boundary Server 的優點，您的網路中必須有 SecureWay Policy Director。因爲如此可讓 Firewall proxy 使用者儲存在 SecureWay Directory （LDAP） 中。

HTTP 範例（Windows NT Firewall）： 在典型的情節中，在網際網路上 HTTP 內容的要求會來自用戶端機器。要求首先會流至 WEBsweeper。在出埠路徑上，該要求會由 WEBsweeper 虛擬至 Firewall HTTP proxy。

在 Firewall HTTP proxy 中，使用者會受到鑑別。如果這是來自從屬站瀏覽階段作業的第一個要求，就會呈現「使用者 ID/密碼檢核」。使用者會利用使用者 ID ，在由 Policy Director 管理的 LDAP 資料庫中查閱用戶端的安全政策。根據從屬站的 HTTP 鑑別政策，及檢查輸入的密碼之結果，該要求可能會被拒絕或允許繼續串流。鑑別作業可能需要進一步存取 LDAP 資料庫或 Security Dynamics ACE 伺服器。在從相同瀏覽階段作業的後續要求中，瀏覽器會自動提供該使用者 ID/密碼。從屬站不會再度被檢核，不過每一個要求仍要經過和第一個要求相同的鑑別處理。

如果鑑別順利完成，該要求會被虛擬至所要求的網際網路伺服器。

當來自網際網路伺服器的內容接收回 Firewall HTTP proxy 時，該內容會由 SurfinGate plugin 檢查。從 LDAP 資料庫取得的使用者群組資訊會提供給 plugin，作爲決策之用。如果內容中沒有包含 SurfinGate 要找的資訊，即可快速通過 plugin，其處理時間極短。包含 JavaScript 的內容會在 plugin 中過濾。包含 Java 或 ActiveX 的內容會被轉遞至 SurfinGate 伺服器進行過濾，而過濾過的內容會被傳回 Firewall HTTP proxy。由 SurfinGate plugin 處理過後的結果內容會被送回 WEBsweeper 伺服器。

當內容抵達 WEBsweeper 伺服器時，會根據 WEBsweeper 政策加以過濾，然後才傳回從屬站。

HTTP 範例（AIX Firewall）： 在 AIX 上，流量的流程也相同，不過在 AIX Firewall 上沒有 SurfinGate plugin 可用。因此，SurfinGate 伺服器必須設定成是從屬站至 Firewall 的 proxy 鏈結中的一個 proxy。 WEBsweeper 應設定爲轉遞要求至 SurfinGate 伺服器，而不是直接至 Firewall HTTP proxy。 SurfinGate 伺服器必須架構爲轉遞要求至 Firewall HTTP proxy。在 SurfinGate 伺服器上沒有群組資訊可用，因此決策只能根據 IP 位址。

郵件範例： MAILsweeper 設定成一個郵件閘道。抵達 MAILsweeper 伺服器的郵件，在被轉遞到下一個郵件伺服器之前，其內容會經過過濾。

必須將您的每一部安全郵件伺服器架構爲將從屬站郵件要求轉遞至 MAILsweeper 伺服器。必須將 Firewall 郵件交換程式必須架構爲將進入郵件轉遞至 MAILsweeper 伺服器。

必須將 MAILsweeper 架構爲將指定送往外部領域的郵件，傳送至 Firewall 郵件交換程式。必須將 MAILsweeper 架構爲將指定送往爲內部領域的郵件傳送至正確的安全郵件伺服器。

第2章 IBM SecureWay Boundary Server 簡介

本章提供 SecureWay Boundary Server 的概觀並且包括下列各節：

- 『什麼是 SecureWay Boundary Server？』
- 『爲何我需要 SecureWay Boundary Server？』
- 第6頁的『SecureWay Boundary Server 如何整合到 FirstSecure？』
- 第6頁的『SecureWay Boundary Server 有哪些元件？』

什麼是 SecureWay Boundary Server？

IBM SecureWay Boundary Server 首次將完整的界限安全解決方案整合在一起。SecureWay Boundary Server 提供防火牆保護、虛擬專用網路 VPN 及內容安全等功能。 SecureWay Boundary Server 將安全工業的技術集中在一套整合的解決方案中，並以 IBM 支援及服務做後盾。此解決方案包括：

- IBM SecureWay Firewall 4.1 （包括 Security Dynamic ACE/Server）
- 來自 Content Technologies 的 MIMEsweeper
  - MAILsweeper 4.1_2
  - WEBsweeper 3.2_5
  - WEBsweeper HTTPS proxy 1.0_2
- 來自 Finjan 的 SurfinGate 4.05
  - SurfinGate Server
  - SurfinConsole
  - SurfinGate 資料庫
  - SurfinGate Plugin for WTE integration for Windows NT 1.0

為何我需要 SecureWay Boundary Server？

到處都需要有安全界限--包括各部門之間，如工程和人力資源部門、總公司網路和遠端辦公室之間、您的公司網路和網際網路之間、您的公司 Web 應用程式和客戶之間，及您的公司網路和協力廠商之間。界限安全不只可以保護您的網路、應用程式及資訊，它也可以延伸其觸角範圍。適當的界限安全要求控制哪些人可以存取您的網路，及哪些資料進出您的網路。

SecureWay Boundary Server 如何整合到 FirstSecure？

IBM SecureWay FirstSecure 是一套整合的產品套件。它提供廣泛的組織架構，可協助您確保在網際網路及其它網路上所有網路功能的安全。它協助您以模組化、可交互操作的產品在您現有的投資上建立，並降低採行安全電子商業所需的總持有成本。它提供病毒保護、存取控制、流量內容控制、加密、數位式憑證、防火牆、工具集及實作服務。

Boundary Server 是可整合到 FirstSecure 內的產品套件。它建立與網際網路的界限，您可以使用此界限封鎖可能有害的病毒（使用連結的病毒掃描產品）、Java Script、Java Applet、ActiveX 控制，甚至包括垃圾電子郵件（SPAM）。透過 Boundary Server，您可以完全控制哪些資料可以從網際網路進入您的網路。經由 SecureWay Policy Director，您可以管理 Firewall proxy 使用者及其鑑別政策。

SecureWay Boundary Server 有哪些元件？

SecureWay Boundary Server 的三個元件包括 IBM Firewall、MIMEsweeper 及 SurfinGate。 SecureWay Boundary Server 提供和 IBM SecureWay Policy Director 整合。

IBM SecureWay Boundary Server 概觀

IBM SecureWay Boundary Server 對大型組織提供運用電子商業所需要的保護、存取控制及內容安全，它讓組織可以安全地對客戶、供應商與協力廠商開放其企業。其特性包括：

- 網路防火牆保護
- 虛擬專用網路（VPN），延伸網路觸角
- 電子郵件及 Web 流量內容掃描，保護您的公司的資料、影像及責任與生產力

SecureWay Boundary Server 將安全產業的最佳技術集中成一套整合的解決方案，並以 IBM 支援及服務作後盾。此產品包括 AIX 及 Windows NT 作業系統兩種版本。

SecureWay Boundary Server 的功能

SecureWay Boundary Server 引用封包過濾、proxy 及 socks 伺服器技術與內容安全，隱藏及保護您的網路系統。這些技術讓管理者可明確地定義哪些資料可進入及流出您的網路。此功能可協助防止「拒絕服務式的攻擊」及電腦駭客嘗試侵入網路，並且限制法律責任。 SecureWay Boundary Server 提供的 VPN 解決方案，可讓您以網際網路爲基礎的的解決方案，來取代遠端伺服器與數據中心。

SecureWay Boundary Server 若與 Policy Director 一起佈署時，可根據集中式政策計劃，來鑑別使用者。防毒軟體可以和 SecureWay Boundary Server 一起用來提供網站病毒保護。

IBM SecureWay Policy Director 概觀

Policy Director 是一套獨立式授權及安全管理解決方案，它能爲散佈各地的企業內網路及企業外網路提供端對端資源安全保護。企業外網路是一種虛擬專用網路（VPN），使用存取控制及安全特性，僅讓特定的用戶將企業內網路連接至網際網路。 Policy Director 提供鑑別、授權、資料安全及資源管理服務。 Policy Director 可和標準的網際網路型應用程式一起使用，建置安全及管理良好的企業內網路和企業間網路。

IBM SecureWay Policy Director 的功能

IBM SecureWay Policy Director 和 SecureWay Boundary Server 一起使用時，可提供用來儲存 proxy 使用者政策及鑑別資訊的儲存體。

IBM SecureWay Firewall 概觀

IBM SecureWay Firewall 是網路安全保護程式。防火牆是介於一或多個安全的內部專用網路及其它網路或網際網路之間的封鎖。防火牆可防止不受歡迎或未經授權的通信進出安全網路。

IBM SecureWay Firewall 的功能

IBM SecureWay Firewall 可限制受保護的網路、網際網路及其它網路集之間的存取作業。它也可以執行下列作業：

- 限制人員由妥善控制的點進入
- 防止攻擊者靠近其它防禦
- 限制人員由妥善控制的點離開
- 內部防火牆可將敏感的內部資訊與未獲授權的員工隔離
- 限制進出網路的流量

MIMEsweeper 概觀

MIMEsweeper 提供「內容安全檢查」功能，可分析經由電子郵件或全球資訊網流經 Firewall 的資料。「內容安全檢查」可讓企業有效地管理與使用電子郵件和全球資訊網相關的商業問題。這些問題可區分爲網路完整性及商業完整性。

網路完整性過濾可以：

- 識別並且移除進入及送出的電子郵件中的病毒
- 過濾不要的檔案類型

- 管理過大的檔案
- 防止因郵件炸彈攻擊導致的網路擁塞或服務流失

商業完整性過濾可以：

- 防止侵害機密及喪失商業機密
- 減少法律責任
- 降低因員工誤用電子郵件及全球資訊網造成的損失
- 防止因誤用及惡意攻擊造成的網路服務損失

對網路完整性的威脅，會毀損或消除資料、中止電子郵件的流通，並且損害系統硬體，這些都可能會造成網路故障、損失生產力及清理與回復成本過高。

對商業完整性所構成的威脅，則可能更具有破壞力，它會導致龐大的法律成本、損失智慧財產及商譽受損。商業完整性問題可能會使得您的商務運作停頓。

MIMEsweeper 是業界領先的安全產品，可以使組織不必面臨因使用電子郵件及網際網路，而衍生的網路與商業完整性問題。

MIMEsweeper 的功能

MIMEsweeper 可以：

- 在出埠郵件中加入法律的除外聲明
- 保護機密文件及資料
- 授權及控制電子郵件與 Web 使用者
- 隔離或封鎖攻擊性的資訊
- 封鎖垃圾電子郵件
- 掃描附件及下載檔案中是否包含不適當的內容
- 阻擋病毒及惡意的程式碼
- 封鎖不適當的網頁及網站
- 報告、記載及保存

SurfinGate 概觀

SurfinGate 4.05 是機動程式碼安全工具，專供以網際網路、企業外網路或企業內網路進行商業交易的任何企業使用。透過檢驗機動程式碼的內容，包括 JavaScript 在內，SurfinGate 有助於讓電腦網路免於惡意或無意的損壞，例如產業間諜、資料修改及資訊刪除等。 SurfinGate 的內容檢驗處理會在閘道層次和遠離重要資源之處，視察 Java、JavaScript 及 ActiveX 機動程式碼的內容，並指定唯一的 ID 與 Applet 安全設定檔 （ASP） 給程式碼、記下任何可能的安全侵犯事項。 SurfinGate 會在程式碼進入網路之前，識別潛在的問題程式碼。

SurfinGate 4.05 包括四個元件：

- SurfinGate Server
- SurfinConsole
- SurfinGate 資料庫
- SurfinGate Plugin for WTE integration for Windows NT

SurfinGate Server 功能如同 HTTP proxy 伺服器。 SurfinGate 可以和 Firewall HTTP proxy 及 WEBsweeper proxy 一起作爲 proxy 鏈結的一部份。如果是 Windows NT，它可以替代性地作爲 Firewall HTTP proxy 的 plugin。當作爲 plugin 使用時，SurfinGate 會爲提出要求的 proxy 使用者取得群組資訊。 SurfinGate 的過濾政策即可根據此群組資訊進行。此架構可在機動程式碼發生攻擊之前，先停止及視察機動程式碼流量。此元件可根據企業安全政策提供保護。

SurfinConsole 是一個親切的使用者介面，可用來管理及設定機動程式碼的中央企業安全政策。 SurfinConsole 可控制網路上的多部 SurfinGate Server，並且可根據個別使用者、個別群組，或透過自訂的不可接受與可接受程式碼清單，在整個公司內實施機動程式碼規則。

SurfinGate 資料庫中儲存 Applet 安全設定檔 （ASP） 的明細，包括有關使用者和群組及其對應的安全政策資訊。此資料庫可以使用內建的存取資料庫引擎，也可以使用現有的 Oracle 資料庫。由於 SurfinGate 會隨時視察所有機動程式碼的內容，因此並不需要這個資料庫來確保安全，不過它在大型作業中確實可增進效能。

SurfinGate 的功能

SurfinGate 提供：

- 對 Java applet、Active X controls、JavaScript 的閘道層次內容檢驗伺服器
- 即時監視、動態檢驗
- 針對以 Web 爲主的機動程式碼實施安全政策
- 檢驗「機動程式碼」（例如，Java applet、ActiveX control、JavaScript、Visual Basic script、plug-in、cookies）

SurfinGate 可和 proxy 鏈結中的 proxy 一起使用，或透過 Firewall for Windows NT 上的 WTE plugin來運作。

第3章 在安裝 SecureWay Boundary Server 之前

本章說明如何使用精靈來安裝 SecureWay Boundary Server，並且包括下列各節：

- 『如何準備？』
- 第13頁的『SecureWay Boundary Server』

如何準備？

本節說明如何準備 SecureWay Boundary Server 的元件。

與 SecureWay Policy Director 整合

若要在 Windows NT 或 AIX 上設定基本的 IBM SecureWay Policy Director，請執行下列步驟：

1. 驗證您的作業系統是否已適當架構爲可支援 Policy Director。
2. 決定哪一個伺服器元件最適合您的佈署基本要求，及要在哪些機器上安裝這些元件。
3. 如果還沒有的話，請安裝及架構一個 DCE 基礎架構。
4. 安裝及架構 SecureWay Directory （LDAP）。
5. 如果您打算要做從屬站憑證鑑別，架構「憑證授權服務」（CAS）。
6. 安裝 NetSEAT 從屬站。
7. 安裝 Policy Director 伺服器元件。
8. 安裝「管理主控台」。

如需取得有關 Policy Director 的其餘資訊，請參閱 *Policy Director 啓動與執行 3.0*。

SecureWay Firewall

若要在 Windows NT 或 AIX 上設定基本的 IBM Firewall，請執行下列步驟：

1. 確定您已經具有第15頁的『SecureWay Boundary Server 硬體基本條件』列出的必備需求。
2. 規劃您的 IBM Firewall 設定。事先決定要使用哪些防火牆功能及要如何使用那些功能。
3. 告訴 Firewall，它的哪一個介面連接至安全網路。您必須要有一個安全介面和一個非安全介面，您的防火牆才能適當運作。從架構從屬站導覽樹狀結構中，開

啓「系統管理」資料夾，然後按一下**介面**，即可看到在您防火牆上的網路清單。若要變更介面的安全狀態，請選取該介面，然後按一下**變更**。

註: 如果您要連接至網際網路，請洽詢您的網際網路服務提供者 （ISP），取得防火牆非安全介面的登錄 IP 位址。

4. 存取「系統管理」資料夾中的**安全政策**對話框，以便設定一般安全政策。如果是典型的 Firewall 架構：
   - 容許 DNS 查詢
   - 拒絕廣播訊息至非安全介面
   - 拒絕 Socks 至非安全配接卡
5. 設定領域名稱服務及郵件服務。如果您未提供 DNS 解析，通信不會有效率。這些功能是從架構從屬站導覽樹狀結構上的「系統管理」資料夾存取。
6. 使用架構從屬站導覽樹狀結構上的**網路物件**功能，定義您的網路關鍵元素至防火牆。網路物件會控制經過 Firewall 的流量。定義下列關鍵元素作爲網路物件：
   - Firewall 的安全介面
   - Firewall 的非安全介面
   - 安全網路
   - 您的安全網路上的每一個子網路
   - 如果適合的話，您的「安全性動態」伺服器及您的 Windows NT 領域伺服器之主電腦物件。
7. 啓用 Firewall 上的服務。這些方法（如 socks 或 proxy）讓在安全網路內的使用者可以存取非安全網路。實際上施行的服務，是取決於您在規劃階段所做的決定。實施服務通常需要設定一些連接架構，允許特定的流量類型。例如，若要讓您的安全網路使用者透過 HTTP proxy 瀏覽網際網路上的 Web，您不只需要在 Firewall 上架構 HTTP proxy 常駐程式，也需要設定允許 HTTP 流量的連接。如果您打算要設定 Policy Director，請參閱第11頁的『與 SecureWay Policy Director 整合』一節。
8. **僅 Windows NT**：由於強化處理會停用 NETBIOS，因此如果您要使用 Windows NT 領域密碼以便鑑別，您必須架構 Windows 從屬站程式碼，使其實施搜尋受信任的 Windows NT 領域進行鑑別的功能。受信任的 Windows NT 伺服器必須具有 TCP/IP 主電腦名稱及位址，並且具有它們和 Firewall 之間的 TCP/IP 連通性。防火牆管理者需要建立 Firewall 與受信任的 Windows NT 伺服器之間的連接，使流量可在兩邊之間串流。
9. 如果您要使用網址轉換，請先洽詢您的 ISP 取得登錄的網際網路位址，作爲多對一位址轉換之用。此位址是和在第11頁的3步驟要求的額外位址。然後，跳至*新增 NAT 架構*畫面，將已登錄的網際網路位址新增至*多對一 IP 位址*欄位中。

遵循這些步驟，應可完成防火牆的基本架構並開始執行。 IBM Firewall 尚提供其它功能，如系統日誌，可協助您確定您的網路的安全性。

當 Firewall 因一般或異常因素關閉時，您的架構資料不會受影響，因爲架構資料已儲存在硬碟中，並且會在重新開機時，自動再啓動。不過，會出現一些防火牆日誌訊息，指出部份作用中的連線被岔斷，例如，作用中的 FTP 階段作業。

SecureWay Boundary Server

您可以使用 SecureWay Boundary Server 精靈，設定 Firewall 使用 IBM SecureWay Policy Director 作爲使用者管理，和 Policy Director 整合。此精靈也可將 Firewall HTTP Proxy 架構爲傳遞鑑別資訊至 SurfinGate plugin（僅限 Windows NT）。

爲 Firewall 架構 IBM SecureWay Boundary Server 需要的資訊如下：

- Firewall 將要使用的 IBM SecureWay Directory 伺服器的主電腦名稱及領域。
- IBM SecureWay Directory 伺服器監聽的連接埠號碼。預設埠號是 389。
- IBM SecureWay Directory 伺服器的 SecurityMaster 密碼。
- 用來區分此 Firewall 的 proxy 使用者的領域名稱。任何使用此名稱的防火牆都會管理同一組使用者。通常您會使用 Firewall 機器的完整主電腦名稱。
- 用來存取 proxy 使用者的 Firewall 管理者名稱會儲存在 SecureWay Directory 中。此名稱會被授與修改在 SecureWay Policy Director 中建立的所有 proxy 使用者的存取權。您應該使用 Firewall 機器的完整主電腦名稱。
- 「識別名稱」，讓 IBM SecureWay Directory 作爲起點，並從該處開始搜尋資料庫中的 Firewall 使用者。此識別名稱是您在 SecureWay Directory 中建立用來儲存 Policy Director 使用者的字尾。
- 要連接 IBM SecureWay Directory 伺服器時使用的 Firewall 管理者 ID 的密碼。

您需要建立一個連接，讓流量可在 Firewall 及 SecureWay Directory 伺服器之間串流。

確定您已經具有第15頁的『SecureWay Boundary Server 硬體基本條件』列出的必備需求。

SurfinGate

若要準備開始使用 SurfinGate，您必須先安裝 Windows NT Service Pack 5。確定您已經具有第15頁的『SecureWay Boundary Server 硬體基本條件』列出的必備需求。

執行下列步驟，準備使用 SurfinGate：

- 如果您是使用 Oracle 資料庫，必須先將其架構好。

- 如果您是使用 Windows NT Firewall，您需要決定要使用 plugin 或 proxy 模式。
- 若要在 WTE 上啓用 SurfinGate plugin，將 SurfinGate plugin 安裝在 Firewall 機器上，然後執行 SecureWay Boundary Server 精靈。
- 您需要建立一個連接，讓流量可在 SurfinGate plugin 及 SurfinGate 伺服器之間串流。

MIMEsweeper

若要準備開始使用 MIMEsweeper，您需要瞭解您的網路要如何運作。確定您已經具有第15頁的『SecureWay Boundary Server 硬體基本條件』列出的必備需求。

MAILsweeper

如果您要架構 MIMEsweeper，MAILsweeper 和 WEBsweeper 必須位在不同的機器上。

在開始架構 MAILsweeper 之前，請先執行下列作業：

- 決定在內部使用的郵件領域。必須架構 MAILsweeper 及 Firewall 郵件交換程式以便接受來自這些郵件領域的郵件。
- 決定哪些安全郵件伺服器要支援哪個領域。必須架構 MAILsweeper ，將指定送往任何您的郵件領域的郵件轉遞至正確的安全郵件伺服器。
- 決定 MAILsweeper 伺服器的位址。必須架構您的每一個安全郵件伺服器爲將從內部從屬站接收到的郵件，轉遞至 MAILsweeper 伺服器。
- 決定 Firewall 的位址。必須架構 MAILsweeper 爲將定址爲外部領域的郵件轉遞至 Firewall 郵件交換程式。

WEBsweeper

在開始架構 MAILsweeper 之前，請先執行下列作業：

- 決定 WEBsweeper 伺服器的位址。在您的網路中的每一個從屬站 Web 瀏覽器都需要此位址。瀏覽器必須架構爲使用 WEBsweeper 伺服器作爲其 HTTP、FTP 及 HTTPS 的 proxy。
- 決定 Firewall 的安全介面位址。必須架構 WEBsweeper 以便轉遞 proxy 要求至位在 Firewall 上的 HTTP proxy。
- 如果您不希望從屬站略過 Web 內容過濾程序，您需要在 Firewall 上設定一個連接，限制 proxy 存取您的 WEBsweeper 及/或 SurfinGate 伺服器。

第4章 IBM SecureWay Boundary Server （SBS） 基本要求

本章提供有關 SecureWay Boundary Server 的基本要求資訊。

SecureWay Boundary Server 硬體基本條件

Boundary Server 元件產品的硬體基本條件顯示在以下表格中。

表 2. Boundary Server 元件產品硬體基本條件

Boundary Server 元件	機型	磁碟空間	記憶體	其它
Policy Director	無	64 MB	16 MB	無
IBM Firewall	• Windows NT：266 MHz 或更高 • AIX：支援 4.3.2 的 RS/6000 機器	Windows NT：200 MB AIX：200 MB	Windows NT：64 MB AIX：128 MB	2 張網路介面卡（NIC）
ACE/Server	• Windows NT：166 MHz 或更高（僅限單一處理器） • AIX：支援 AIX 4.2 的機器	• 主伺服器軟體： 50 MB • 備份伺服器：22MB • 起始使用者資料庫： 4 MB • 安裝： 240 MB	最少： 32 MB	實際儲存體需求根據使用者人數而定
MAILsweeper	Windows NT：400 MHz 處理器或更高	1 GB	128 MB	無
WEBsweeper	Windows NT：450 MHz 處理器或更高	1 GB	128 MB	無
WEBsweeper 系統需要高容量環境	Windows NT：450 MHz 處理器或更高	3 GB	512 MB	無

表 2. Boundary Server 元件產品硬體基本條件 (繼續)

SurfinGate 4.05 Server	Windows NT：233 MHz 處理器或更高	20 MB	256 MB	無
SurfinGate 4.05 Console	Windows NT：233 MHz 處理器或更高	15 MB	64 MB	無

註: 請參閱 IBM SecureWay Firewall for AIX 或 Windows NT 版設定與安裝多國語言版中的明細。Netscape 瀏覽器也需要 138 MB 磁碟空間。

SecureWay Boundary Server 軟體基本要求

Boundary Server 元件產品的軟體基本要求顯示在以下表格中。

表 3. Boundary Server 元件產品基本軟體基本要求

產品	Windows	AIX	其它
Policy Director 伺服器	Windows NT 版本 4.0 ，具有 Service Pack 5	4.3.1	無
IBM Firewall	Windows NT 版本 4.0 ，具有 Service Pack 5	4.3.2	無
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	無
MAILsweeper	Windows NT 版本 4.0 具 Service Pack 5； Internet Explorer 4.01 或更新版；Microsoft Management Console 1.1; NTFS 磁碟機；Windows Messaging	無	您打算使用的防毒工具
WEBsweeper	Windows NT 版本 4.0 ，具有 Service Pack 5	無	您打算使用的防毒工具
SurfinGate Server	Windows NT 版本 4.0 ，具有 Service Pack 5	無	無

表 3. Boundary Server 元件產品基本軟體基本要求 (繼續)

SurfinGate 4.05 Console	Windows NT 版本 4.0 ，具有 Service Pack 5 或 Windows 95	無	無

第5章 安裝及架構 SecureWay Boundary Server

本章說明如何在 Windows NT 及 AIX 上架構及安裝 SecureWay Boundary Server。

- 『安裝 SecureWay Boundary Server 元件』
- 第21頁的『架構 SecureWay Boundary Server 元件』
- 第29頁的『侵入封鎖』

安裝 SecureWay Boundary Server 元件

本節協助您安裝 IBM SecureWay Firewall、SurfinGate 及 MIMEsweeper Windows NT 與 AIX 版。

安裝 SecureWay Firewall

如需取得有關 SecureWay Firewall for Windows NT and AIX 基本架構的其餘資訊，請參閱第11頁的『如何準備？』。其中說明如何定義安全介面、如何決定您的安全政策及如何定義網路物件。如需取得安裝 SecureWay Firewall 的其餘資訊，請參閱 *IBM SecureWay Firewall 安裝手冊 AIX 版* 及 *IBM SecureWay Firewall 安裝手冊 Windows NT 版*。

安裝 SecureWay Directory

如果您要使用 SecureWay Boundary Server 的 LDAP 特性，您必須安裝 SecureWay Directory，請參閱 *IBM SecureWay Policy Director 啓動與執行 3.0 版*。

SecureWay Directory 伺服器必須位在您的 Firewall 的安全端，或位在 Firewall 安全非防禦區 （DMZ） 內。

安裝 SecureWay Policy Director

如果您要使用 SecureWay Boundary Server 的 LDAP 特性，您必須安裝 SecureWay Policy Director（請參閱 *IBM SecureWay Policy Director 啓動與執行 3.0 版*）。

安裝 SecureWay Boundary Server

如果要在 Windows NT 上安裝 SecureWay Boundary Server，請執行下列步驟：

- 安裝 SecureWay Firewall for Windows NT
- 從 SecureWay Boundary Server CD，執行 setup.exe
- 選擇您的語言，然後按一下**確定**

- InstallShield 會詢問您要將 SecureWay Boundary Server 安裝在哪裡。 Windows NT 版的預設目錄是： C:\Program Files\IBM\SBS
- 重新開機

如果要在 AIX 上安裝 SecureWay Boundary Server，請執行下列步驟：

- 安裝 SecureWay Firewall for AIX
- 放入 CD 然後使用 SMITTY 進行安裝
- 選取「軟體的安裝與維護」
- 選取「安裝與更新軟體」
- 選取「安裝與更新最新的軟體」
- 當被要求提供輸入裝置時，請列出選擇，然後選擇「光碟機」
- 列出要安裝的軟體選項，然後選擇 sbs。
- 按 **Enter** 開始安裝軟體
- 重新開機

安裝 SurfinGate

SurfinGate 具有兩個元件：SurfinGate Server 及 SurfinGate Console。若要安裝 SurfinGate 的任何元件，請參閱位在 SurfinGate CD 上的「安裝」手冊 \docs\install.pdf。

SurfinGate plugin

若要將 SurfinGate plugin 安裝在 IBM SecureWay Firewall For Windows NT 上，請參閱 SurfinGate CD 上 \docs 目錄內的安裝手冊。

安裝 MIMEsweeper

MIMEsweeper 具有三個元件：MAILsweeper、WEBsweeper 及 WEBsweeper HTTPS。

: MAILsweeper 4.1 必須安裝在 NTFS 分割區中。

安裝 MAILsweeper

若要安裝 MAILsweeper，請參閱位在 MIMEsweeper CD 上的 \install\MSW4_0_2\docs\qsg.pdf 內的*入門手冊* 。

請勿將 MAILsweeper 安裝在和 WEBsweeper HTTP proxy 相同的機器上。

請勿將 MAILsweeper 安裝在和 WEBsweeper HTTPS proxy 相同的機器上。

如果您從 Windows NT CD 安裝 MAPI32.dll，然後從 MIMEsweeper CD 安裝 Microsoft Management Console 1.1 時， MAPI32.dll 的正確版本會被和 Microsoft Management Console 一起安裝的前一個版次改寫。在安裝 Microsoft Management Console 之後，請確定要安裝 MAPI32.dll 版本 4.0 或更新版。 dll 通常位在 Windows Messaging 元件中。

安裝 WEBsweeper

要安裝 WEBsweeper 時，請參閱位在 MIMEsweeper CD 的 \install\WSW3_2_5\docs\manual.pdf 內的 *Administrator's Guide* 。

: **請勿**將 WEBsweeper 安裝在和 MAILsweeper 相同的機器上。

安裝 WEBsweeper HTTPS

要安裝 WEBsweeper HTTPS 時，請參閱位在 MIMEsweeper CD 的 \install\WSWHTTPS1_0_2\readme.txt內的 *Readme* 。

請勿將 WEBsweeper HTTPS proxy 安裝在和 MAILsweeper 相同的機器上。

架構 SecureWay Boundary Server 元件

架構 SecureWay Firewall

基本的 IBM Firewall 設定：

1. 規劃您的 IBM Firewall 設定。事先決定要使用 Firewall 的哪些功能及要如何使用那些功能。
2. 告訴 Firewall ，它的哪一個介面連接至安全網路。您必須要有一個安全介面和一個非安全介面，您的防火牆才能適當運作。從架構從屬站導覽樹狀結構中，開啓「系統管理」資料夾，然後按一下**介面**，即可看到在您防火牆上的網路清單。若要變更介面的安全狀態，請選取該介面，然後按一下**變更**。
3. 存取「系統管理」資料夾中的**安全政策**對話框，以便設定一般安全政策。如果是典型的 Firewall 架構：
   - 容許 DNS 查詢
   - 拒絕廣播訊息至非安全介面
   - 拒絕 socks 至非安全配接卡
4. 設定領域名稱服務及郵件服務。如果您未提供 DNS 解析，通信不會有效率。這些功能是從架構從屬站導覽樹狀結構上的「系統管理」資料夾存取。
5. 使用架構從屬站導覽樹狀結構上的**網路物件**功能，定義您網路的關鍵元素至 Firewall。網路物件會控制經過 Firewall 的流量。定義下列關鍵元素作爲網路物件：

- Firewall 的安全介面
- Firewall 的非安全介面
- 安全網路
- 您的安全網路上的每一個子網路
- 如果適合的話，您的「安全性動態」伺服器及您的 Windows NT 領域伺服器之主電腦物件。

6. 啓用 Firewall 上的服務。這些方法（如 socks 或 proxy）讓安全網路內的使用者可以存取非安全網路。實際上施行的服務是取決於您在規劃階段做的決定。實施服務通常需要設定一些連接架構，允許特定的流量類型。例如，若您要讓您的安全使用者以 HTTP proxy 使用網際網路上的 Web，您不只需要在 Firewall 架構 HTTP proxy 常駐程式，還需要設定讓 HTTP 交流的連接。
7. 設定 Firewall 使用者。如果您要求針對出埠 Web 存取等功能或 Firewall 管理者進行鑑別，您需要定義這些使用者至 Firewall。如果您要使用 SecureWay Policy Director 將 proxy 使用者儲存於 LDAP 中，請勿在此時建立 proxy 使用者。請於架構 Policy Director 時，使用 Policy Director 主控台建立 Firewall proxy 使用者。

這些步驟應可協助您完成 Firewall 的基本架構並開始執行。 IBM Firewall 尚提供其它功能，如系統日誌，可協助您確定您網路的安全性。

當 Firewall 因一般或異常因素關閉時，您的架構資料不會受影響，因爲架構資料已儲存在硬碟中，並且會在重新開機時，自動再啓動。不過，會出現一些防火牆日誌訊息，指出部份作用中的連線被岔斷，例如，作用中的 FTP 階段作業。

架構 SecureWay Firewall 進行 Policy Director 整合

必須架構 Firewall，將 IBM SecureWay Policy Director 和 SecureWay Boundary Server 精靈一起使用，才能取得和 Policy Director 整合的優點。如果沒有使用 IBM SecureWay Policy Director， proxy 使用者只能透過「 Firewall 圖形式使用者介面」（GUI）定義。這類使用者不能由 SecureWay Policy Director 管理。

必須建立一個連接，才能讓 SecureWay Firewall 和 SecureWay Directory 通信。SecureWay Directory 必須位在 Firewall 的安全端，這可以是在安全 DMZ 內或安全網路內。

如需有關如何設定連接的其餘資訊，請參閱 *IBM SecureWay Firewall for Windows NT 使用手冊*及 *IBM SecureWay Firewall for AIX 使用手冊*。設定連接的資訊如下。

對於要求，以下是設定出埠規則所需的項目：

- 來源爲 Firewall 的安全配接卡位址。
- 目的地爲 SecureWay Directory 位址。

- 來源端連接埠必須大於 1023。
- 目的地連接埠等於 389。
- 介面爲安全介面。
- 遞送爲本端遞送。
- 方向爲出埠。

對於回答，以下是設定入埠規則所需的項目：

- 來源爲 SecureWay Directory 位址。
- 目的地爲 Firewall 的安全配接卡位址。
- 來源端連接埠等於 389。
- 目的地連接埠必須大於 1023。
- 介面爲安全介面。
- 遞送爲本端遞送。
- 方向爲入埠。

連接範例顯示如下：

```
# 服務 : ldap
# 說明 :

permit 9.67.130.153 255.255.255.255 9.67.141.85
255.255.255.255 tcp gt 1023 eq 389 secure both
outbound l=y f=y t=0 e=none a=none

permit 9.67.141.85 255.255.255.255 9.67.130.153
255.255.255.255 tcp/ack eq 389 gt 1023 secure local
inbound l=y f=y t=0 e=none a=none
```

執行 SecureWay Boundary Server 設定精靈。選取使防火牆和 Policy Director 一起使用的選項。如需其餘資訊，請參閱第25頁的『架構 SecureWay Boundary Server 進行 Policy Director 整合』。

架構 SecureWay Firewall 使用 SurfinGate Plugin（僅限 Windows NT）

必須建立一個連接，才能讓 SecureWay Firewall 和 SurfinGate 伺服器通信。SurfinGate 伺服器必須位在 Firewall 的安全端。

如需取得如何設定連接的其餘資訊，請參閱 *IBM SecureWay Firewall for Windows NT 使用手冊*。設定連接的資訊如下。

對於要求，以下是設定出埠規則所需的項目：

- 來源爲 Firewall 的安全配接卡位址。
- 目的地爲 SurfinGate 伺服器的位址。
- 來源端連接埠必須大於 1023。
- 目的地連接埠等於 3141。
- 介面爲安全介面。
- 遞送爲本端遞送。
- 方向爲出埠。

對於要求，以下是設定入埠規則所需的項目：

- 來源爲 SurfinGate 伺服器的位址。
- 目的地爲 Firewall 的安全配接卡位址。
- 來源端連接埠等於 3141。
- 目的地連接埠必須大於 1023。
- 介面爲安全介面。
- 遞送爲本端遞送。
- 方向爲入埠。

此種連接的範例顯示如下：

```
# 服務 : SurfinGate Plugin Communication
# 說明 :
permit 9.67.143.113 255.255.255.255 9.67.143.115 255.255.255.255 tcp gt 1023 eq 3141
secure local outbound l=y f=y
permit 9.67.143.115 255.255.255.255 9.67.143.113 255.255.255.255 tcp eq 3141 gt 1023
secure local inbound  l=y f=y
```

附註：連接應出現在同一行。

您還需要架構 SurfinGate 伺服器，以容納將被掃瞄的資料。在 SurfinConsole（SurfinGate 管理介面）上，您需要勾選「一般」標籤下的 **Plugin 模式**選項。您也要在 Proxy 標籤的「下一個 Proxy」欄位中，輸入 Firewall 的 HTTP proxy 位址與埠號。

架構 SecureWay Firewall 使用 MAILsweeper

SecureWay Firewall 中定義的 Mail Exchanger 需要指向 MAILsweeper 機器，而不是實際的安全郵件伺服器。 MAILsweeper 本身會遞送郵件至安全郵件伺服器。

架構 SecureWay Policy Director

確定已安裝好 SecureWay Directory。您必須知道安裝 SecureWay Directory 機器的位址、它監聽的連接埠、 SecureWay Directory 伺服器上的管理者 ID 及管理者密碼。

將 SecureWay Directory LDAP 從屬站安裝在和 SecureWay Policy Director 相同的機器上。（如果您的 SecureWay Directory 及 SecureWay Policy Director 位在相同的機器上，就表示從屬站可能已經安裝好了。）

您必須修改 SecureWay Directory 的 LDAP 綱目，以支援 Policy Director eProxyUsers。綱目新增資訊儲存在 Policy Director 提供的兩個檔案中。您會需要位在 Policy Director CD 上 /schema 目錄內的 secschema.def 及 puschema.def 檔案。

若要修改 SecureWay Directory 伺服器上的 LDAP 綱目，請在 Policy Director 機器上執行以下指令：

```
ldapmodify -h <LDAPHOST> -p <LDAPPORT>  -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f secsch
ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f puschem
```

其中：

- <LDAPHOST> 是 SecureWay Directory 伺服器名稱
- <LDAPPORT> 是伺服器監聽的連接埠
- <LDAPADMINUSER> 是管理者 ID
- <LDAPADMINPWD> 是管理者密碼

當您修改好 LDAP 綱目以便支援 proxy 使用者之後，您必須啓用 Policy Director Console 的 proxy 使用者操作。要執行此動作時，您必須將位在 \Program Files\IBM\IVConsole 目錄內，console.properties 檔案的 Proxyusers TaskView 這一行取消註解標示。

架構 SecureWay Directory

您必須定義一個字尾至 SecureWay Directory，作爲儲存 Policy Director 使用者的根位置。若要新增字尾至 LDAP，請參閱 *IBM SecureWay Directory 管理手冊*。例如，典型的字尾可能如下：

```
o=yourcompany,c=yourcountry
```

當您新增好用來儲存 Policy Director 使用者的字尾之後，您必須正確設定其存取控制清單 （ACL）。您必須將新字尾的所有存取權提供給 Policy Director 安全群組。Policy Director 安全群組的識別名稱 （DN） 是：

```
cn=securitygroup,secauthority=default
```

架構 SecureWay Boundary Server 進行 Policy Director 整合

您可以使用精靈架構來 SecureWay Boundary 伺服器。此精靈會導引您經過一些步驟，以便設定 Firewall，使其和 Boundary Server 及 Policy Director 中的其它產

品一起使用。接下來出現的畫面會詢問您有關您 LDAP 伺服器的問題。當您填入所有必需的資訊之後，精靈會設定 Firewall 使用 Policy Director 用在使用者和群組政策的相同 LDAP 資料庫。此精靈也可以架構 Firewall HTTP Proxy，使其傳遞鑑別資訊至 SurfinGate plugin（僅限 Windows NT Firewall），或取消此架構。

若要架構 IBM SecureWay Boundary Server，請執行 SecureWay Boundary Server 精靈。在 AIX 上，執行指令 **sbswizard**，在 Windows NT 上，選取**開始->程式集->SecureWay Boundary Server**。如此即會啓動 SBS 精靈。

1. 選取**設定 Firewall 以便和 Policy Director 共用 LDAP 資料庫**選項。
2. 使用第13頁的『SecureWay Boundary Server』中的資訊，回答所提出的問題。

架構 SecureWay Boundary Server 啓用 SurfinGate Plugin （僅限 Windows NT）

選取**開始->程式集->SecureWay Boundary Server**。如此即會啓動 SBS 精靈。

1. 選取**架構 Firewall HTTP Proxy 以便傳遞鑑別資訊至 SurfinGate plugin** 選項。
2. 完成對話。

架構 SurfinGate

在 Windows NT 上共有兩種方式可架構 SurfinGate：

- 架構爲鏈結的 proxy
- 架構爲 Firewall HTTP proxy 的 plugin

在 AIX 上僅有一種方式可架構 SurfinGate：

- 架構爲鏈結的 proxy

架構 SurfinGate 為鏈結的 Proxy

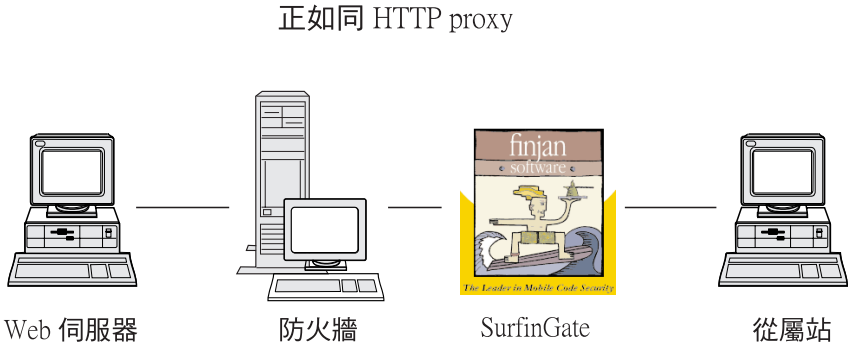

圖 2. SurfinGate 配置

必須架構從屬站 Web 瀏覽器以使用 SurfinGate 作爲其 HTTP、FTP 及 HTTPS 的 proxy。請務必要指定 SurfinGate 監聽的埠號（預設值是 8080）。

在 SurfinConsole（SurfinGate 管理介面）上，您需要勾選「一般」標籤下的 **Proxy 模式**選項。您也要在 Proxy 標籤的「下一個 Proxy」欄位中輸入 Firewall 的 HTTP proxy 位址與埠號。另外，如果您有已經定義的額外 proxy，您可以指向這些 proxy 做爲下一個 proxy。

架構 SurfinGate 為 Firewall HTTP Proxy 的 Plugin

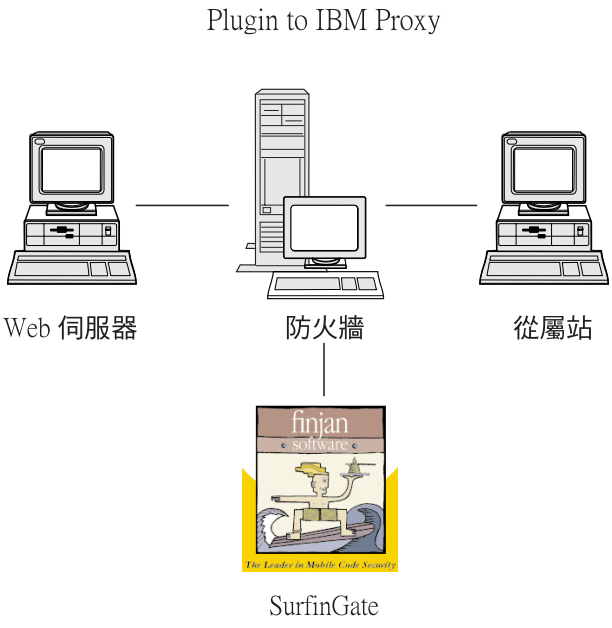

圖 3. SurfinGate 配置

從屬站 Web 瀏覽器必須架構爲使用 Firewall HTTP proxy 作爲其 HTTP、FTP 及 HTTPS 的 proxy。指定 Firewall HTTP proxy 監聽的埠號（預設值是 8080）。

在 SurfinConsole（SurfinGate 管理介面）上，您需要勾選「一般」標籤下的 **Plugin 模式**選項。您也要在 Proxy 標籤的「下一個 Proxy」欄位中輸入 Firewall 的 HTTP proxy 位址與埠號。

註: 此項功能僅在 SecureWay Firewall for Windows NT 上才有。

架構 MIMEsweeper

架構 MAILsweeper

圖 4. MAILsweeper 配置

如果您的環境很單純，則在安裝時回答問題，即可架構 MAILsweeper。若要進行額外的配置，請執行下列步驟：**開始->程式集->MAILsweeper for SMTP->MAILsweeper for SMTP Console**。 如需取得其餘資訊，請參閱 *MAILsweeper Getting Started Guide*。

架構 WEBsweeper

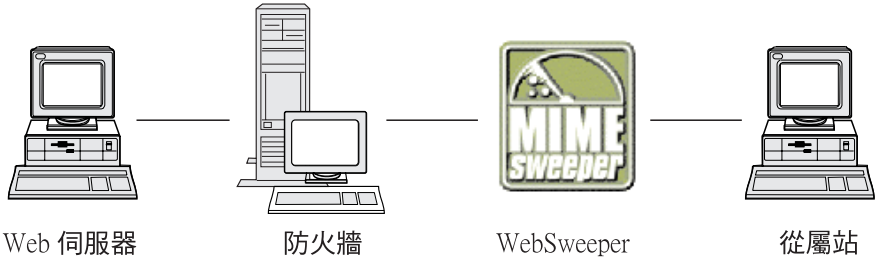

圖 5. WEBsweeper 配置

要進行架構時，請至控制台並且選取 WEBsweeper applet。如需取得其餘資訊，請參閱 MIMEsweeper CD 上的 *WEBsweeper Administrator's Guide*。

架構 WEBsweeper HTTPS

要進行架構時，請至控制台並且選取 WEBsweeper HTTPS applet。如需其餘資訊，請參閱 *WEBsweeper 管理手冊*。

侵入封鎖

使用指令行公用程式，建立可以封鎖特定 IP 位址的過濾程式。可在檢驗內容之後，動態決定要封鎖的位址。指令爲：

- fwadd_deny
- fwdelete_dynamic

fwadd_deny

如果程式啓動時未包含任何參數，它會顯示一則提示，要求指定所需的參數格式。

參數爲：

過濾程式 ID

如果是 Windows NT Firewall，適用以下情況： 可指定一個 ID 至過濾程式，以組織其維護作業。從 1 開始以升冪順序指定 ID，並且如果提供的 ID 高於下一個可用的號碼時，則指定的 ID 會是下一個可用的號碼，而不是提供給程式的 ID 號碼。例如，如果某些規則已有 ID 1 存在，而您嘗試以 ID 3 建立一組過濾規則，則會改爲指定 ID 2。相同的 ID 可以指定給多項規則。當使用 delete_dynamic 程式刪除規則時，會以 ID 來參照規則，因此當依 ID 建立規則時，要先規劃，如果這些規則共用相同的 ID 時，則刪除它們時將之視爲群組刪除。

當新增好規則時，所使用的 ID 號碼會顯示出來。

過濾程式 ID

如果是 AIX Firewall，適用以下： ID 可以號碼指定。例如，如果過濾程式 ID 是 ID 12，則可以指定 ID=12。在 AIX 上，不同的過濾程式不可指定相同的 ID。每一支過濾程式必須具有其唯一的 ID。

來源 IP 位址

作爲封包來源的 IP 位址，必須輸入爲以點隔開的十進位記數法，如 255.255.255.255。

來源 IP 遮罩

此欄位和來源 IP 位址配合使用，並且要輸入以點隔開的十進位記數法。例如，如果輸入的來源 IP 位址是 10.5.8.0，並且來源遮罩是 255.255.255.0，則從 10.5.8.1 到 10.5.8.255 之間的所有封包都符合。

目的地 IP 位址

作爲封包目的地的 IP 位址必須輸入爲以點隔開的十進位記數法，如 255.255.255.255。

目的地 IP 遮罩

此欄位和目的地 IP 位址配合使用，並且要輸入以點隔開的十進位記數法。例如，如果輸入的目的地 IP 位址是 10.5.8.0，並且目的地遮罩是 255.255.255.0，則從 10.5.8.1 到 10.5.8.255 之間的所有封包都符合。

配接卡 配接卡規格爲：

S 指定爲安全的配接卡

N 指定爲非安全的配接卡

B 所有配接卡（包括安全及非安全）

來自配接卡的封包若符合指定的類型，即符合規則。

範圍 通過防火牆的封包範圍是以此參數指定，它可以是下列其中一個值：

L 本端封包

R 遞送封包

B 本端及遞送封包

方向 指定流量流向爲入埠、出埠或雙向。

I 入埠流量

O 出埠流量

B 入埠及出埠流量

日誌記載

指定 Y 啓用記載，或 N 關閉動態過濾程式活動記載。

fwdelete_dynamic

如果此程式啓動未附加參數，則會列出目前定義的所有動態過濾程式。

```
>>>>  動態規則                    =  1
 >>>>>>>>  跳過                   =  0
 >>>>>>>>  過濾程式動作           =  拒絕
 >>>>>>>>  來源端位址             =  9.192.8.7
 >>>>>>>>  來源端遮罩             =  255.255.255.0
 >>>>>>>>  目的地位址             =  9.192.240.1
 >>>>>>>>  目的地遮罩             =  255.255.255.0
 >>>>>>>>  通信協定               =  任何
 >>>>>>>>  來源端連接埠           =  任何 0
 >>>>>>>>  目的地連接埠           =  任何 0
 >>>>>>>>  配接卡                 =  兩者 （安全及非安全）
 >>>>>>>>  範圍                   =  兩者 （遞送及本端）
 >>>>>>>>  方向                   =  兩者 （入埠及出埠）
 >>>>>>>>  通道 Id                =  0
 >>>>>>>>  啓用日誌記載           =  無法使用
 >>>>>>>>  容許片段               =  否
```

註: 首先必須使用 `fwdelete_dynamic` 指令驗證要刪除的規則是否具有可預期的 ID。

如果程式是以有效的過濾程式 ID 啓動，則會刪除動態規則，並且刪除的規則數目會顯示成找到 x 個規則的 id 爲： x。

警告：如果您嘗試新增重複的過濾程式，系統會告訴您該過濾程式已經存在。如果您嘗試新增過濾程式但未指定「過濾程式 ID」，您會接收到一則錯誤警告訊息。

: 如果高層規則集合中有規則存在，便可以覆寫 AIX 入侵封鎖。如果使用入侵封鎖，
: 則大部份的規則必須位在低層設定中。動態規則會新增至這兩套規則的中間。如
: 果高層中的規則容許流量通過，您不可以利用動態規則來關閉流量。

測試您的配置

當您完成前一章中說明的所有設定之後，必須測試設定是否可行。若要測試 SecureWay Boundary Server 的配置，請執行下列步驟：

1. 使用 Policy Director 設定 Firewall Proxy 使用者。設定使用者使用 Firewall 密碼進行安全 telnet ，並且設定使用者的密碼。
2. 執行 SecureWay Boundary Server 精靈，建立 Firewall 及 Directory （LDAP）之間的鏈結。
3. 從一安全從屬站啓動一個 proxy telnet 階段作業。
4. 輸入在 Policy Director 中設定的使用者。
5. 您會被提示輸入密碼。
6. 您現在已通過鑑別。

第6章 相關的文件

您可以使用本章列出的文件，來尋找有關 IBM SecureWay Boundary Server 版本 2.0 及相關產品的其餘資訊。

IBM SecureWay FirstSecure

以下這本書 *IBM SecureWay FirstSecure Planning and Integration，版本 2.0* 中包含有關 FirstSecure 的資訊。本書說明 FirstSecure 及組成 FirstSecure 的產品，並且可協助您開始規劃如何使用所有的 IBM SecureWay 產品。

IBM SecureWay Firewall

下列文件包含有關 IBM SecureWay Firewall for Windows NT 的資訊，此資訊在 IBM SecureWay Firewall CD 上的 `x:\books\zh_TW` 目錄內以 PDF 及 HTM 格式提供：

- *IBM SecureWay Firewall for Windows NT 設定與安裝手冊*
- *IBM SecureWay Firewall for Windows NT 使用者手冊*
- *IBM SecureWay Firewall for Windows NT 參考手冊*
- *Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3*（紅皮書）

下列文件包含有關 IBM SecureWay Firewall for AIX 的資訊，此資訊在 IBM SecureWay Firewall CD 上的 `books/zh_TW` 目錄內以 PDF 及 HTM 格式提供：

- *IBM SecureWay Firewall for AIX 設定與安裝指南*
- *IBM SecureWay Firewall for AIX 使用者手冊*
- *IBM SecureWay Firewall for AIX 參考手冊*
- *A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions*（紅皮書）

MIMEsweeper

MAILsweeper

下列文件包含有關 MAILsweeper 的資訊，此資訊在 MIMEsweeper CD 上的 \INSTALL 目錄內以 PDF 及 HTM 格式提供：

- *Getting Started Guide*位在 \install\MSW4_0_2\Doc\qsg.pdf
- Readme 位在 \install\MSW4_0_2\README.htm

WEBsweeper

下列文件包含有關 WEBsweeper 的資訊，此資訊在 MIMEsweeper CD 上的 \INSTALL 目錄內以 PDF 及 HTM 格式提供：

- *WEBsweeper Administrator's Guide* 位在 \install\WSW3_2_5\Doc\manual.pdf
- 版本注意事項位在 \install\WSW3_2_5\Doc\RELNOTES.htm

WEBsweeper HTTPS Proxy

下列文件包含有關 WEBsweeper HTTPS proxy 的資訊，此資訊在 MIMEsweeper CD 上的 \INSTALL 目錄內以 TXT 文字檔格式提供：

- Readme 位在 \install\WSWHTTPS1_0_2\readme.txt

SurfinGate

下列文件包含有關 SurfinGate 的資訊，此資訊在 SurfinGate CD 上的 \docs 目錄內以 PDF 格式提供：

- *SurfinGate Installation Guide* 位在 \Docs\install.pdf
- *SurfinGate User's Manual* 位在 \Docs\manual.pdf
- 版本注意事項位在 \Docs\SFG 405 RelNotes.pdf
- 有關 SurfinGate plugin 的資訊位在 \docs 目錄內。

附錄A. 疑難排解

本章可協助您偵測與解決與 SecureWay Boundary Server 相關的問題。

解決 IBM SecureWay Firewall 的一般問題

遞送問題

IBM Firewall 在**安全政策**對話框中提供一個特性，稱爲*測試 IP 遞送*，此功能有助於進行遞送問題除錯。請啓用此勾選框，啓動「連線配置」，然後啓用「連線規則記載」。接下來檢查您的 `firewall log`，檢視其中有關通過您的防火牆的所有封包詳細資訊。

首先使用 IP 位址執行這些測試，然後再使用主電腦名稱做測試。

無法從防火牆連通測試主電腦

問題說明

您的網路介面未正確架構。

建議動作

請參閱您的作業系統文件。

問題說明

至非安全網路的連線未正確架構。

建議動作

請連絡您的網際網路服務公司取得協助。

問題說明

如果您的安全網路隔離在路由器之後，您的防火牆必須具有至該路由器的靜態路徑。請使用 `netstat -rn` 驗證靜態路徑：

```
netstat -rn
```

Protocol Family 2 的輸出應如下 ：

```
目的地        閘道              旗號        ....
default       nrr.nrr.nrr.nrr   UG
nnn.nnn.nnn   nnn.nnn.nnn.nnn   U
sss.sss.sss   sss.sss.sss.sss   U
ss1.ss1.ss1   srr.srr.srr.srr   UG
127           127.0.0.1         U
```

圖 6. netstat -rn 輸出範例.

nrr.nrr.nrr.nrr

代表至網際網路的路由器並且是預設路徑。預設路徑是靜態路徑（旗號=UG）。

nnn.nnn.nnn

代表您的非安全領域。此爲介面路徑（旗號=U）。

nnn.nnn.nnn.nnn

代表您的非安全介面。

sss.sss.sss

代表您的安全領域。此爲介面路徑（旗號=U）。

sss.sss.sss.sss

代表您的安全介面。

ss1.ss1.ss1

代表在您的網路的安全端上的次領域，並且 srr.srr.srr.srr 代表至該次領域的路由器。此爲靜態路徑（旗號=UG）。

127.0.0.1

是迴路或區域主電腦。此爲介面路徑（旗號=U）。

每一個介面都應該有一個介面路徑，並且您的預設路徑應指向防火牆的非安全端上的路由器。

建議動作

新增一條通往路由器的靜態路徑。請連絡您的路由器管理者。使用 `route add` 指令。

問題說明

在安全介面或您嘗試要連接的主電腦上的子網路遮罩可能不正確。

建議動作

使用您的從屬站配置公用程式更正遮罩設定。

無法從安全主電腦連通測試非安全主電腦（反之亦然）

問題說明

與防火牆相鄰的每一個路由器都必須包含一個靜態路徑，指定防火牆做爲目的地網路在防火牆之外時的閘道。

建議動作

連絡路由器管理者。

問題說明

如果您的安全網路使用的位址未經過登錄，並且無法在非安全網路上遞送，包括 RFC 1597 中指定的專用位址，則將無法將封包遞送回傳送者。

建議動作

僅限 Windows NT：使用具有已登錄位址的從屬站。防火牆的 NAT 特性可使用於 TCP 及 UDP 流量，但 NAT 不會像 ping 一樣轉換 ICMP 封包中的位址。

建議動作

僅限 AIX：使用具有已登錄位址的從屬站。

DNS 失效

註: DNS 僅對 Windows NT 有效。

問題說明

您接收到 DNS 錯誤訊息，因爲您使用 Microsoft DNS Service Manager 架構 Microsoft DNS Service。

建議動作

參照安裝指示，並且

1. 藉由刪除整個目錄的方式，來移除 Microsoft DNS：
   `\winnt\system32\DNS`
2. 重新安裝 Microsoft DNS
3. 重新開機
4. 重新安裝 DNS 快速修復
5. 重新開機

解決一般問題-MIMEsweeper

WEBsweeper 及 MAILsweeper 好像無法在相同的機器上使用

問題說明

嘗試在相同的機器上執行 MAILsweeper 及 WEBsweeper 時發生問題。

建議動作

將 MAILsweeper 及 WEBsweeper 安裝在不同的機器上。

WEBsweeper 速度很慢

問題說明

使用 WEBsweeper 時，下載 Web 內容速度太慢。

建議動作

1. 使用 WEBsweeper Control Panel applet 停用日誌記載。
2. 將 WEBsweeper 安裝在您擁有的最快速機器上。

WEBsweeper 授權問題

問題說明

將 WEBsweeper 3.2_5 安裝在曾經安裝前一版 WEBsweeper 的機器上時，可能會有授權金鑰問題。當 WEBsweeper 啓動時，如果發生 Internal Windows 錯誤訊息：2140，請檢查事件檢視器中的應用程式日誌。來自 WEBsweeper 的訊息是：″PAKMSG 錯誤：使用者名稱與先前定義的授權區段衝突。″

建議動作

移除 Windows 登錄中的舊授權金鑰。載入 regedit 並在路徑 \\HKEY_LOCAL_MACHINE\SOFTWARE\Content Technologies\MIMEsweeper\License 下尋找。如果此處有一個以上的金鑰，請刪除沒有 ″IBM MIMEsweeper System″ 標籤的那一個。重新開機。

WEBsweeper 下載大型檔案時發生問題

問題說明

WEBsweeper 在進行過濾時，可能沒有足夠的虛擬記憶體可儲存檔案。

建議動作

增加 WEBsweeper 伺服器上的實際記憶體數目。

解決一般問題--SurfinGate

SurfinConsole 在開啓 Microsoft Internet Explorer 後停止回應

問題說明

當 Internet Explorer 開啓時，SurfinConsole 應用程式顯示怪異行爲或停止回應。這兩個應用程式互相衝突，因此不能同時執行。

建議動作

不要同時載入 Internet Explorer 及 SurfinConsole。

SurfinGate Plugin 速度緩慢

問題說明

使用 SurfinGate Plugin 時，透過 Web 下載機動程式碼速度很慢。

建議動作

確定 SurfinConsole 上的 Proxy 區段中，「下一個 Proxy」欄位設定爲 SecureWay Firewall HTTP proxy。

附錄B. 注意事項

在其他國家中，IBM 不見得有提供本書中所提供的各項產品、程式或服務。本書在提及 IBM 產品、程式或服務時，不表示或暗示只能使用 IBM 產品、程式或服務。只要不侵犯 IBM 的智慧財產權，任何功能、產品或服務都可以取代 IBM 的產品。不過，其他非 IBM 產品、程式或服務在運作上的評價與驗證，其責任屬於使用者。

在這本書或文件中可能包含著 IBM 所擁有之專利或專利申請案。本書使用者並不享有前述專利之任何授權。 您可以用書面方式來查詢授權，來函請寄到 IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

本程式之獲授權者若欲取得相關資料，以便使用下列資訊者可洽詢 IBM。其下列資訊指的是： （1） 獨立建立的程式與其他程式（包括此程式）之間交換資訊的方式 （2） 相互使用以交換資訊之方法。若有任何問題請連絡：

Site Counsel, IBM SWG
IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

本「程式」並非由「IBM 客戶合約 (ICA)」的條款所授權使用。而是由「IBM 國際程式授權合約 (IPLA)」的條款所授權使用。

本文件未必將付印出書，且僅以「現狀」提供本文件，而不提供任何保證 (包括可售性或符合特定效用之保證)。

本產品包含 CERN 建立及提供的電腦軟體。此說明應該在任何包括此處的 CERN 電腦軟體或其組件的產品中完整陳述。

商標

下列專有名詞是 IBM 公司在美國或（及）其他國家的商標。

AIX

IBM

Microsoft 及 Windows NT 是 Microsoft Corporation 在美國及其它國家的商標或註冊商標。

**SurfinGate 是 Finjan Software, Ltd的商標。

**MIMEsweeper、 **MAILsweeper 及 **WEBsweeper 是 Content Technologies, Ltd 的註冊商標。

由雙星號(**)所標註的其他公司、產品和服務名稱可能是第三者的商標或服務標記。

名詞解釋

六劃

企業內網路（intranet）. 一套安全專用的網路，將網際網路標準及應用程式（如 Web 瀏覽器）與組織的現有電腦網路基礎架構整合。

七劃

伺服器位址（server address）. 分派給透過網路提供共用服務給其它電腦的每一台電腦之唯一的代碼，如檔案伺服器、列印伺服器或郵件伺服器。標準的 IP 位址是一個 32 位元位址欄位。伺服器位址可以是以點隔開的十進位 IP 位址或主電腦名稱。

伺服器（server）. 透過網路提供共用服務給其它電腦的電腦，如檔案伺服器、列印伺服器或郵件伺服器。

防火牆（Firewall）. 一個功能單元，用來保護及控制網路之間的連接。防火牆可防止不受歡迎或未獲授權的通信流量進入受保護的網路，並且僅讓特定的通信流量離開受保護的網路。

八劃

服務（service）. 由一或多個節點提供的功能；例如，HTTP、FTP、Telnet。

十劃

迴圈介面（loopback interface）. 一種介面，當資訊要傳送至相同系統中的實體時，可用來略過不必要的通信功能。

十一劃

偵測（ping）. 一個指令，會傳送網際網路控制訊息通信協定 （ICMP）回應要求封包至主電腦、閘道或路由器，並預期會收到回答。

埠（port）. 一個號碼，用來指出分出的通信裝置。在預設的情況下，Web 伺服器使用連接埠 80。

從屬站（client）. 向其它電腦系統或處理（通常稱爲伺服器）要求服務的電腦系統或處理。多個從屬站可能共用存取共同的伺服器。

通信協定（protocol）. 當發生通信時，支配通信系統的功能單元作業的一套規則。通信協定可決定機器對機器介面的低階明細，如位元組中的位元傳送次序；也可以決定應用程式之間的高階交換，如檔案轉送。

十三劃

逾時（timeout）. 允許作業發生的時間間隔。

閘道（gateway）. 一個功能單元，可交互連接兩個不同架構的電腦網路。

預設值（default）. 未明確指定時所假設的值、屬性或選項。

十四劃

精靈（wizard）. 應用程式中的一個對話，使用逐步式指示，指引使用者經歷特定的作業。

網際網路（Internet）. 全球性的交互連接網路集合，使用網際網路通信協定及集允許公共存取。

D

DMZ. 非防禦區。一種裝置，用來防止外來使用者直接存取具有公司資料的伺服器。

F

FTP（檔案轉送通信協定）. 一種應用程式通信協定，用來在網路之間雙向轉送檔案。 FTP 需要有使用者 ID，有時也會要求使用密碼來允許存取位在遠端主電腦系統上的檔案。

I

ICMP. 網際網路控制訊息通信協定。在網際網路通信協定 （IP）層次用來處理錯誤及控制訊息的。問題及不正確的資料封目的地報告，會傳回其原始的資料封來源。

IP. 網際網路通信協定。一種無連線的通信協定，經由網路或交互連接的網路遞送資料。 IP 的功能是作爲高階通信協定層及實體層之間的媒介。

IP 位址（IP address）. 網際網路通信協定地址。唯一的 32 位元地址，指定網路上每一個裝置或工作站的實際位置。亦稱爲網際網路位址。

IPSEC. 網際網路通信協定安全。仍在開發中的標準，目標是確定網路通信中網路或封包處理層的安全。

N

NAT. 網址轉換。在防火牆中，將安全 IP 位址轉換爲外部登錄的位址。此功能可促成和外部網路通信，但會遮蔽在防火牆內使用的 IP 位址。

P

PICS. 網際網路內容選擇的平台。可 PICS 的從屬站可讓使用者決定要使用哪一級的服務，及每一級服務可接受與不可接受的等級。

S

shell. 接受及處理來自使用者工作站的指令行之軟體。 Korn shell 是多個 UNIX shell 中的一種。

SMTP. 全文爲「Simple Mail Transfer Protocol」，意指「簡單郵件轉送通信協定」。在網際網路通信協定集中的一個應用程式通信協定，供轉送在網際網路環境中的使用者郵件。 SMTP 指定郵件交換順序及訊息格式。它假設傳輸控制通信協定爲基礎通信協定。

T

TCP. 傳輸控制通信協定。在網際網路上使用的通信協定。 TCP 提供可靠的主電腦對主電腦的資訊交換。使用 IP 作爲基礎通信協定。

TCP/IP. 全文爲「Transmission Control Protocol/Internet Protocol」，意指「傳輸控制通訊協定/Internet 通訊協定」。一組通信協定集，其設計目標爲促進網路之間的通信，不論每一個網路使用哪一種通信技術。

Telnet. 終端機模擬通信協定，是遠端連接服務的 TCP/IP 應用程式通信協定。 Telnet 讓位在某個網站上的使用者存取遠端主電腦，如同該使用者的工作站是直接連接至該遠端主電腦。

U

UDP. 使用者資料封通信協定。在網際網路通信協定集中，提供可靠、無連線式資料封服務的一種通信協定。它讓位在某台機器上或處理的應用程式可傳送資料封至位在其它機器或處理上的應用程式。 UDP 使用網際網路通信協定（IP）遞送資料封。

V

VPN. 虛擬專用網路（VPN）。一個由一或多個安全 IP 通道連接一或多個網路組成的網路。

W

Web. 包含程式及檔案的 HTTP 伺服器網路，其中許多是超本文文件，包含連結位在 HTTP 伺服器上的其它文件的鏈結。亦稱爲全球資訊網。

WTE. Web 流量高速公路（WTE）。一個 Proxy 快取伺服器，可透過高效率的快取機制，加速一般使用者回應時間。彈性 PICS 過濾可協助網路管理者從一中心位置控制對 Web 型資訊的存取。

IBM SecureWay Boundary Server
for Windows NT and AIX
啟動與執行
版本 2.0

讀者意見表

折疊線

台北市敦化南路一段二號十二樓

中臺灣國際商業機器股份有限公司
文心支援中心 啟

寄

折疊線

廣告回信
台灣北區郵政管理局
登記證
北台字第0587號
（免貼郵票）

寄件人 姓名：
地址：

讀者意見表

爲使本書盡善盡美，本公司極需您寶貴的意見；懇請您使用過後，撥冗填寫下表，惠予指教。

請於下表適當空格內，填入記號（∨）；我們會在下一版中，作適當修訂，謝謝您的合作!

評估項目	評　估　意　見		備　註
正確性	內容說明與實際程序是否符合	□是□否	
	參考書目是否正確	□是□否	
一致性	文句用語及風格，前後是否一致	□是□否	
	實際畫面訊息與本書所提之畫面訊息是否一致	□是□否	
完整性	是否遺漏您想知道的項目	□是□否	
	字句、章節是否有遺漏	□是□否	
術語使用	術語之使用是否恰當	□是□否	
	術語之使用，前後是否一致	□是□否	
可讀性	文句用語是否通順	□是□否	
	有否不知所云之處	□是□否	
內容說明	內容說明是否詳盡	□是□否	
	例題說明是否詳盡	□是□否	
排版方式	本書的形狀大小，版面安排是否方便使用	□是□否	
	字體大小，顏色編排，是否有助於閱讀	□是□否	
目錄索引	目錄內容之編排，是否便於查考	□是□否	
	索引語錄之排定，是否便於查考	□是□否	
	※評估意見爲"否"者，請於備註欄說明。		

其他：（篇幅不夠時，請另紙說明。）

上述改正意見，一經採用，本公司有合法之使用及發佈權利，特此聲明。

Part Number: CT6RZTC

Printed in Singapore

CT6RZTC