IBM® SecureWay® FirstSecure

規劃與整合

版本 2

SC40-0503-00

IBM® SecureWay® FirstSecure

規劃與整合

版本 2

SC40-0503-00

備註

使用本資訊及其支援的產品之前，請先閱讀第89頁的『附錄. 注意事項』下面的一般資訊。

第一版（1999 年 10 月）

本修訂版適用於 IBM SecureWay FirstSecure 版本 2 與所有後續版次，直到新修訂版中另有指示爲止。

目錄

圖

表

關於本書

IBM® SecureWay® FirstSecure，亦稱爲 FirstSecure，是一套範圍廣泛的組織架構，它可以協助您的公司：

- 保護透過 Web 及其它網路的所有網路功能層面。
- 建立在您目前的電子商業投資上。模組化設計可讓您在已規劃好的部署上，添加安全保護。
- 縮減實施安全電子商業 (e-business)所帶來的總持有成本。

本書說明 FirstSecure 和 FirstSecure 的組成元件，並且可讓您開始規劃如何使用產品。

本書中說明的產品是屬於分階段發行的一部份。可能無法同時供應所有產品或在所有國家供應。有關任何這些產品何時開始供應的資訊，請洽詢爲您提供服務的 IBM 業務代表。

本書圖示

本書顯示的圖示僅供規劃之用。每一個圖示僅說明一種可能適用您的組織的伺服器、從屬站及應用程式的安排，其實際安排方式可以有無數種。

您會看到的圖示格式是根據書籍的提供方式而定：

- 在書籍的可攜式文件格式 （PDF） 版本中的大部份圖示都比較簡化，以簡省磁碟空間並便於快速列印。
- 在印出版本中的圖示則較複雜，因此需要較多儲存體空間，列印時間也較長。

不過這兩種版本中的圖示功能都相同，並且已具有相同的標題與替代性本文。

本書的適用對象

本書是給負責規劃和整合 Web 型系統安全的系統管理者閱讀。讀者應該已經瞭解其網路及電子商業應用程式。

本書的結構

本書包含以下各篇：

- 第1頁的『第1篇 FirstSecure 概觀』提供 FirstSecure 概觀、其元件產品及可用的附件。

- 第15頁的『第2篇 規劃安全的電子商業 (e-business)網路』說明如何規劃一個安全的電子商業網路。
- 第49頁的『第3篇 安裝及整合注意事項』說明 FirstSecure 產品的安裝基本要求及整合明細。
- 第77頁的『第16章 FirstSecure 隨附的文件』說明 FirstSecure 的所有可用文件。
- 第93頁的『名詞解釋』定義本書中使用的安全相關術語。

本書亦包含一份參考書目，說明每一個產品的文件。

公元 2000 年

IBM SecureWay FirstSecure 準備說明如下。

IBM SecureWay FirstSecure 中的 IBM 產品

這些產品皆已做好 2000 年的因應。以符合其相關文件指示的方式使用時，這些產品都可以正確地處理、提供及（或）接收 20 世紀與 21 世紀交替之間的日期資料，只要和這些產品一起使用的所有產品（例如，硬體、軟體與韌體）也都能交換精確的日期資料。

其它供應商產品

其它產品都向 IBM 表示他們的產品都已做好公元 2000 年的因應。不過，IBM 本身不表示或提供這些產品的公元 2000 年因應保證。有關這些產品之公元 2000 年因應方面的任何疑問，請直接洽詢其製造商。有關非 IBM 產品及服務的資訊都是根據 Information and Readiness Disclosure Act，「再發佈」由其它公司針對其供應的產品及其服務所提供的資訊。這些公司都向 IBM 表示他們的產品都已做好公元 2000 年的因應。不過，IBM 本身不表示或提供這些產品的公元 2000 年因應保證。有關此產品的公元 2000 年因應方面的任何疑問，請直接洽詢其製造商。IBM 並未分別驗證這些「再發佈」內容也不負責此類「再發佈」中包含的資訊之完整正確性。

服務與支援

請聯絡 IBM 以取得 SecureWay FirstSecure 中所包含之所有產品提供的服務與支援資訊。這些產品有些是指非 IBM 支援。如果您是從 SecureWay FirstSecure 銷售套件中取得這些產品，請聯絡 IBM 取得服務與支援。

慣例

本書使用下列印刷慣例：

- **粗體字**表示您選取的項目名稱、指令名稱、使用者輸入的文字或顯示文字中的範例。
- 等寬字型表示範例（如虛構的路徑或檔名）或顯示在螢幕上的文字。

Web 資訊

有關 FirstSecure 的最新更新資訊可在下列網際網路上的 www.ibm.com/software/security 位置取得：

IBM SecureWay FirstSecure

www.ibm.com/software/security/firstsecure

文件位於 www.ibm.com/software/security/firstsecure/library

IBM SecureWay Policy Director

www.ibm.com/software/security/policy

文件位於 www.ibm.com/software/security/policy/library

IBM SecureWay Boundary Server

www.ibm.com/software/boundary

文件位於 www.ibm.com/software/boundary/library

IBM SecureWay Trust Authority

www.ibm.com/software/security/trust

文件位於 www.ibm.com/software/securitytrust/library

ITSO Redbook *Understanding the IBM SecureWay FirstSecure Framework*（書號 SG24-5498-00）可在網際網路上的 www.ibm.com/redbooks 取得。

第1篇 FirstSecure 概觀

本篇是 FirstSecure 及其元件產品的概觀，其中包含對每一個產品的簡短說明。

本篇說明 IBM 實作服務。

第1章 什麼是 FirstSecure？

IBM SecureWay FirstSecure 是屬於 IBM 整合安全策略的一部份。 FirstSecure 是一套範圍廣泛的建置基礎，可以協助您的公司：

- 建立安全的電子商業 (e-business)環境。
- 簡化安全規劃，縮減少安全裝置的總持有成本。
- 以更簡易的方式施行安全政策。
- 建立一個更有效率的電子商業 (e-business)環境。

FirstSecure 的元件包括病毒預防、侵入偵測、存取控制、流量內容控制、加密、數位式憑證、防火牆技術及應用程式開發工具。這些功能是在 IBM SecureWay 系列安全產品及由其他供應商的產品中，結合數家安全產品供應商的最佳元件。此外，實作服務也附在特定的 FirstSecure 元件中。 FirstSecure 建置基礎包括：

- SecureWay Policy Director
- SecureWay Boundary Server
- 免入侵
- 公開金鑰基礎建設，透過 IBM SecureWay Trust Authority 提供
- IBM SecureWay Toolbox

由於 FirstSecure 是一些可個別安裝的產品集合，因此，您可以分段施行安全環境的計畫。您可以從某個區域開始進行，測試改進功能，然後繼續移向更安全的層次。此方式可降低複雜性與減少成本，並可加速佈署 Web 應用程式與資源。

為什麼您需要 FirstSecure？

您的資料及資源對您的電子商業非常重要。 FirstSecure 中的產品共同提供：

授權 每個人都必須遵循規則。經由授權可只讓受核准的使用者存取您的系統、資料、應用程式及網路。

說明性 您可以確切知道誰在什麼時候做了那些事。說明性可讓您找出誰做了動作及哪個動作在哪個時間間隔發生。

確定性 您可以確定系統可以維持其安全承諾。此項保護可以彰顯及驗證確實可以實施您所宣稱的安全層次。

可用性 系統可以隨時爲您使用。此項保護協助您將系統、資料、網路及應用程式維持在隨時可讓您的員工、供應商、協力廠商及客戶使用的狀態。

管理 您可以定義要施行的規則。此項保護可讓您定義、維護、監視及修改政策資訊。

您可以根據全企業政策來施行這些保護，在您的企業的整個網路、系統及應用程式環境中提供一個保護網。在該網中的任何產品之間只要有一個弱點鏈結存在，即會使其餘的基礎結構完全無用。

本書將每一個 SecureWay 建置基礎產品連結至其提供的保護清單中。

什麼是 FirstSecure 建置基礎？

FirstSecure 包含的元件產品可以一次整組購買，也可以分別購買相關產品。這些產品也可能會有一或多個元件產品。您可以從任何產品開始，然後逐漸建置成完整的安全解決方案。

Policy Director

Policy Director 是安全規劃的中心焦點。Policy Director 對分佈廣泛的企業內網路及企業外網路上的 Web 資源，提供端對端之間的安全授權與管理。 Policy Director 提供鑑別、授權、資料安全及資源管理等功能。將 Policy Director 和標準的網際網路型應用程式配合使用，可建置安全及妥善管理的企業內網路。 Policy Director 包括：

- 安全服務程式
- 管理主控台
- 管理伺服器
- 安全管理程式（NetSEAL 及 WebSEAL）
- NetSEAT 從屬站
- 目錄服務分配管理系統
- 授權伺服器（協力廠商應用程式支援）

Policy Director 可在 Windows NT、AIX 及 Solaris 上執行。

請參閱第29頁的『第5章 將 Policy Director 規劃在您的網路中』，取得 Policy Director 的更進一步完整說明。

SecureWay Boundary Server

SecureWay Boundary Server 產品爲 Web 型的電子商業 (e-business)應用程式提供確定性、管理及可靠性。在各部門之間的任何環節都需要有安全界限，如工程和人力資源部門、總公司網路和遠端辦公室之間、您公司的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。適當的界限安全要求控制誰可以存取您的網路及控制進入與離開您網路的資訊。

本節說明 SecureWay Boundary Server 的建置區塊。請參閱第55頁的『第12章 SecureWay Boundary Server 基本要求及安裝注意事項』，取得規劃及整合注意事項。

IBM SecureWay Firewall

IBM SecureWay Firewall 亦稱爲 IBM Firewall，藉由控制進出網際網路的所有通信，達到安全穩固的電子商業 (e-business)環境。 IBM Firewall 提供三個關鍵的防火牆功能--過濾、proxy 及電路層閘道 -- 提供您高層次的安全與彈性。

ACE/Server

ACE/Server 是 Security Dynamic 開發的產品，包括 SecurID 記號（2 個使用者授權及 2 個記號）。ACE/Server 新增管理者登入及*虛擬專用網路* （VPN） 連接至 IBM SecureWay Firewall。

MIMEsweeper for IBM SecureWay Release 2

MIMEsweeper 來自 Content Technology，包括網際網路安全元件。 MAILsweeper 會檢查電子郵件，確定其中沒有夾帶機密資訊離開您的電子商業 (e-business)，及沒有不受允許的電子郵件傳進來。

WEBsweeper 會防止不必要的 Web 資料進入您的企業。它會先掃描然後接受來自 Java applet、可執行碼或網站的可接受資料。

SurfinGate

SurfinGate 來自 Finjan Software Ltd.，是一套電子商業的機動程式碼安全解決方案。由於機動程式碼現在經常會從企業內網路之外自動及定期地進入您的電子商業網路中，因此除了防火牆之外，您還需要更多的保護。 SurfinGate 會保護您的網路以避免受到 Java、ActiveX 及 JavaScript 程式碼的攻擊。它會在攻擊進入您的網路之前，識別出潛伏的惡意攻擊，使其遠離重要資源。它會在接受可疑的資料之前，先將其隔離起來供您檢查。

免入侵

免入侵透過全企業的偵測及產品保護來提供保證。請參閱第61頁的『第13章 免入侵基本要求及安裝注意事項』中的免入侵基本要求資訊。免入侵包括 Tivoli Cross-Site for Security 及 Norton AntiVirus。

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security 提供容易受攻擊的系統入侵偵測。使用 Tivoli Cross-Site for Security，您可以：

- 將 Cross-Site for Security 代理程式安裝在您的網路中，向 Cross-Site for Security 管理伺服器報告可疑的事件。
- 在預先定義及自訂的報告中檢視入侵資料。
- 即時偵測及記載未獲授權或可疑的活動。
- 調整安全代理程式，減少假警告的數目。

Norton AntiVirus

Norton AntiVirus 是 Symantec Corporation 的產品，這是一套全球領先的防毒軟體產品之一。 Norton AntiVirus 可在背景持續執行，協助您的電腦免於受到電子郵件附件、 ActiveX control、Java applet、網際網路下載、磁片、軟體 CD 或透過網路傳送的檔案中夾帶的病毒感染。使用 Norton AntiVirus，您可以隔離受感染的檔案。您可以配置 Norton AntiVirus 使其自動通知您更新及新發現的病毒。

公開金鑰基礎建設

IBM FirstSecure 藉由提供 IBM SecureWay Trust Authority，支援公開金鑰基礎建設 (PKI) 標準的加密及交互作業能力。

SecureWay Trust Authority 是一安全解決方案，它支援發出、重訂及廢止數位式憑證。這些憑證可以用在範圍寬廣的網際網路應用程式中，提供方法給鑑別使用者並且確保可靠的通信。 Trust Authority 是以 *Internet Engineering Task Force* (IETF) 的*公開金鑰基礎建設* (PKI) 工作群組規格爲基礎。其中包括：

- 支援 IBM AIX 及 Microsoft Windows NT 伺服器
- 一個註冊管理中心 （RA）
- 一個憑證管理中心 （CA）
- 用來申請憑證及管理發出的憑證之使用者介面
- 一個整合的 *IBM SecureWay Directory*
- 一套*審核子系統*
- SecureWay 4758 加密輔助處理器支援
- *智慧型卡片*支援

此基礎架構支援完整的憑證生命週期，包括登記及初始憑證、金鑰對更新、憑證重訂、發佈憑證與憑證廢止清單，及憑證廢止。請參閱第67頁的『第14章 公開金鑰基礎建設基本要求及安裝注意事項』取得其餘資訊。

工具箱

FirstSecure工具箱 是一套安全及與安全相關的工具集，是 FirstSecure 主要元件的一部份或可與其交互作用。此工具集可協助您：

- 將您的應用程式與 FirstSecure 整合。

- 使用 FirstSecure 自訂解決方案及應用程式。
- 建立佈署 FirstSecure 用的 ISV 及 OEM 應用程式。

FirstSecure 工具箱 API 支援下列安全功能：

- 授權服務
- 憑證及管理服務
- 目錄服務
- 安全 SOCKETS 層次通信協定服務
- KeyWorks 加密及信任管理服務
  - IBM Key Recovery Service Provider 1.1.3.0 API。IBM Key Recovery Service Provider 可回復加密的資訊。
  - IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0 是一個應用程式，在接到獲授權的要求時，可在沒有金鑰、遺失或損壞的情況下回復加密的資訊。

    這兩個工具集提供標準介面，可讓應用程式用來啓動關鍵的安全服務及安全產品公司可插入其工具集的標準介面。標準介面是以一般資料安全架構（CDSA） 爲基礎。這些工具集提供 Windows NT、Solaris 及 AIX 版。

實作服務

FirstSecure Implementation Services 可協助您的電子商業 (e-business)快速且有效率地架設好 FirstSecure 並開始運作。這些可分別收費的服務是由 IBM 提供並由具有豐富經驗的團隊執行。 FirstSecure Implementation Services 包括一個 FirstSecure Implementation Workshop 及產品層次的 QuickStart 安裝服務。 IBM 也可以針對您的個別環境，特別裁訂一套 FirstSecure 系統整合服務。

如需取得資訊及訂價選項，請洽詢爲您提供服務的 IBM 業務代表。

第2章 版次 2 有哪些新功能

版次 2 簡化了 IBM SecureWay FirstSecure 產品的規劃及安裝程序。個別產品之間的整合性更高，增加了新產品，同時管理與控制更加集中。

Policy Director

Policy Director 具有下列加強功能：

- 支援 IBM SecureWay Directory 的使用者和群組證明資訊儲存體。
- 包含 Open Group 對「授權 API」規格的最新更新。
- 可使用 Policy Director「管理主控台」，定義及編輯 IBM Firewall proxy 使用者認證。
- 包含 Policy Director「認證獲取服務」（CAS），提供使用外部鑑別服務支援。
- 使用最新的 Policy Director「認證獲取服務」支援從屬站端憑證式鑑別。
- 可藉由使用 WebSEAL 及 Policy Director CAS 之間的「介面定義語言」（IDL）介面，撰寫您自己的自訂認證獲取服務。 Policy Director 也提供一般伺服器組織架構，可處理 Policy Director CAS 伺服器功能，如啓動、伺服器登錄及信號處理。
- 除了同屬安全服務（GSS） 通道之外，也可以選擇使用安全 SOCKETS 層次（SSL）通道機制。
- 使用 Policy Director 管理主控台或指令行介面管理登入及密碼政策。
- 使用 Policy Director 管理主控台或指令行介面管理單一登入使用者、群組及（目標）。
- 一個 Web 型單一登入目標密碼管理工具。
- 一套整合的安裝程序。

SecureWay Boundary Server

SecureWay Boundary Server 具有下列加強功能：

- 一個配置 GUI，將 SecureWay Boundary Server 及 Policy Director 的部份功能連結在一起。
- 一個新的配置 TaskGuide，將 SecureWay Boundary Server 及 Policy Director 的部份功能連結在一起。

IBM SecureWay Firewall for AIX and NT 有哪些新功能

IBM SecureWay Firewall，亦稱爲 IBM Firewall，具有下列加強功能：

增強安全郵件 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 SPAM 者的訊息（除外清單）、驗證檢查訊息的有效性與可靠度（封鎖不受歡迎訊息的已知方法）、可配置每則郵件訊息的數目限制、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，包括可無痕跡地追蹤防火牆及 Domino 之間的訊息

增強 socks 通信協定版本 5

socks 通信協定版本 5 已經升級，其中包括使用者名稱-密碼鑑別（UNPW）、檢核回應鑑別 （CRAM） 及鑑別 plug-in。

日誌記載已強化爲提供使用者更多控制，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，避免在 Web 瀏覽作業中使用 sock 伺服器。使用者可以存取網際網路上的有用資訊，而不需要犧牲內部網路的安全，也不需要改變其從屬站環境，以施行 HTTP proxy。

遠端存取服務

Windows NT Remote Access Service （RAS） 透過撥號式、ISDN 或 X.25 媒體使用點對點通信協定 （PPP），提供網路連接。 NDISWAN 是一個網路驅動程式，提供作爲 RAS 的一部份，可將基礎 PPP 資料轉換爲類似的乙太區域性網路資料。

IBM SecureWay Firewall AIX 版增強功能

IBM SecureWay Firewall for AIX 提供爲數眾多的擴充：

強化的 IPSec 支援

已強化的 IPSec 支援，包括支援新的標頭。它也支援和多種 IBM 伺服器、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。

多重處理器（MP）支援

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

透過配置可提供更好的效能與彈性。您可以藉由選擇要在何處放置不同的過濾規則類型，以調整 IBM SecureWay Firewall 的效能。有一頻率指示器會提供連接使用次數。

網址轉換

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。

安裝精靈

協助進行 IBM Firewall 起始配置的精靈。此設定精靈讓不具有 IBM Firewall 廣泛知識的使用者，可在安裝之後快速地進行基本的配置並開始執行。

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 IBM Firewall，察看有無安全漏洞或配置錯誤。此種方法較快速，同時也較健全。

MIMEsweeper for IBM SecureWay Release 2 有哪些新功能

MAILsweeper 的增強功能包括：

- 掃描關鍵字，封鎖侵犯或誹謗郵件並且保護寶貴資料免於流出您的公司
- 封鎖進入的垃圾電子郵件
- 封鎖個人或群組傳送或接收特定的檔案類型
- 依大小別封鎖或延遲檔案傳送，避免網路競爭

WEBsweeper 的增強功能包括：

- 封鎖員工存取與工作不相關的指定網站
- 協助防止透過 HTML 或電子郵件位址擷取文件及經由 cookies 取得網站資訊時遭到攻擊

SurfinGate 有哪些新功能

SurfinGate 具有下列加強功能：

- JavaScript 內容檢驗
- 工作攸關的效能監督
- 增加政策管理
- 支援檔案轉送通信協定 （FTP） 及 HTTPS 通信協定

- Plug-in 與防火牆 HTTP proxy 整合
- 可封鎖特定可執行檔下載至使用者電腦的能力

免入侵

免入侵產品現在包括 Tivoli Cross-Site for Security。

Tivoli Cross-Site for Security 有哪些新功能

Tivoli Cross-Site for Security 提供侵入偵測。它可讓您監視網路攻擊，以維護您的電子商業 (e-business)的完整性。

Norton AntiVirus Solution Suite 有哪些新功能

Norton AntiVirus Solution Suite 版次 3.0.4 包括下列更新版本：

- Norton AntiVirus 5.02 for Windows 95/98 and Windows NT Workstation
- Norton AntiVirus 5.02 for Windows NT Server
- Norton AntiVirus for IBM Operating System/2 (OS/2) 5.02
- Norton AntiVirus OS/2 for Lotus Notes 2.0
- Norton AntiVirus for Lotus Notes 2.0
- Norton AntiVirus for Microsoft Exchange 1.5.2

公開金鑰基礎建設

公開金鑰基礎建設元件現在包括 Trust Authority。Trust Authority 包括：

- 一個安裝精靈，可指導您通過在 Windows NT 上的簡式安裝程序。
- 4758 加密卡的預先設定配置。不過您可以變更此資訊。
- 一個配置精靈，可在背景配置程式開始之前，檢查資料的有效性。
- 錯誤訊息及報告。
- 線上文件，包括與安裝精靈的上下文相關的說明、註冊管理中心桌上管理程式及一個實體尾端的從屬站應用程式。

IBM SecureWay Toolbox

工具箱具有下列加強功能：

- Policy Director API 及文件。
- 目錄服務 API。
- 公開金鑰基礎建設 (PKIX) API 及文件。

- IBM Key Recovery Server 1.1.3.0 現在內含在工具箱中。此產品僅提供英文版。

第2篇 規劃安全的電子商業 (e-business)網路

第二篇說明如何規劃一個安全的電子商業網路。

以下各章說明典型的網際網路流量及安全顧慮，然後會說明 FirstSecure 產品如何在您的電子商業 (e-business)網路中運作。

本節包含下列各章：

- 第17頁的『第3章 電子商業 (e-business)網路概觀』說明典型的電子商業 (e-business)網路及存在網路中的使用者、資源與互動類型。您的網路特性可能與此略有差別，不過您一樣會有相同的安全顧慮並且需要相同的安全保護。
- 第27頁的『第4章 將 FirstSecure 規劃在您的電子商業 (e-business)網路中』將 FirstSecure 產品納入網路中。
- 第29頁的『第5章 將 Policy Director 規劃在您的網路中』
- 第33頁的『第6章 將 SecureWay Boundary Server 規劃在您的網路中』
- 第39頁的『第7章 將免入侵規劃在您的網路中』
- 第45頁的『第8章 將公開金鑰基礎建設規劃在您的網路中』

第3章 電子商業 (e-business)網路概觀

您的電子商業 (e-business)網路實際上是由各種資源組成：資料及資料庫、使用者、客戶、供應商、程式設計師、硬體、公司資訊等等。現在讓我們看看其中的某些區域及哪裡需要安全保護。

網際網路是一個複雜的創作。資料透過它，從一部伺服器傳到另一部，從一位使用者傳到另一位，其路徑完全不固定，每個傳輸都不相同。

您的業務資料傳輸經過網際網路時，和其它網際網路流量完全混雜在一起。在傳輸過程中，您的重要商務資料可能會經過位在任何角落的任何伺服器。並且任何網際網路使用者都可能嘗試存取您的資源、您的員工資訊及您的資料。不幸地，除了承載教育、商業及娛樂方面的合法流量外，網際網路中也承載許多惡意的流量，這些可能是無意，也可能是故意造成的。 第18頁的圖1是網際網路概觀，顯示您的流量流經網際網路時，其中也充滿其他人的流量。

FirstSecure 可協助您將您的傳輸和其它所有流量區隔開來，並且鞏固您的傳輸。

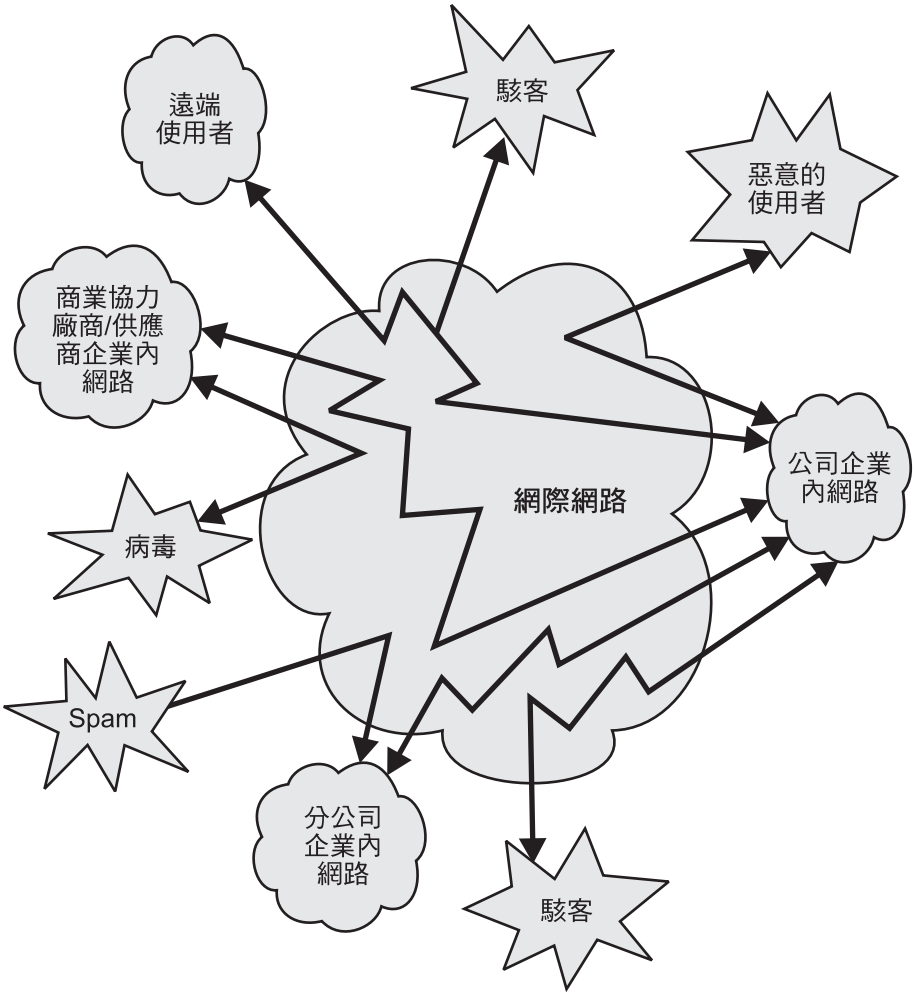


圖 1. 忙碌的網際網路中具有不相關活動的概觀

您不會想在這種網際網路中操作您的商務。您要的是第19頁的圖2中的環境，由 FirstSecure 保護安全的網際網路。

受 FirstSecure 保護的理想網際網路

您的大部份電子商業 (e-business)流量都會透過網際網路。不過，您並不想要典型的網際網路環境，它像一個充滿隨機資料的大集合，任何人都可使用家用電腦一窺究竟。 第19頁的圖2顯示您眞正想要的網際網路。

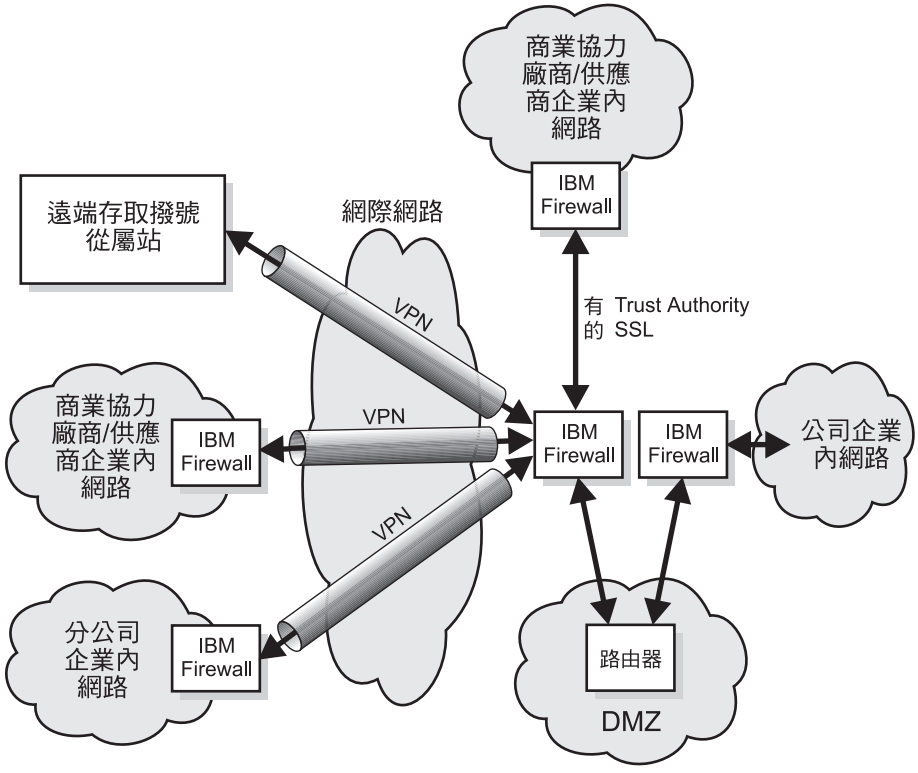


圖 2. 您要的網際網路

網際網路中提供許多有用的資訊，但您也需要可以護衛您的商業的應用程式、資料及存取。您需要確定

- 您的員工不會轉移對已分派工作的注意力。
- 您的員工不會收到不適當的電子郵件。
- 您的業務機密資訊不會流出您的公司。

虛擬專用網路

虛擬專用網路 （VPN） 是專用連線的概念，不讓網際網路上的非相關人員存取。第20頁的圖3顯示典型的 VPN。對於兩個端點的使用者而言，其連線都可免於受不必要的使用者或應用程式的入侵。 FirstSecure 產品（如 IBM SecureWay Firewall）可協助您設定及支援 VPN。

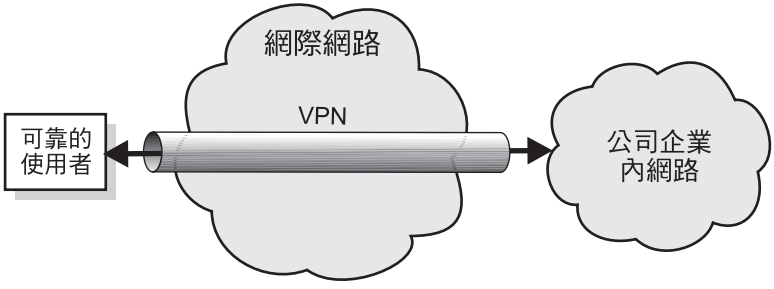


圖 3. 典型的虛擬專用網路。

非防禦區

非防禦區（DMZ）是您容許外部使用者存取的資源部份。您使用 IBM Firewall、MIMEsweeper 及其它 FirstSecure 產品，確定只有您滿意的使用者可以存取 DMZ，並且他們只能存取指定的資源。進出 DMZ 的流量應受監視，以確定其是否合適。

您的公司的型錄可放在 DMZ 中，讓任何潛在的客戶瀏覽。或者，您可能在其中放些介紹您的公司的參考用資訊。您的 FirstSecure 元件只會讓您的可靠的使用者存取您的 DMZ 以外的資訊。

第21頁的圖4顯示典型的 DMZ。

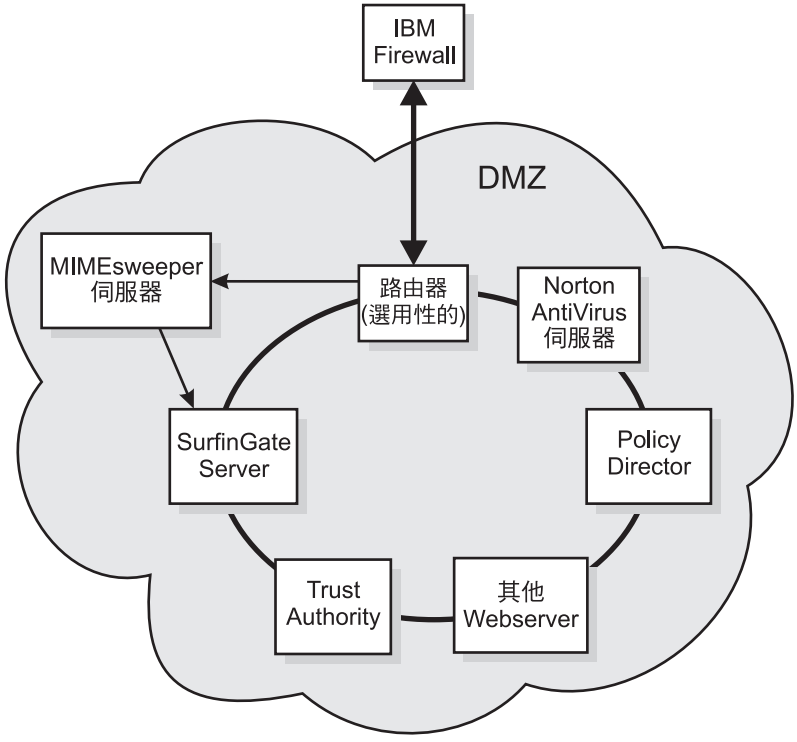


圖 4. 具有系統資源的典型 DMZ

當您發展安全應用程式時，您可以在公開讓大眾存取那些應用程式之前，使用 DMZ 作爲企業內網路的測試環境。

現在讓我們來看看您使用網際網路及您的企業內網路的資訊類型。

典型的企業內網路

您的企業內網路是您的公司內部通信所在之處。其中包含您不希望和網際網路共用的資訊及資源。您的員工們可共用其中的資料、互相交換電子郵件、存取企業內的資源，如資料庫、印表機及掃描器等。 第22頁的圖5顯示典型的企業內網路。

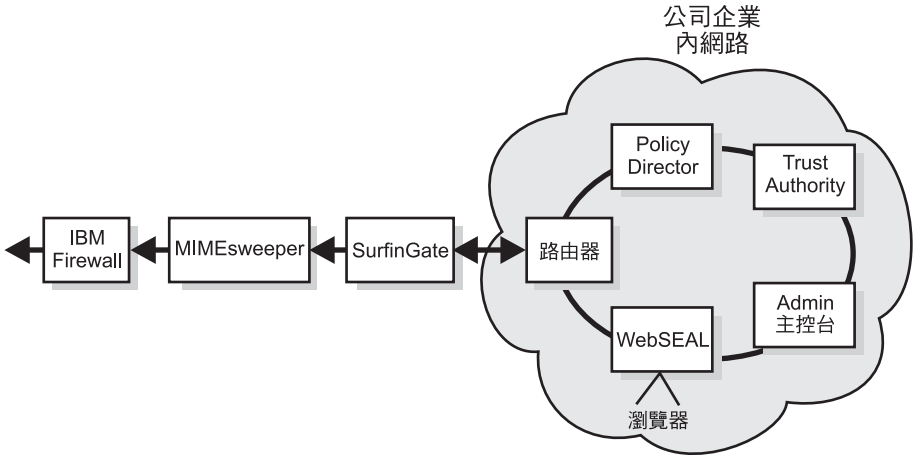


圖 5. 典型的企業內網路概觀

您必須確定您公司的機密資訊不會流傳到外面，並且只有獲授權者可以存取該資料。不過，有些資料您希望讓您的客戶使用及存取。例如，您希望您的銀行的存戶可以檢查他們的帳戶結餘，但是您不希望存戶存取員工記錄。 IBM Firewall 可使您的專用資訊保持私密性。

IBM FirstSecure 產品可協助您維持企業內網路的安全。Policy Director 讓您設定存取規則。 IBM SecureWay Trust Authority 會確定使用者的身份。 Tivoli Cross-Site for Security 讓您知道是否有未獲授權者嘗試存取您的企業內網路資源。

典型的企業分公司企業內網路

在您分公司的遠端員工需要和您的內駐員工一樣，存取相同的資料及其它資源。不過，使用電話連線傳送及接收資訊速度緩慢，並且無法避免受惡意入侵。您要使用網際網路作爲節省成本的方法並且用來加強交易的保護。 第23頁的圖6顯示典型的分公司透過網際網路與總辦公室通信。

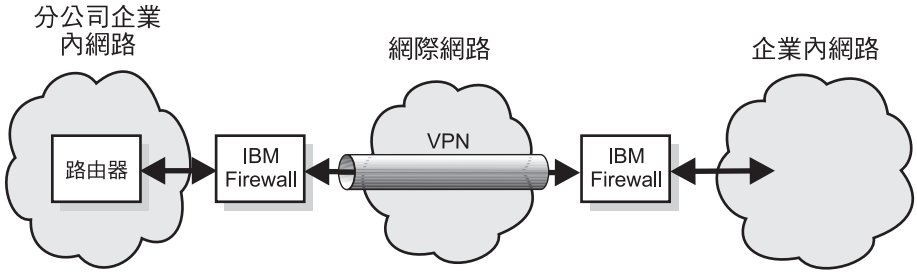


圖 6. 分公司透過虛擬專用網路連接至總辦公室

您希望您的傳輸及資料如同在企業內一樣安全。*虛擬專用網路*（VPN）即是透過網際網路的安全通道。您可以將網際網路當作是在專用企業內網路一樣使用。

典型的遠端存取員工

您的某些員工可能偶爾或永久地需要在總辦公室以外工作。員工可能經由撥號或租賃線路以透過網際網路存取您的網路。

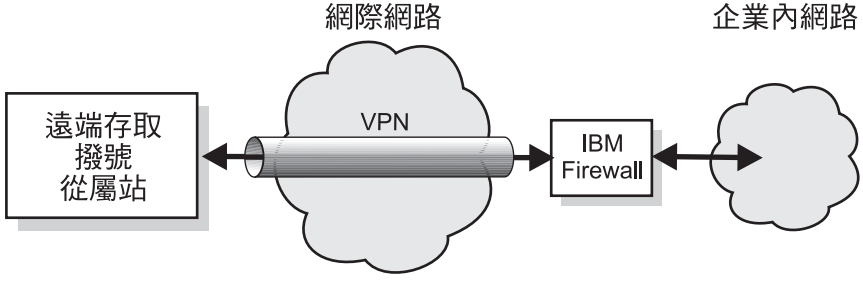


圖 7. 遠端存取撥號從屬站透過虛擬專用網路連接至總辦公室。

IBM Firewall 保護此員工的傳輸。

典型的商業夥伴或供應商企業內網路

如果您的協力廠商及供應商可以直接存取您的某些資料，您的生意會更有效率。某個供應商可能獲授權可以檢查庫存層次並且可在指定的層次時，可以送新的貨品。另一個協力廠商可能可以存取選定的記錄。會計公司可能需要存取課稅記錄，但不能存取協力廠商記錄。 第24頁的圖8及第24頁的圖9 顯示典型的供應商或協力廠商。您希望生意交易在網際網路中的流動如同是在專用連線中一樣。

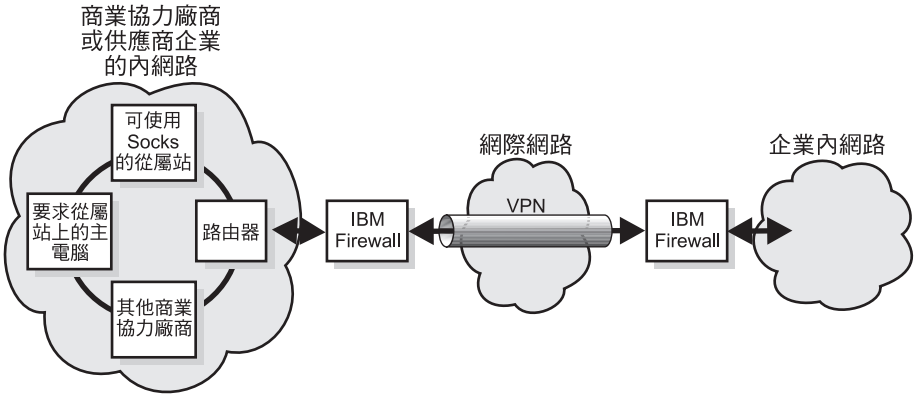


圖 8. 使用虛擬專用網路（VPN）的典型商業夥伴或供應商企業內網路

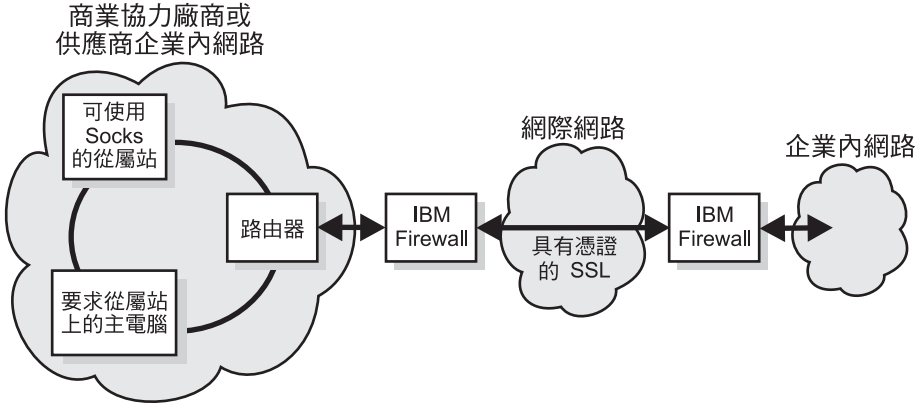


圖 9. 使用安全 SOCKETS 層次 (SSL) 傳輸通信協定的典型商業夥伴或供應商企業內網路

此協力廠商使用安全 SOCKETS 層次 （SSL） 而不是使用 VPN，因爲傳輸的兩端都經過加密。（使用者也可以使用 VPN 作爲附加的安全層次。）

您需要保護這些使用者免於受到惡意入侵及侵擾。您需要保護他們的資料傳輸不會受未獲授權的監聽及傳送。同時您也需要確定這些使用者只能存取您可讓他們存取的資料。並且您要確定這些使用者都是您接受的使用者。

資料及資料庫

資料是任何企業的最寶貴資源。某些電子商業 (e-business)資料是設計給所有網際網路使用者使用。例如，一家五金經銷商將其產品及售價清單放置在網路上供線上購物之用。服飾零售商提供線上型錄，以圖例顯示款式、顏色及大小供線上購物之用。

在授與存取資料的權限之前，您需要知道要求端是誰，及他們需要該資料的原因。使用 Trust Authority 可發出憑證給可靠的使用者。

其它待保護的區域

本書不涵蓋其它安全區域的對策。您還必須規劃：

- 網站安全、存取與外出權及劃分
- 膝上型電腦、個人電腦及工作站與其它儲存體的實體安全
- 個人安全背景檢查
- 責任、合約的法律不承諾，及如
- 作業方式，如金鑰管理、資訊控制及安全警覺與訓練

作業系統

大部份作業系統都配置爲可用性及豐富的功能集合。有效的安全方式是只讓給定作業擁有必需的基本功能。您可能要考慮解除安裝或停用您不希望侵入者存取的作業系統特性。

典型的使用者

網際網路上的使用者形形色色，有些是優良使用者，有些則否。電子商業 (e-business)需要的使用者是在線上搜尋及交易的客戶。並且電子商業 (e-business)也希望協力廠商可存取特定的資料，檢查庫存、做出製造決策或對企業內的計畫及活動提供意見。電子商業 (e-business)也需要讓員工存取他們執行其分派工作所需要的資料。

網際網路上也有電子商業 (e-business)不歡迎的使用者：電腦駭客及惡意的網路訊息散播者、散佈病毒者和意圖存取您的機密資料的使用者。這些使用者甚至可能就在您的電子商業 (e-business)內。

在您授與任何資源的存取權之前，您需要知道提出要求者是誰，該使用者對資料及應用程式需要何種存取權及應對該使用者存取做哪些記錄。

應用程式及建立應用程式

應用程式設計時可併入安全考量。您可以使用將欲傳輸的資料加密、鑑別要求存取的使用者、審核日誌使用者及異動日誌等優點。

工具箱 API 讓您在您的應用程式中加入安全保護。

硬體安全

伺服器及資料庫是安全系統的一部份。雖然本書不涵蓋硬體部份，您需要規劃用來管理安全措施的伺服器及工作站的實體安全。

Trust Authority 硬體安全

雖然本節僅只針對 Trust Authority 元件，不過此處的注意事項適用所有 FirstSecure 元件。

隔離區域

將伺服器裝置在一個隔離的房間中，專供 CA 活動使用。如果可能的話，該房間需要有強化的牆壁，實心的硬木或鋼材門，及建造堅固的天花板，沒有天窗。該房間同時要有高架地板，以防止萬一發生火災時，造成放電。

維護該區域

該房間應有一個不斷電電源供應器，給電腦、照明設備、移動偵測器及空調系統使用。您也必須檢查該房間的通風狀況，以確定其溫度足可抵銷各種設備產生的熱度。

控制對該區域的存取

您可以多種方法提供該實體區域的存取，例如，使用識別證或鍵控門鎖。如果要防止個人的惡意侵擾，您需要安裝一些控制措施，需要至少由兩個可靠的個人鑑別過的適當證明。

您也必須監視該房間，追蹤安全區域被存取的時間及由誰存取。爲了更進一步確保安全，在該房間的裡外都安裝移動偵測器。

控制通信

在 Trust Authority 伺服器上不應該有備用的開啓連接埠存在。您應該將系統架構爲只聽從明確指定給作用中的 Trust Authority 應用程式使用的連接埠監聽要求。

遵循您自己的商業程序及基本要求，確保在您的電子商業 (e-business)中使用的硬體安全。

第4章 將 FirstSecure 規劃在您的電子商業 (e-business)網路中

本篇中的下列各章將 FirstSecure 內含的產品放在您的電子商業 (e-business)中。各章都以第17頁的『第3章 電子商業 (e-business)網路概觀』圖示爲主。每一個產品都會提供一些明細。如需取得有關特定產品的資訊，請參考該產品隨附的文件。其中的佈署實務僅是建議而已。

在每一個佈署實務中，您需要遵循相同的基本步驟：

1. 在您的整個網路中使用共同的時間參照，以簡化審核日誌同時也較準確。
2. 從您的企業內網路開始安裝及測試元件。
3. 當您滿意企業內網路的測試時，即可開始在您的安全的非防禦區 （DMZ）內建置應用程式。
4. 介於企業內網路及非防禦區之間的流量應透過防火牆。
5. 建立您的外部網際網路應用程式並且利用測試資料加以測試。
6. 安裝防火牆，保護網際網路及您的 DMZ 之間的流量。
7. 讓使用者存取您的網路。

規劃完整的 FirstSecure 系統

以下是在您的網路中佈署 FirstSecure 產品的建議次序。此程序已盡量簡化。請參閱第49頁的『第3篇 安裝及整合注意事項』，取得每一個產品的軟硬體基本要求及整合注意事項。此外，請閱讀每一個產品隨附的安裝基本要求及指示。許多產品也在網際網路上提供最新的資訊。 第xi頁的『Web 資訊』列出具有 FirstSecure 資訊的網站。紅皮書 *Understanding IBM SecureWay FirstSecure Framework*（書號 SG24-5498）中包含多個更詳細的實務。

1. 規劃您需要的安全基本要求。
2. 安裝 Policy Director 以符合那些基本要求。
3. 建立及測試您的客戶伺服器應用程式。暫時將其保留在您的企業內網路之中，還不要讓網際網路使用。
4. 安裝 IBM Firewall，保護客戶伺服器應用程式。
5. 新增 SurfinGate 至 DMZ。
6. 當您開始讓網際網路使用那些應用程式時，在您的非防禦區 （DMZ） 中，加入 MIMEsweeper 及 Norton AntiVirus，來保護您的應用程式。當您開始讓外部流量使用那些應用程式時，將其配置爲指向您的伺服器。

7. 安裝 Tivoli Cross-Site for Security 產品，進行免入侵及偵測。
8. 在您的 DMZ 中新增：
   - Web 伺服器
   - Web 型錄伺服器
   - Web 庫存伺服器
   - 客戶從屬站應用程式
   - 安全客戶從屬站應用程式
   - 一或多個 Cross-Site for Security 代理程式

   在對外開放應用程式之前，先在防火牆內測試所有應用程式。使用 SecureWay Boundary Server's Network Security Auditor 工具，測試您設定的規則。
9. 安裝 IBM SecureWay Firewall 的一個案例，保護 DMZ 內的軟體。您的預設配置應該是『沒有流量』，因此您可以在對外開放之前，先測試安裝。
10. 安裝 Trust Authority 並發出憑證給可靠的使用者。
11. 在完成所有測試之後，向網際網路開放您的應用程式。
12. 在對外公佈存取之前，從您的系統之外執行 Network Security Auditor，測試那些規則。
13. 檢查由 FirstSecure 元件程式建立的審核日誌，確定沒有非預期的事件發生。
14. 繼續檢查審核日誌，並在將應用程式新增至網路時，加入 Cross-Site for Security 代理程式。

第5章 將 Policy Director 規劃在您的網路中

FirstSecure 提供您一個合併的政策驅動式混合式 Web 環境控制點。在使用者透過瀏覽器存取多個後端 Web 伺服器的環境中， Policy Director 可提供

- 每一個 Web 使用者單一登入
- 身份驗證
- 檢查要求存取受保護的網頁之使用者授權

擁有此項支援，您可以授權及鞏固：

- TCP/IP 交換，如 HTML、Telnet 及 POP3
- 協力廠商應用程式，如資料庫系統
- 網路管理工具
- 自行發展的應用程式

在 FirstSecure 中，使用者可以使用下列機制，向 Policy Director 鑑定身份：

- 透過安全 SOCKETS 層次 （SSL） 的基本鑑別
- 透過 SSL 的套表型登入
- SSL 使用從屬站憑證
- Kerberos 登入

FirstSecure 接下來會控制已鑑別的使用者對個別 Web 物件及網路服務的存取，並可限制未獲授權者存取這些資源的子集。

Policy Director 佈署

Policy Director 會管理使用者、群組及資源之間的映射。使用 Policy Director 管理主控台可以：

- 定義會使用您的資源的使用者和群組。
- 定義需要保護的物件。這些物件可能是 Web、TCP 連接埠、方法及介面等。
- 定義使用者應如何存取資源及要用什麼規則保護那些資源，如讀取、修改、管理、執行或刪除。

下表說明一般的 Policy Director 元件配置。決定您的網路需要的適當配置。然後在安裝期間選取那些元件。

請參閱 *IBM SecureWay Policy Director Up and Running*，以取得詳細資料。

配置範例	已安裝的元件
一部伺服器執行安全領域的管理伺服器之單一案例。 在此實務中，管理伺服器獨自位在自己的系統上。管理伺服器會維護安全領域的主要權限資料庫、複製此資料庫於安全領域中，並且維護在安全領域中的其它 Policy Director 伺服器的位置資訊。	僅管理伺服器
WebSEAL 伺服器。 此實務代表保護 Web 空間的解決方案。WebSEAL 支援後端伺服器，以提高其可用性及容錯效能。	安全管理程式具有 WebSEAL
NetSEAL 伺服器。 此實務代表保護虛擬專用網路 （VPN） 安全並且提供對舊型系統及協力廠商網路服務的存取控制解決方案。	安全管理程式具有 NetSEAL
WebSEAL 及 NetSEAL 伺服器組合。	安全管理程式具有 WebSEAL 及 NetSEAL
伺服器提供存取協力廠商應用程式的 Policy Director 應用程式服務。	授權伺服器
伺服器提供開發者開發環境，使其建置使用授權 API 的協力廠商應用程式。	授權伺服器及 ADK
伺服器提供上述所有配置的合併服務。	所有元件

Policy Director 是一套分佈極寬的安全系統，可以將其元件佈署在一或多部機器的多種配置中。以下是將 Policy Director 佈署在您的網路中的概觀。完整的安裝指示在 *IBM SecureWay Policy Director Up and Running*。

1. 安裝 Policy Director 安全伺服器。

   至少在安全領域中的一部電腦必須含有 Policy Director 安全伺服器，設定 Policy Director 安全領域。請參考您需要的平台之安裝及管理手冊及技術支援資源。

   其餘伺服器可作爲僅安裝 DCE 從屬站（或在 Windows NT 系統上的 NetSEAT）。
2. 安裝 SecureWay Directory （LDAP） 伺服器。
3. 安裝 Policy Director。
   - 必須先佈署 Policy Director 安全伺服器（請參閱步驟1）。
   - 所有 Policy Director 伺服器安裝都需要 Policy Director Base。
   - 如果這是安全領域中的*第一部*或*唯一*的機器，您必須安裝管理伺服器。

如果這是在具有現存管理伺服器的現有安全領域中的額外機器，不要安裝另一個管理伺服器。任何安全領域中只能有一個管理伺服器案例。

- WebSEAL、NetSEAL 及協力廠商授權伺服器元件爲可選用的部份。
- 安全管理程式會與 WebSEAL 合併，提供 WebSEAL HTTP 伺服器元件及細膩的 HTTP 存取控制，並且與 NetSEAL 合併，提供 NetSEAL 粗略的 TCP/IP 存取控制元件。

4. 安裝管理主控台。

   管理主控台需要您在作業系統上安裝一部 DCE 從屬站（或 NetSEAT for Windows NT），請參閱步驟第30頁的1。

5. 下列相依關係適用以 Authorization ADK 開發的應用程式：
   - 您需要有 Policy Director 資料包。
   - 在應用程式機器上安裝 IVAuthADK。
   - 執行應用程式的作業系統上必須具有一部 DCE 從屬站或 NetSEAT for Windows NT 系統。
   - 執行應用程式的安全領域中，必須至少安裝一部授權伺服器。在典型的開發環境中，授權伺服器是位在和 Authorization ADK 相同的作業系統上。

第6章 將 SecureWay Boundary Server 規劃在您的網路中

FirstSecure 提供 Web 型應用程式安全保護，使用現有的安全標準的優點，如「安全 SOCKETS 層次」（SSL）、SOCKS 及 IPSec。

如果您的作業環境中所包括的連線是介於使用不同信任性質的兩個網路部份之間， FirstSecure 的 SecureWay Boundary Server 元件可協助您符合下列要求：

- 安全的網際網路連線，縮減未獲授權者存取您的專用網路的可能
- 大型企業外網路基礎架構，提供協力廠商及供應商共用挑選的資料
- 使用網際網路或其它相關的不可靠網路區段作爲虛擬專用網路 （VPN），使訊息在通過不可靠網路的基礎架構時維持私密

FirstSecure 的 SecureWay Boundary Server 使用網址過濾、內容過濾、proxy 及電路層閘道技術。透過這兩種技術的組合，SecureWay Boundary Server 可藉由控制具有不同信任性質的網路之間的通信，達到政策驅動、安全性及安全的電子商業作業。

SecureWay Boundary Server 包括：

- IBM SecureWay Firewall，包括 ACE/Server
- MIMEsweeper for IBM SecureWay Release 2
- SurfinGate 4.05 for Windows NT
- 增強政策管理

請參閱第34頁的圖10，取得在完整的 SecureWay Boundary Server 安裝中的資料流程概觀。

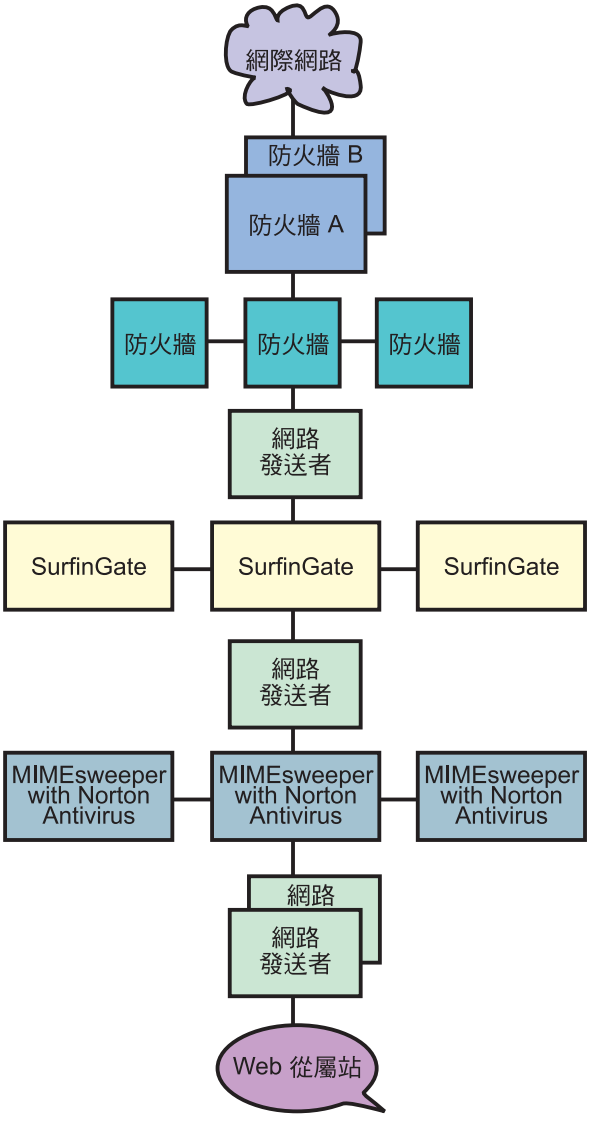


圖 10. SecureWay Boundary Server 產品中的資料流程概觀

IBM SecureWay Firewall 佈署

IBM SecureWay Firewall 亦稱爲 IBM Firewall，控制與網際網路之間的雙向通信。此防火牆技術也已用來保護 IBM 自己的資產。

請參閱第57頁的『SecureWay Boundary Server 元件注意事項』中的安裝注意事項。

您的網路功能顧慮包括：

- 需要連接至網際網路但必須防止未獲授權者存取您的網路、應用程式及資料
- 內部使用者濫用網路資產
- 規劃大型企業外網路基礎架構供協力廠商及供應商使用的方式，雖然配置管理成本極高
- 連接分公司的專線成本極高
- 因低效率、延遲或與協力廠商及供應商的誤解通信造成的低生產力
- 管理非本國語言軟體的高管理成本

IBM Firewall 可解決這些顧慮。只允許明確許可的流量通過防火牆， IBM Firewall 可將外人隔離在您的網路之外。爲了做更進一步的保護，IBM Firewall 內含的弱點檢查軟體可*強化*執行 IBM Firewall 所在的伺服器，確定電腦駭客無法進入或通過防火牆。內部網路的 IP 位址及配置都隱藏而不讓不可靠網路存取。通過防火牆的所有流量都會記載下來並且可用來產生使用者活動報告。

IBM Firewall 及其 VPN 配置應用程式可讓您以低成本方式佈署及管理大型 VPN 基礎架構。網路研究顯示客戶使用 VPN 可以實現比使用專線方式節省更多成本。

有 IBM Firewall 時，您可以使用網際網路將分公司連接起來，將防火牆佈署在每一個分支並使用 IPSec 型通道。

IBM Firewall 隨附於 ACE/Server 中，這是 Security Dynamics Technologies, Inc. 的產品。ACE/Server 提供企業網路強力的集中式鑑別服務，使得只有獲授權使用者可以存取網路檔案、應用程式及通信。延續 Security Dynamics Technologies, Inc. 獲專利的 SecurID 記號技術，ACE/Server 會建立障礙，防止未獲授權者存取。其鑑別依靠兩個因數：使用者必須同時*具有*某些東西（一個 SecurID 記號卡）並且*知道*某些東西（一個 PIN）才能通過鑑別。

MIMEsweeper 佈署

MIMEsweeper 是 Content Technologies Ltd. 的產品，會執行網際網路及企業內網路資料的內容分析，以識別任何隱藏的威脅，並保護您的網路使用者免於遭受那些威脅。

請參閱第57頁的『SecureWay Boundary Server 元件注意事項』中的安裝注意事項。

MIMEsweeper 中包含兩個基本模組，MAILsweeper 及 WEBsweeper，可以不同的方式保護您的使用者。當郵件及其它 Web 資料進入 MIMEsweeper 時，MIMEsweeper 會驗證傳送者與接收者的位址，然後會將檔案分解成其各元素部份。MAILsweeper 及 WEBsweeper 接下來會分析這些部份，以降低威脅進入您的專用網路的機會。

FirstSecure 包括 MAILsweeper 4.0 及 WEBsweeper 3.2_5。每一個都可分別安裝、配置及使用。

MAILsweeper 可：

- 與您選擇使用的病毒掃描器配合，驗證已分解的檔案沒有包含病毒
- 偵測及封鎖巨集炸彈
- 掃描關鍵字以：
  - 協助防衛電子郵件中夾帶攻擊或冒犯性的語言
  - 協助防止寶貴資料流出公司
- 封鎖流入的電子郵件 spam，使網路不致擁塞並且縮減員工生產力流失
- 封鎖個人或群組傳送或接收特定檔案類型，如 AVI 或 MPEG
- 依檔案大小封鎖或延遲檔案傳送，直到網路可以較快疏通流量爲止

WEBsweeper 可：

- 封鎖員工存取似乎不與工作有關的網站
- 協助防止無意的機密或敏感文件喪失

此外，MIMEsweeper 中包含一個應用程式設計介面 (API)，可用來整合協力廠商的 URL 封鎖器。

MIMEsweeper 可以是保護您的公司及您的使用者免於受到網際網路安全威脅的主要資產。

註: 雖然 MIMEsweeper 文件中可能有提供 Content Technologies 的服務及支援聯絡資訊，但如果您取得 MIMEsweeper for IBM SecureWay Release 2 作爲 SecureWay FirstSecure 銷售或 SecureWay Boundary Server 銷售的一部份時，您必須連絡 IBM 取得服務與支援。

SurfinGate 佈署

SurfinGate Finjan Software Ltd. 的產品，會視察機動程式碼，如 JavaScript 碼、Java applets 及 ActiveX 控制，保護您的網路免於遭受如因資料修改、資訊刪除及不法的資料收集等造成的損壞。 SurfinGate 會在閘道層次視察機動程式碼，並在其進入您的網路之前，識別具威脅的程式碼。機動程式碼可以選擇性地封鎖或允許依使用者或隨部門別方式放行，並且程式碼可依據其要進行的功能，被容許或拒絕存取您的公司網路。有 SurfinGate 時，管理者可以啓用機動程式碼並加以管理、控制及對 ActiveX、Java、JavaScript、 Visual Basic Script、plug-in 及 cookies 實施全公司化的安全政策。

SurfinGate 包括下列元件：

- SurfinGate 伺服器
- SurfinConsole
- SurfinGate 資料庫
- WTE 整合 plugin

SurfinGate Server 功能如同 HTTP proxy 伺服器、作爲防火牆或 proxy 的服務。SurfinGate Server 可以放置在企業的防火牆及任何其它現有的 proxy 之後，並且可以作爲像 HTTP 伺服器的功能。此架構可在機動程式碼發生攻擊之前，先停止及視察程式碼流量。

網路管理者可使用 SurfinConsole 來管理及設定機動程式碼的中央企業安全政策。SurfinConsole 可以控制網路上的多部 SurfinGate Servers，並且可在整個公司內，依使用者或群組或透過自訂的不可接受與可接受的程式碼清單，實施機動程式碼規則。

SurfinGate 資料庫中儲存 Applet Security Profiles (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。由於 SurfinGate 會動態地視察所有機動程式碼的內容，因此資料庫在安全中並不需要，不過資料庫在大型作業中可增進效能。

註: 雖然 SurfinGate 文件中可能有提供 Finjan 的服務及支援聯絡資訊，但如果您取得 SurfinGate for Windows NT 作爲 SecureWay FirstSecure 銷售或 SecureWay Boundary Server 銷售的一部份時，您必須連絡 IBM 取得服務與支援。

第7章 將免入侵規劃在您的網路中

截至目前爲止說明的安全技術都強調避免安全威脅。另一項同等重要的安全措施是偵測威脅。 FirstSecure 中的免入侵產品提供的入侵偵測及防毒功能，可讓您的公司偵測出安全威脅。

防毒軟體可保護以避開有害程式碼，包括 Trojan horse、 worm、巨集病毒、 rogue ActiveX control 及 rogue Java applet 等。病毒保護是任何安全解決方案中的必要部份。 FirstSecure 的防毒產品符合這些關鍵的防毒基本要求：

- 涵蓋廣泛的從屬站，提供工作站及機動從屬站的廣泛及一致的防毒要求。
- 病毒記號訂閱服務。定期更新病毒記號是維護有效率的保護措施，防止最新型或有害程式碼的重要因素。
- 政策驅動式從伺服器分送防毒更新至從屬站，確定您的防毒政策的確有在推行。

Tivoli Cross-Site for Security 佈署

Tivoli Cross-Site for Security 提供容易被入侵的系統網路型的入侵偵測。您可以將 Tivoli Cross-Site for Security 代理程式佈署在任何管理領域連接至網際網路的位置。 Tivoli Cross-Site for Security 會監視網路，以偵測內部及外部攻擊。其優點如下：

- 即時入侵偵測，警示 Cross-Site for Security 管理者潛在的入侵
- 可配置政策，讓您針對位在 DMZ 及企業內網路中的代理程式設定不同的政策
- 線上修改安全代理程式政策，讓您回應快速變更的環境
- 與 Tivoli' Enterprise 應用程式整合，因此您可以擴大您的 Tivoli 企業管理系統

Tivoli Cross-Site for Security 可：

- 偵測掃描及氾濫
- 監視 IP 流量
- 監視連接埠服務
- 偵測 DNS、裝載服務及網路檔案系統要求與回答
- 偵測埠映射服務站服務要求及回答傾出
- 偵測 RStatd 呼叫
- 偵測對特定的映射名稱及檔名的要求
- 偵測 SMB 型攻擊 PC 檔案伺服器

- 偵測網際網路控制訊息通信協定

Cross-Site for Security 可讓您監視網路流量及偵測攻擊與入侵嘗試。它可監視使您的企業內網路與網際網路隔絕的 DMZ 及您的內部網路上的流量。

Cross-Site for Security 可以偵測的入侵類型包括：

- 記號或型樣偵測
- 氾濫偵測
- 網路型攻擊
- Windows 網路攻擊
- 遠端程序攻擊
- 服務濫用
- 未獲授權者網路流量
- 可疑活動

Cross-Site for Security 會使用 Cross-Site for Security 代理程式及 Cross-Site for Security 管理伺服器守衛您的網路。當代理程式偵測到嚴重的攻擊時，會傳送加密事件至 Cross-Site for Security 管理伺服器，使其立即記載該資訊並做回應。您可以將 Cross-Site for Security 管理伺服器配置爲傳送警示至主控台、發電子郵件給管理者或以呼叫器傳呼管理者。

取得 Tivoli Cross-Site for Security 授權金鑰

若要啓用您的 Tivoli Cross-Site for Security 產品，您需要一個自訂的授權金鑰。

您可以至 Tivoli Cross-Site 網站並完成下列步驟，取得授權金鑰：

1. 找出 FirstSecure 產品隨附的 Passport Advantage Proof of Entitlement 文件，包括 Tivoli Cross-Site for Security CD-ROM 及 *Tivoli Cross-Site for Security Installation*。
2. 在您的 Passport Advantage Proof of Entitlement 上找出訂單號碼（這是一個以 5 開頭的 8 個數字號碼），及您的客戶（網站）號碼，這是以 7 開頭的 7 個數字號碼。第一次存取 Tivoli Cross-Site 網站時，您需要使用這些號碼。
3. 在可存取網際網路的電腦上，使用 Web 瀏覽器登入 Tivoli Cross-Site 網站。該網站的 URL 是 `www.cross-site.com/support/licensing/`。
4. 輸入您的訂單號碼、客戶號碼及聯絡資訊。您也必須要提供您打算用來安裝 Tivoli Cross-Site for Security 的伺服器之領域名稱。
5. 遵循 Web 上的其它指示。

6. 如果您無法存取 Tivoli Cross-Site 授權金鑰網站，請聯絡 Tivoli Cross-Site 支援的電話 1-800-2-TIVOLI，分機 9396，或傳送電子郵件至 licensing@cross-site.com。

相關的 Tivoli Cross-Site 產品

Tivoli Cross-Site 產品系列包括不屬於 FirstSecure 系列的其它元件：

- Tivoli Cross-Site for Availability 會監視及報告一般使用者是否順利存取您的網站。
- Tivoli Cross-Site for Deployment 會延伸您的企業範圍，可讓您透過網際網路分送及管理重要的應用程式與資訊。

雖然這些產品可能會在 Tivoli Cross-Site for Security 文件中提到，但它們必須另外分別購買。

以 Tivoli Cross-Site for Security 監視流量

Cross-Site for Security 代理程式是一套智慧型的網路監督攔截器。它會持續不斷地監視網路上的封包。 Cross-Site for Security 代理程式會過濾這些封包，尋找代表可疑活動的記號。這些記號可能表示網路上的攻擊。

Cross-Site for Security 代理程式在 UNIX 上會執行並成爲一個*常駐程式*，在 Windows NT 上則執行作爲一個 NT 服務。 Cross-Site for Security 會配置爲當系統啓動時跟著自動啓動。不論有無使用者登入，它都會常駐並在系統的背景執行。

當偵測到潛伏的攻擊時，代理程式會判斷其嚴重性並決定要立即通知管理伺服器或記載警示至一個本端檔案。日誌會定期上載至管理伺服器。

代理程式也會定期連絡 Cross-Site for Security 管理伺服器，讓其知道代理程式仍在作用及執行中。此種通信類型稱爲*心跳*。您可以配置心跳的間隔。

當管理伺服器接收到代理程式的心跳時，管理伺服器會通知代理程式任何更新的配置資訊、新的記號及上載時程表。代理程式會自動下載及安裝這些更新。

Tivoli Cross-Site for Security 在您的網路中

您可以將 Cross-Site for Security 配置爲最適合您的企業需求的狀況。主要決策包括：

- 在哪裡安裝 Cross-Site for Security 管理伺服器?
- 需要多少 Cross-Site for Security 代理程式?
- 在哪裡安裝 Cross-Site for Security 代理程式?

這些注意事項，加上大小、拓蹼及網路頻寬與流量，對於決定管理伺服器與代理程式的數目有極大影響。請參閱第61頁的『預防侵入的軟硬體基本要求』中的 Tivoli Cross-Site for Security 安裝注意事項。

註: 雖然 Tivoli Cross-Site for Security 文件中可能有說明如何取得服務與支援，如果您取得 Tivoli Cross-Site for Security 作爲 SecureWay FirstSecure 銷售的一部份時，您必須連絡 IBM 取得服務與支援。

Norton AntiVirus 佈署

Norton AntiVirus 來自 Symantec Corporation，是世界領先的防毒軟體產品。 Norton AntiVirus 可：

- 隔離受感染的檔案
- 防止病毒及有害的 ActiveX control 及 Java applet
- 防止可能由電子郵件附件、網際網路下載、磁片、軟體 CD 或網路中夾帶的病毒

您可以排定 Norton AntiVirus 在背景的執行間隔，協助協助保護您的電腦安全。Symantec 研究人員不時加入 Norton AntiVirus 可以偵測的病毒。您可以使用 LiveUpdate 特性，每週從 Symantec 自動擷取新的防毒定義。

Norton AntiVirus 的檢疫特性會隔離受感染或可疑的檔案於您的電腦上的安全位置，與其它檔案分開，防止您在修正檔案時，病毒漫延開來。

「掃描與遞送」精靈可讓您傳送可疑的檔案至 Symantec 做評估。 Symantec AntiVirus Research Center （SARC） 會回應並協助您修正問題。

Norton AntiVirus 的掃描器 *Bloodhound*，是在背景執行，會觀察並將可能受最新病毒感染的應用程式行爲分類。如果應用程式的行爲很像病毒並且試圖感染其它程式時， Bloodhound 會停止該程式，防止其感染其它檔案，直到您接收到新的病毒更新程式爲止。

FirstSecure 中提供的 Norton AntiVirus Solution Release 3.04 產品包括：

- 桌上型解決方案：
  - Norton AntiVirus 4.08 for DOS
  - Norton AntiVirus 4.08 for Windows 3.51
  - Norton AntiVirus 5.02 for Windows 95/98
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 5.03 for Macintosh
  - Norton AntiVirus 5.02 for OS/2
- 伺服器解決方案：

  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 4.04 for NetWare
  - Norton AntiVirus 2.0 for Lotus Notes™ and OS/2
  - Norton AntiVirus 1.52 for Microsoft Exchange
- Gateway 解決方案：
  - Norton AntiVirus 1.02A for Internet E-mail Gateways for NT
  - Norton AntiVirus 1.04 for Firewalls
- 管理：
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 for Macintosh Administrator
  - Norton AntiVirus Plus 5.0 for Tivoli Enterprise
  - Norton AntiVirus Plus 5.0 for Tivoli IT Director
  - 其它管理工具，包括 Norton AntiVirus Network Manager (NAV32/NAVNETW） v3.01

有關 Norton AntiVirus 的其餘資訊位在 Norton AntiVirus CD 根目錄內的 contents.txt 檔案中。

註: 雖然 Norton AntiVirus 文件中可能有提供 Symantec 的服務及支援聯絡資訊，如果您取得 Norton AntiVirus Solution Release 3.04 作爲 SecureWay FirstSecure 銷售的一部份時，您必須連絡 IBM 取得服務與支援。

如需詳細的安裝步驟，請參閱各特定產品隨附的文件，軟硬體基本要求在第61頁的『第13章 免入侵基本要求及安裝注意事項』。

第8章 將公開金鑰基礎建設規劃在您的網路中

公開金鑰基礎建設中的 Trust Authority 元件提供網際網路應用程式一些方法來鑑別使用者並確定可靠的通信。以公開金鑰基本設施 (PKI) 標準作爲加密及交互作業能力的基礎，Trust Authority 系統可提供用來發出、發佈及管理數位式憑證所需的基礎結構。其中包括：

- 支援 IBM AIX 及 Microsoft Windows NT 伺服器平台。
- 一個「註冊管理中心」（RA），處理使用者登錄後的管理作業。此管理可以透過自動化處理或人工決策過程施行，包括下列作業類型：
  - 確認使用者的身份
  - 核准或拒絕申請、重訂或廢止憑證要求
  - 驗證使用者具有與憑證中的公開金鑰相關的私密金鑰
  - 遵循給定的商務處理或憑證設定檔的規則，發出特定的憑證類型給特定的使用者類型

  RA 也會發佈有關位在整合公開金鑰目錄 （IBM SecureWay LDAP Directory）中的憑證資訊。
- 一個可靠的憑證管理中心 （CA）。CA 可：
  - 發出數位式憑證及產生數位金鑰對，使憑證可被鑑別
  - 支援完整的憑證生命週期，從起始的登記到憑證重訂與廢止
  - RA 會在憑證廢止時更新目錄
  - 可以使用加密硬體，如 IBM SecureWay 4758 PCI 密碼輔助處理器及智慧型卡片，以延伸其保護金鑰的能力。
- Credential Central 是一 Web 型登記介面，極容易取得瀏覽器憑證、伺服器憑證及特定裝置的憑證，如智慧型卡片。管理者也可以使用這些登記表格爲一般使用者預先登記 PKIX 憑證。
- Trust Authority Client 爲一獨立式 Windows 介面，可讓使用者不需使用 Web 瀏覽器即可取得、重訂及廢止 PKIX 憑證。
- RA 桌面是一 Web 型管理介面，可讓管理者以手動方式核准或拒絕申請、重訂或廢止憑證要求。
- 有一審核子系統會使用訊息鑑別碼 （MAC） 以確定其從 Trust Authority RA 及 CA 接收到的事件可被鑑別。有一可配置的選項使審核記錄在記載時，做整合性保護。

- 多種管理介面可配置系統、變更安全密碼、交互認證 CA、完整性檢查審核日誌及安全地啓動與停止系統元件。
- 一應用程式設計介面 （API） 讓應用程式開發者可撰寫自訂的 PKI 應用程式。
- IBM DB2 Universal Database 整合執行時間支援。IBM SecureWay Directory 及 RA、CA 及審核元件都有各自的資料庫。

Trust Authority 佈署

請參閱 *IBM SecureWay Trust Authority 更新與執行*，取得詳細的規劃及安裝資訊。本書包含安裝在 Windows NT 伺服器及 AIX 上的實務步驟。

第9章 將 SecureWay 工具箱規劃在您的企業中

計畫將 FirstSecure工具箱安裝在開發環境中，而不是您的網路內。在向外部使用者公佈您的應用程式之前，請先在開發環境中做測試。

授權服務

授權服務可讓您監視誰獲授權可存取您的網站。鑑別是根據密碼或公開金鑰。這些措施可保護您的網站上的資料完整性及私密性。授權服務會建立存取控制清單（ACL），其中定義誰可存取您的網站上的物件及他們存取那些物件的方式。授權服務也可讓您定義受保護的物件並建立供單一登入的密碼。所有這些安全工具都集中在一處，使安全政策極容易管理。授權服務受 IBM SecureWay Policy Director 授權 API 支援。

憑證管理中心服務

憑證管理中心服務受多平台 X.509 公開金鑰基礎建設 (PKI) 及 IBM KeyWorks Toolkit 支援。

憑證管理中心服務可讓您透過數位式憑證管理來確保安全。這些服務包括 API 可處理完整的憑證生命週期：發出、重訂及廢止。它們也會發佈憑證廢止清單。 API 使用公開金鑰加密法及智慧型卡片技術作爲鑑別憑證使用者的方法。

多平台 X.509 公開金鑰基礎建設 (PKI) 亦稱爲 PKIX，是透過 PKIX API 提供。這些 API 透過結束實體 （EE）、憑證管理中心 （CA） 及註冊管理中心 （RA） 等元件，建立、管理、儲存、分送及廢止憑證。 API 可作爲與 IBM SecureWay Trust Authority 間的介面，並且都是以 IBMKeyWorks 爲基礎。

如需取得有關 PKIX API 的資訊，請參閱 *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference*。如需取得有關 IBM KeyWorks 的資訊，請參閱第77頁的『第16章 FirstSecure 隨附的文件』，取得工具箱隨附的文件清單。

目錄服務

目錄服務是由 IBM SecureWay Directory 從屬站支援。

目錄服務使用 Lightweight Directory Access Protocol （LDAP） 組織、控制及存取目錄。這些服務都是根據主從架構模式提供從屬站存取 LDAP 伺服器。目錄服務提供一種方法，可在一個集中位置維護目錄資訊，執行儲存、更新、擷取及交換作業。目錄服務使用安全 SOCKETS 層次 (SSL) 將資訊加密。

如需取得有關目錄服務的資訊，請參閱第77頁的『第16章 FirstSecure 隨附的文件』，以取得工具箱隨附的完整 IBM SecureWay Directory Client 文件清單。

KeyWorks 加密及信任管理服務

加密及信任管理服務受 IBM KeyWorks Toolkit（亦稱爲 KeyWorks）支援。

KeyWorks 加密及信任管理服務對資訊加密及解密，以控制可存取資訊的人員。這些服務會建立及驗證數位簽章，鑑別網路上的個人與電腦身份。金鑰回復系統，不需分送該金鑰，即可回復加密的資訊，它包含在 IBM Key Recovery Service Provider 中。

KeyWorks 是一套加密及信任服務工具集。它包含一組分層的安全服務及相關的程式設計介面，可供給整合的資訊與通信安全功能。每一個層次都是建置在緊接其下的更基礎的服務上。這些層次從基本的元件開始，如加密演算法、亂數及在下一層中的唯一識別資訊，然後往上建置成數位式憑證、金鑰管理及回復機制，然後是最高層中的安全交易通信協定。

KeyWorks 已經有國際語言支援 （NLS），表示此產品不受限於任何語言、 script、文化及編碼字集。

如需取得有關 KeyWorksC API 的其餘資訊，請參閱第77頁的『第16章 FirstSecure 隨附的文件』，以取得工具箱隨附的 KeyWorks 文件清單。

安全 SOCKETS 層次通信協定服務

安全 SOCKETS 層次通信協定服務是由 IBM 安全 SOCKETS 層次 (SSL) 工具集所提供。

SSL 通信協定服務可讓您決定誰可以存取您的資料。這些服務使用公用及私密金鑰將資料加密的目的有多個，包括使用者鑑別、預防未獲授權的從屬站進行存取及預防資料被侵擾。您可以完全掌握要發出憑證給誰，因此可以控制誰可獲得信任存取您的資料。 SSL 技術納入其它數個 API 中，作爲加密資料及建立密碼之用。

第3篇 安裝及整合注意事項

本節說明各元件如何互相配合運作。其中列出每一個產品的軟硬體基本要求及任何必要的應用程式或資料庫產品。

第10章 規劃安裝 FirstSecure

在您開始安裝 FirstSecure 元件產品之前，請先閱讀以下各節，確定您有必需的軟硬體。有關 FirstSecure 的最新更新資訊位在以下網站：
www.ibm.com/software/security/firstsecure。請於開始安裝產品之前，先檢查該網站上是否有最新的更新。

安裝及配置 FirstSecure 元件產品的逐步明細隨附在每一個元件產品的文件中。

一般系統需求

本節說明 FirstSecure 產品的整體系統需求。有關每一個元件產品的特定軟硬體基本要求，請參閱該特定產品。

若要安裝 FirstSecure 元件，您需要可以執行下列其中一種伺服器作業系統的硬體：

- Microsoft Windows NT 版本 4，具有 service pack 5。
- AIX 版本 4.3.1 或更新版。
- Sun Solaris 版本 2.6 或更新版。

  註: 在 Solaris 上，工具箱需要 Sun Solaris 版本 2.6，並具有 May, 1999 Fix Pack。

每一個 FirstSecure 元件產品至少可在上面列出的其中一種作業系統上執行。每一個元件產品區段會顯示受支援的作業系統平台及每一個元件產品的其它必備軟體。在那些作業系統中，您需要有伺服器、管理主控台及從屬站系統。下列各節提供那些基本要求的概觀。

伺服器及從屬站的作業系統基本要求

請參閱表1，取得 SecureWay 產品的作業系統基本要求。

表 1. 伺服器及從屬站的作業系統基本要求

作業系統	基本伺服器層次	基本從屬站層次
Windows NT	版本 4.0, Service Pack 5	版本 4.0, Service Pack 5
IBM AIX	版本 4.3.1	版本 4.3.1
Sun Solaris	版本 2.6	版本 2.6
Windows 95	無	所有版本皆支援
Windows 98	無	所有版本皆支援

表 1. 伺服器及從屬站的作業系統基本要求 (繼續)

作業系統	基本伺服器層次	基本從屬站層次
Windows 3.1 （僅 Norton AntiVirus）	無	所有版本皆支援
IBM OS/2 （僅 Norton AntiVirus）	無	版本 4.0，FixPak 6 或更新版

元件產品明細及基本要求

以下各節顯示 FirstSecure 元件產品的軟硬體基本要求。以下各章詳細說明建置區塊並提供每一個建置區塊的軟硬體基本要求。同時各章中亦提供每一個產品的安裝及配置概觀，包括討論與其它元件整合。

- 第53頁的『第11章 Policy Director 基本要求及安裝注意事項』
- 第55頁的『第12章 SecureWay Boundary Server 基本要求及安裝注意事項』
- 第61頁的『第13章 免入侵基本要求及安裝注意事項』
- 第67頁的『第14章 公開金鑰基礎建設基本要求及安裝注意事項』
- 第71頁的『第15章 工具箱安裝基本要求及注意事項』

第11章 Policy Director 基本要求及安裝注意事項

本章列出 Policy Director 的軟硬體基本要求。其中也提供與其它 FirstSecure 產品整合的任何安裝注意事項。

Policy Director 軟硬體基本要求

表2 列出 Policy Director 的硬體基本條件。

表 2. Policy Director 的硬體基本條件

平台	基本磁碟空間	基本記憶體
Windows NT 伺服器：Intel 或 Intel 相容 80486 133 MHZ 或更高	16 MB	64 MB
AIX 伺服器：硬體執行 AIX 4.3.1	16 MB	64 MB
Solaris 伺服器：硬體執行 Solaris 2.6	16 MB	64 MB

Policy Director 元件的軟體基本要求包括：

Policy Director 伺服器

- Windows NT 伺服器 版本 4.0, Service Pack 5
- AIX 版本 4.3.1
- Sun Solaris, 版本 2.6

NetSEAT 從屬站

- Windows NT 伺服器 版本 4.0, Service Pack 5
- Windows 95
- Windows 98

管理主控台

- Windows NT 工作站
- Windows NT 伺服器從屬站
- AIX 版本 4.3.1 從屬站
- Sun Solaris, 版本 2.6 從屬站

Policy Director 需要資料包中隨附的其它軟體。請遵循 *IBM SecureWay Policy Director Up and Running* 的指示，安裝您的 Policy Director 佈署所需的軟體。

Policy Director 安裝注意事項

www.ibm.com/software/security/policy 列出對 Policy Director 目前軟體必備需求的任何更新。

整合 Policy Director 及 Trust Authority

IBM SecureWay Trust Authority 提供鑑別的方式是確定每一個使用者的身份確實如他們所宣稱的。 Trust Authority 會根據 IBM SecureWay Directory （有時稱爲 Lightweight Directory Access Protocol 或 LDAP）中的資訊，發出憑證給使用者。

Policy Director 接下來會使用那些憑證並且提供授權，它會確定每一個使用者只存取被允許的資源。 Policy Director 將其資訊儲存在該相同的 IBM SecureWay Directory 中。

您的電子商業 (e-business)可以使用單一的使用者定義來包含所有 Policy Director 許可權及所有 Trust Authority 資訊。如果您也將 SecureWay Boundary Server 資訊儲存在 IBM SecureWay Directory 中， Policy Director 也可以爲您管理。

第12章 SecureWay Boundary Server 基本要求及安裝注意事項

本章列出 SecureWay Boundary Server 的軟硬體基本要求。其中也提供與其它 SecureWay Boundary Server 產品整合的任何安裝注意事項。

SecureWay Boundary Server 軟硬體基本要求

SecureWay Boundary Server 元件產品的硬體基本條件位在表3 及第56頁的表4。

表 3. SecureWay Boundary Server 元件產品的硬體基本條件

SecureWay Boundary Server 元件	機型	磁碟空間	記憶體	其它
IBM SecureWay Firewall[1]	NT：Pentium® 133 MHz 或更高 AIX：支援 AIX 4.3.2 的 RS/6000 機器	NT： 24 MB[2] AIX： 307 MB	NT： 64 MB AIX： 64 MB	2 張網路介面卡
ACE/Server	NT： Pentium 166 MHz 或更高（僅單一處理器） AIX：支援 AIX 4.2 的機器	主伺服器軟體：50 MB 備份伺服器：22 MB 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
SurfinGate				
伺服器	Pentium 233 MHz 或更高	20 MB	最少： 128 MB 建議： 256 MB	
主控台	Pentium 233 MHz 或更高	15 MB	最少： 32 MB 建議： 64 MB	
MIMEsweeper for IBM SecureWay Release 2				
MAILsweeper	Pentium 200 MHz 或更高	1 GB	64 MB	1 張網路介面卡

表 3. SecureWay Boundary Server 元件產品的硬體基本條件 (繼續)

SecureWay Boundary Server 元件	機型	磁碟空間	記憶體	其它
WEBsweeper	Pentium 400 MHz 或更高	1 GB	128 MB 及每一個並行 Web 連線 1 MB	1 張網路介面卡

附註：

1. 請參閱 IBM Firewall 隨附的文件，取得其餘詳細資訊。
2. Netscape 瀏覽器也需要 13 MB 磁碟空間。

表 4. SecureWay Boundary Server 元件產品的軟體基本要求

SecureWay Boundary Server 元件	Microsoft Windows 平台		AIX	Solaris
	從屬站	伺服器	伺服器	伺服器
IBM SecureWay Firewall	Windows 95，IPSec 從屬站	Windows NT 伺服器 版本 4.0, Service Pack 5[1]	AIX 4.3.2	無法選用
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 或更高	Windows NT 伺服器 版本 4.0, Service Pack 5 或更高	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				
伺服器	無法選用	Windows NT 4.0[2]	無法選用	無法選用
主控台	Windows NT 4.0 或更高[2] Windows 95、Windows 98	無法選用	無法選用	無法選用
MIMEsweeper for IBM SecureWay Release 2				
MAILsweeper	無法選用	Windows NT 4.0[3]	無法選用	無法選用
WEBsweeper	Windows NT Workstation 4.0, Service Pack 3 或更高	Windows NT 4.0[4]	無法選用	無法選用

表 4. SecureWay Boundary Server 元件產品的軟體基本要求 (繼續)

SecureWay Boundary Server 元件	Microsoft Windows 平台		AIX	Solaris
	從屬站	伺服器	伺服器	伺服器

附註：

1. 請檢查 IBM Firewall for Windows NT 隨附的文件是否有要求任何必要的修訂程式。
2. 此外：
   - 需要有 Windows network client for Microsoft Windows。
   - Windows NT Workstation 未受支援。
3. 此外：
   - NT 3.5.1 及 Windows NT Workstation 未受支援。
   - 需要下列其中一種環境：
     - Microsoft Exchange
     - SMTP
     - cc:Mail™
     - Groupwise
     - Lotus Notes
4. 請參閱第60頁的『MIMEsweeper 注意事項』，取得 MIMEsweeper 建議。

SecureWay Boundary Server 元件注意事項

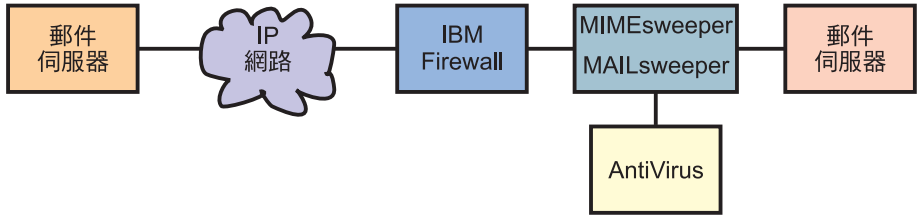
下列各節說明 SecureWay Boundary Server 元件產品的安裝及配置注意事項。

IBM Firewall 注意事項

IBM Firewall 的注意事項主要在於其安裝所在的流量和其它 SecureWay Boundary Server 產品的關係。

範例配置

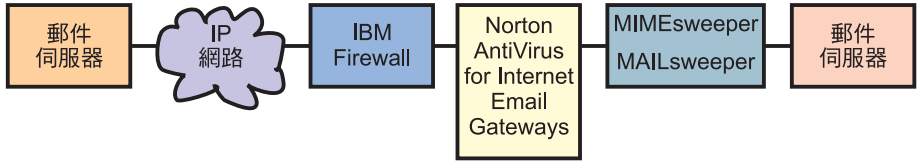
IBM Firewall 及 MAILsweeper 範例配置: 如果您同時安裝 IBM Firewall 及 MIMEsweeper，可使用本節說明的配置。



- MAILsweeper 是 MIMEsweeper 中，負責檢查郵件訊息內容的部份。MAILsweeper 中有一個功能可進行防毒檢查。

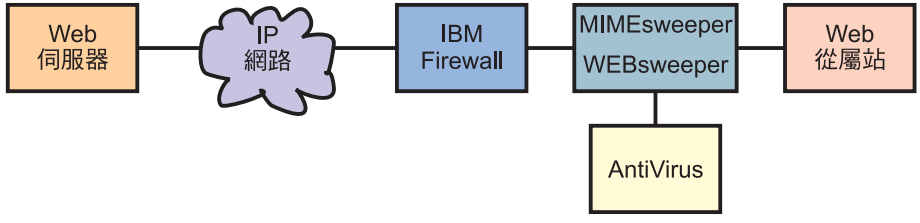
- MAILsweeper 位於 IBM Firewall 及安全 SMTP 伺服器之間。
- IBM Firewall 指向 MAILsweeper 作爲轉遞郵件的郵件主電腦。
  - IBM Firewall 需要設定預先定義郵件規則，使郵件流量可以順利串流。
- SMTP 伺服器也必須指向 MAILsweeper 作爲轉遞郵件的郵件主電腦。
- MAILsweeper 會檢查在雙向串流的已轉遞郵件訊息內容。

IBM Firewall、Norton AntiVirus for Internet Email Gateways 及 MIMEsweeper 範例配置: 如果您同時安裝 IBM Firewall 、 Norton AntiVirus for Internet Email Gateways 及 MIMEsweeper，可使用本節說明的配置。此實務將 IBM Firewall 、 Norton AntiVirus for Internet Email Gateways 及 MAILsweeper 合併在一個鏈結中，以檢查郵件中的病毒與內容，如以下圖解所示。



- 防火牆會指向 Norton AntiVirus for Internet Email Gateways 作爲其安全郵件伺服器。正確的防火牆規則必須設定爲容許此特定流量。
- Norton AntiVirus for Internet Email Gateways 指向 MAILsweeper 作爲其安全郵件的轉遞者，並將要出埠的郵件指向防火牆。
- MAILsweeper 會接收並且檢查轉遞進入的郵件。然後它會根據其遞送表或查閱 MX 記錄，將郵件轉遞至正確的伺服器。如果 MAILsweeper 及 Norton AntiVirus for Internet Email Gateways 位在相同的機器上，您必須變更 MAILsweeper 的接收埠，以避免和 Norton AntiVirus for Internet Email Gateways 發生衝突。

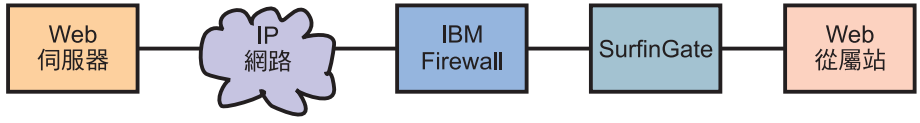
IBM Firewall 及 WEBsweeper 範例配置: 如果您同時安裝 IBM Firewall 及 MIMEsweeper，您可以使用本節說明的配置。



- WEBsweeper 是 MIMEsweeper 中，負責檢查 Web 流量的部份。 WEBsweeper 中有一個功能可進行防毒檢查。

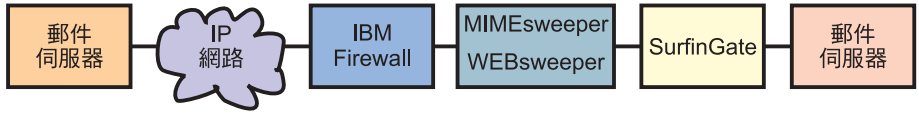
- WEBsweeper 的作用如同中間的 proxy。從屬站指向 WEBsweeper 作爲其 proxy。WEBsweeper 接下來設定轉遞流量至防火牆 proxy。
- 防火牆必須設定規則容許 proxy 流量。
- Proxy 要求只能來自位在防火牆後的安全網路。
- WEBsweeper 不處理 HTTPS。若要使用 HTTPS，您必須略過 WEBsweeper，以避免和防火牆間發生問題，並且確定所有 Web 流量都有經過檢查。您必須直接指向防火牆 proxy。Web 流量仍然維持安全，不過不是由 WEBsweeper 檢查。

IBM Firewall 及 SurfinGate 範例配置: 如果您同時安裝 IBM Firewall 及 SurfinGate，您可以使用本節說明的配置。



- SurfinGate 會檢查 ActiveX control 及其它項目的 Web 流量。
- SurfinGate 作用如同中間的 Web proxy。從屬站指向 SurfinGate 作爲其 HTTP、FTP 及 HTTPS 的 proxy。 SurfinGate 然後轉遞要求至 IBM Firewall proxy。
- 防火牆必須設定規則容許 proxy 流量。
- Proxy 要求只能來自位在防火牆後的安全網路。

IBM Firewall、MIMEsweeper 及 SurfinGate 範例配置: 如果您同時安裝 IBM Firewall 、 MIMEsweeper 及 SurfinGate，您可以使用本節說明的配置。



- SurfinGate 會檢查 ActiveX control 及其它項目的 Web 流量。它使用和 MIMEsweeper 的 WEBsweeper 元件不同的檢查方式。
- SurfinGate 及 WEBsweeper 作用如同中間的 Web proxy。從屬站指向 SurfinGate 作爲其 HTTP 及 FTP 的 proxy。 SurfinGate 然後轉遞要求至 WEBsweeper。WEBsweeper 則轉遞要求至 IBM Firewall proxy。
- 防火牆必須設定規則容許 proxy 流量。這些規則定義於 *IBM eNetwork Firewall Version 3.3 for Windows NT User's Guide*。
- Proxy 要求只能來自位在防火牆後的安全網路。

- WEBsweeper 不處理 HTTPS。使用 HTTPS 時，爲了避免和防火牆發生問題，並且確定所有 Web 流量都有經過檢查，您必須略過 WEBsweeper。您必須直接指向防火牆 proxy。Web 流量仍然維持安全，不過不是由 WEBsweeper 檢查。

MIMEsweeper 注意事項

以下是典型的 WEBsweeper 系統：

- Intel Pentium 400 MHz 或更高
- 1GB 磁碟空間及 128 MB RAM
- Windows NT Server 或 Workstation Version 4.0 Server Service Pack 3 或更高
- TCP/IP 通信協定，包括一台主電腦及領域名稱
- 防毒工具

以下是典型的高容量 WEBsweeper 環境，至少有 500 個並行使用者：

- 一部雙 Intel Pentium II, 450 MHz 或更高
- 3GB 磁碟空間及 256 MB RAM
- Windows NT Server 或 Workstation 版本 4.0 Server Service Pack 3 或更高
- TCP/IP 通信協定，包括一台主電腦及領域名稱
- 防毒工具

如果您的環境支援 500 個以上並行使用者，則建議使用多部 WEBsweeper 伺服器。

第13章 免入侵基本要求及安裝注意事項

本章列出免入侵元件 Tivoli Cross-Site for Security 及 Norton AntiVirus 的軟硬體基本要求。

預防侵入的軟硬體基本要求

下節說明免入侵元件產品的安裝及配置文件。

Tivoli Cross-Site for Security 的軟硬體基本要求顯示在表5、第62頁的表6及第62頁的表7。 Norton AntiVirus 元件產品的軟硬體基本要求顯示在第62頁的表8及第63頁的表9。

表 5. Tivoli Cross-Site for Security 伺服器的軟硬體基本要求

伺服器基本要求	
作業系統	• AIX 4.3.2 • Windows NT 版本 4.0, Service Pack 5 • Solaris 2.5.1 或 2.6
Java	JDK 1.1.6 修訂版 04 或更新版
Web 伺服器	Netscape Enterprise Server 3.51
資料庫	• IBM DB2 版次 5.2 • Oracle 7.3.4（或建議 8.0.4） • Microsoft SQL Server
磁碟空間	• Windows NT 290 MB • AIX 180 MB • Solaris 180 MB
記憶體	256 MB
交換空間	300 MB（建議 400 MB）
註: 1. Netscape Enterprise Server 3.51 及 3.6 未受支援。 2. 請參閱 Tivoli Cross-Site for Security 安裝文件中對 Solaris 修正檔的基本要求。	

表 6. Tivoli Cross-Site for Security 管理主控台的軟硬體基本要求

管理主控台基本要求	
作業系統	• Windows 95 • Windows 98 • Windows NT 版本 4.0, Service Pack 5（166 MHz 或建議速度更高的機器） • 在 Sun SPARC 上執行的 Solaris 2.5.1 或 2.6
磁碟空間	25 MB - 所有平台
記憶體	• Windows NT 40 MB • AIX 64 MB • Solaris 40 MB

表 7. Tivoli Cross-Site for Security 代理程式的軟硬體基本要求

代理程式基本要求	
作業系統	• Windows NT 版本 4.0, Service Pack 5 或更新版 • AIX 4.3.2 • 在 Sun SPARC 上執行的 Solaris 2.5.1 或 2.6
Java	JDK 1.1.6 修訂版 04 或更新版（僅 UNIX 才需要）
磁碟空間	• 在 Windows NT 需 15 MB • 在 AIX 需 10 MB • 在 Solaris 需10 MB
記憶體	• 在 Windows NT 需 32 MB • 在 AIX 需 32 MB • 在 Solaris 需 20 MB
註: 1. Netscape Enterprise Server 3.51 及 3.6 未受支援。 2. 請參閱 Tivoli Cross-Site for Security 安裝文件中對 Solaris 修正檔的基本要求。	

表8列出 Norton AntiVirus 的硬體基本條件。

表 8. Norton AntiVirus 的硬體基本條件。

免入侵元件	**機型**	**磁碟空間**	**記憶體**	**其它**
Norton AntiVirus	Intel CPU	24 MB	最少： 16 MB 建議： 32 MB	光碟機

表 8. Norton AntiVirus 的硬體基本條件。 (繼續)

免入侵元件	機型	磁碟空間	記憶體	其它
Norton AntiVirus for Internet E-mail Gateways	Pentium 133 或更高	6 MB	32 MB	光碟機 500 MB 至 5 GB 以使郵件作業更有效率

表 9. Norton AntiVirus 的軟體基本要求

免入侵元件	Microsoft Windows 平台		OS/2
	從屬站	伺服器	從屬站
Norton AntiVirus[1]	Windows NT 4.0 Windows 95、Windows 98	Windows NT 4.0	OS/2 2.11 或更新版
附註： 1. 此外，Norton AntiVirus for Internet Email Gateways 需要 TCP/IP 網際網路連線。			

Norton AntiVirus 未提供 AIX 及 Solaris 版。

Tivoli Cross-Site for Security 安裝注意事項

以下圖例顯示 Cross-Site for Security 代理程式及 Cross-Site for Security 管理伺服器在電子商業網路中的典型的位置。

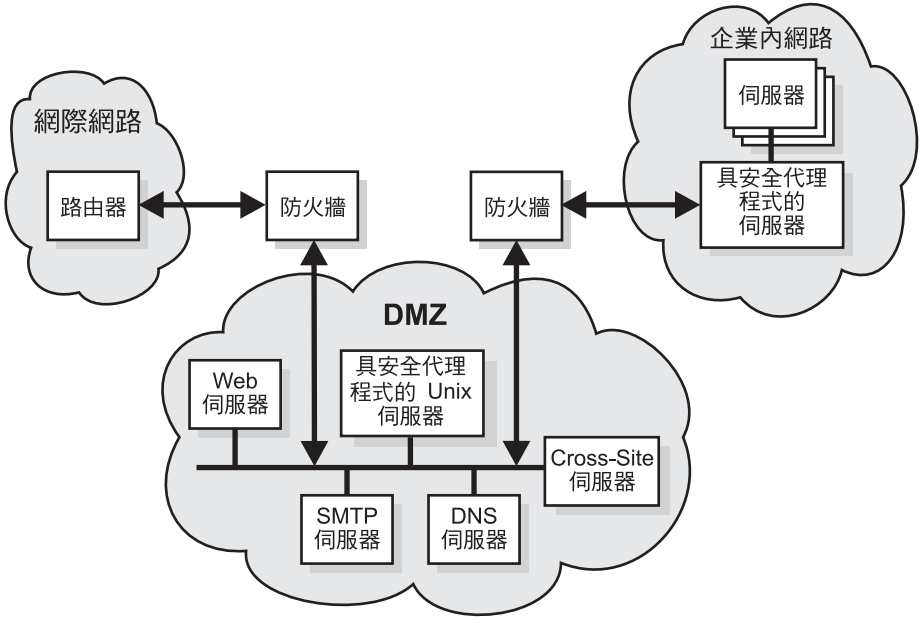


圖 11. 將 Cross-Site for Security 管理伺服器安裝在 DMZ

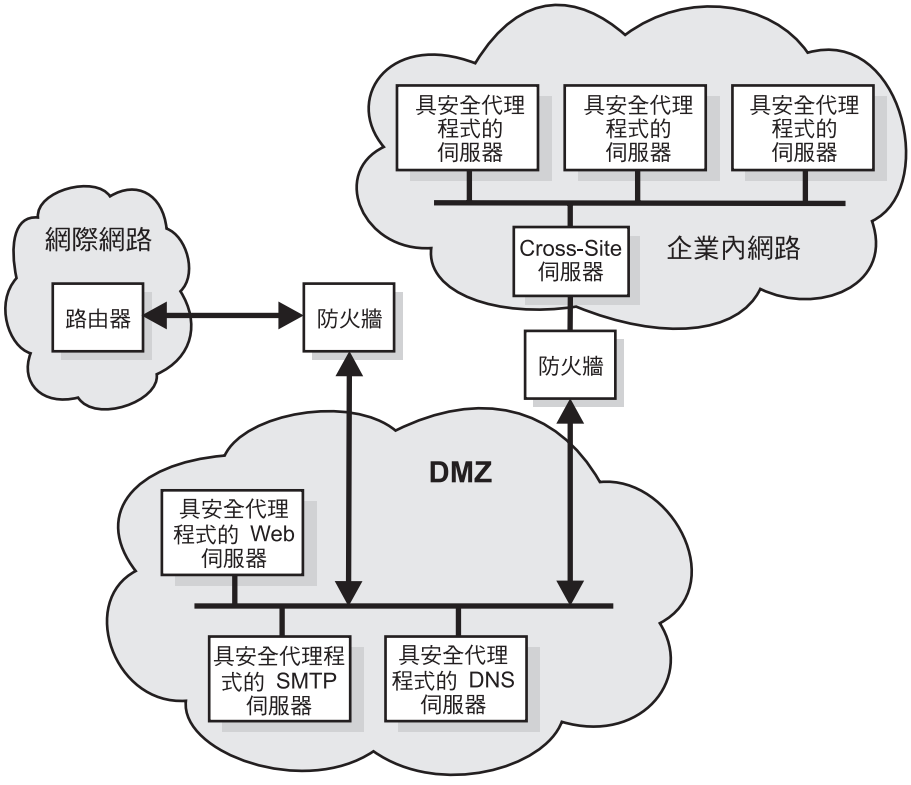


圖 12. 將 Cross-Site for Security 管理伺服器安裝在您的企業內網路

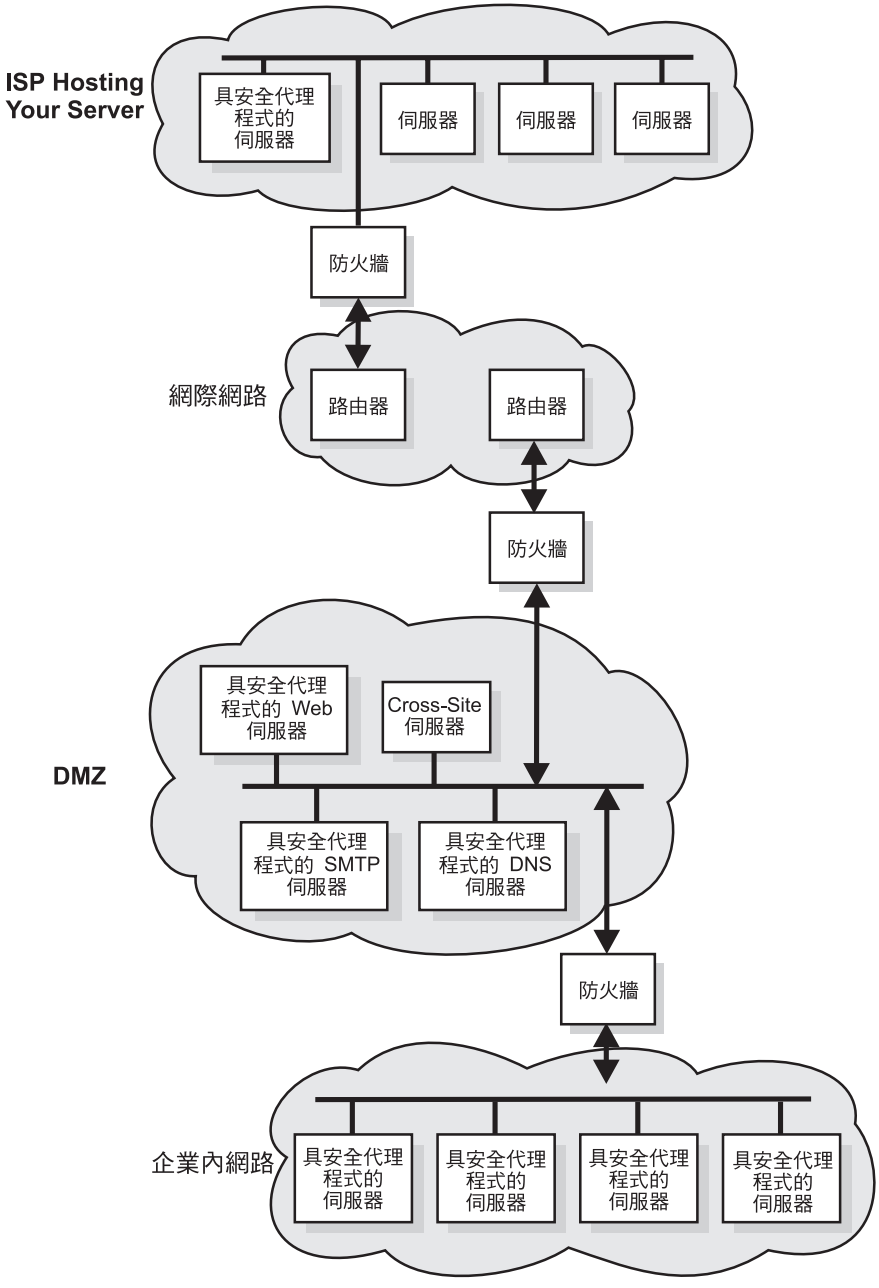


圖 13. 將 Cross-Site for Security 管理伺服器安裝在支援網際網路連線的 DMZ 內

Norton AntiVirus 安裝注意事項

有關安裝 Norton AntiVirus 的資訊位在產品根目錄下的 contents.txt 檔案中。

第14章 公開金鑰基礎建設基本要求及安裝注意事項

今日的公司需要有公開金鑰基礎架構以保障電子商業應用程式的安全，而 FirstSecure Trust Authority 提供兩層功能可施行公開金鑰基礎架構：

- 數位式憑證的完整生命週期管理可提供：
  - 申請、重訂及廢止憑證的能力
  - 一個註冊管理中心可核准憑證申請
  - 一個憑證管理中心可建立數位式憑證及廢止清單
- 強化的註冊功能，可讓企業在線上登錄其可靠的電子商業 (e-business)實體。登錄應用程式建立在下列原則上：
  - 發出及管理的憑證必須是敏感的電子商業應用程式所要求的信任，並且註冊管理中心的建立方式必須符合相同的高信任與安全基本要求。
  - 應用程式必須提供足夠的彈性，支援各種登錄政策，包括手動或自動鑑別、彈性的線上或離線鑑別，及將登錄政策隔離爲不同信任領域的選項。

信任模式有助於保證您的電子交易的可存取性、保密性、完整性及原始性。透過數位加密、憑證及簽章，Trust Authority 可讓您透過網際網路、企業內網路或虛擬專用網路進行安全的電子商業 (e-business)。爲了延伸其簽認金鑰的安全，憑證管理中心設計爲可和加密硬體配合使用。

Trust Authority 伺服器軟硬體基本要求

Trust Authority 元件的伺服器軟體基本要求列出在表10。

表 10. 公開金鑰基礎建設Trust Authority 元件的伺服器軟體及選用的硬體基本條件

產品	附註
下列其中一種作業系統： • IBM AIX/6000 （AIX），版本 4.3.2 • Microsoft Windows NT，版本 4.0 具有 Service Pack 5	• 必要項目。 • 您必須將所有 Trust Authority 伺服器程式安裝在相同的平台上。您不能在相同的系統配置中，混合 AIX 及 Windows NT 機器。
IBM SecureWay Directory 版本 3.1.1	• 必要項目；與 Trust Authority 程式碼整合。 • 安裝 Trust Authority 時，可以將 Directory 軟體安裝在和 Trust Authority 相同的機器上，也可以將其安裝在遠端機器上。

表 10. 公開金鑰基礎建設Trust Authority 元件的伺服器軟體及選用的硬體基本條件 (繼續)

產品	附註
IBM WebSphere Application Server 版本 2.02，標準版。包括 IBM HTTP Server 版本 1.3.3 及 Sun Java Development Kit （JDK） 1.1.7。	• 必要的；隨附在 Trust Authority 媒體包中。 • 安裝 Trust Authority 之前，您必須先將 Web 伺服器軟體安裝在和計畫要安裝 Trust Authority 及 Trust Authority 伺服器軟體的相同機器上。
IBM DB2 Universal Database Enterprise Edition 版本 5.2 具有維護修正檔 9。	• 必要的；隨附在 Trust Authority 媒體包中。 • 每一個伺服器元件都有一個唯一的資料庫案例存在。安裝 Trust Authority 之前，您必須在計畫要作爲 Trust Authority 伺服器的每一台機器上安裝 DB2。
• IBM SecureWay 4758 PCI Cryptographic Coprocessor, Model 001 • IBM SecureWay 4758 CCA Support Program，版本 1.3.0.0 具有維護修正檔 1.3.0.1	• *選用的*，僅 AIX 系統具有；您必須透過 IBM 一般的訂購方式訂購此產品。 • 安裝 Trust Authority 之前，您必須將 4758 硬體及支援程式安裝在計畫要安裝 Trust Authority CA 的伺服器上。 • 4758 加密卡需要一個 RS/6000 上的 PCI 匯流排。

表11及第69頁的表12列出 Trust Authority 的伺服器硬體基本條件。

在表11 及第69頁的表12 上：

- 一個小型生產環境，每天會發出上百張憑證。
- 一個中型生產環境，每天會發出上千張憑證。
- 一個大型生產環境，每天會發出無數張憑證。它也可能是提供協力廠商 CA 服務給其它組織的系統。

如果您計畫在 Windows NT 中執行 Trust Authority， IBM 建議您將其安裝在 IBM Netfinity® 伺服器上。下表根據您預期要透過 Trust Authority 憑證管理中心發出的憑證數目，提供系統估算建議。

表 11. 範例 Windows NT 機器配置

機型	處理器	磁碟空間	記憶體
小型生產環境			
Netfinity 3000	1 （450 MHz, Pentium II）	2 部磁碟機 （9.1 GB）	256 MB
Netfinity 5000	2 （450 MHz, Pentium II）	2 部磁碟機 （9.1 GB）	512 MB
中型生產環境			

表 11. 範例 Windows NT 機器配置 (繼續)

機型	處理器	磁碟空間	記憶體
Netfinity 3000	1 （500 MHz, Pentium III）	4 部磁碟機 （18.2 GB）	768 MB
Netfinity 5000	2 （500 MHz, Pentium III）	4 部磁碟機 （9.1 GB）	1 GB
大型生產環境			
Netfinity 5500	2 （450 MHz, Pentium III）	4 部磁碟機 （9.1 GB 高速）	1 GB
Netfinity 5500	4 （500 MHz, Pentium III Xeon with 1024K L2 Cache）	4 部磁碟機 （9.1 GB 高速）	1 GB
Netfinity 7000	2 （500 MHz, Pentium III with 512K L2 Cache）	4 部磁碟機（9.1 GB 高速）	1 GB
Netfinity 7000	4 （500 MHz, Pentium III Xeon with 1024K L2 Cache）	4 部磁碟機 （18.2 GB）	2 GB

如果您計畫在 AIX 上執行 Trust Authority，您必須將其安裝在 IBM RISC System/6000® 機器上。下表根據您預期要透過 Trust Authority 憑證管理中心發出的憑證數目，提供系統估算建議。

表 12. 範例 AIX 機器硬體配置

機型	處理器	磁碟空間	記憶體
小型生產環境			
F40	2 （233 MHz）	2 部磁碟機 （9.1 GB, Ultra 2 Fast Wide）	512 MB
中型生產環境			
F40	2 （233 MHz）	3 部磁碟機 （9.1 GB, Ultra 2 Fast Wide）	1 GB
大型生產環境			
F50	4 （332 MHz）	5 部磁碟機（1 個 9.1 GB Ultra 2 Fast Wide 加上 4 個 9.1 GB SSA）	2 GB

表 12. 範例 AIX 機器硬體配置 (繼續)

機型	處理器	磁碟空間	記憶體
H50	4 （332 MHz）	5 部磁碟機（1 個 9.1 GB Ultra 2 Fast Wide 加上 4 個 9.1 GB SSA）	2 GB
R50	6 （200 MHz）	2 部磁碟機 （9.1 GB Ultra 2 Fast Wide）	1 GB
R50	8 （200 MHz）	5 部磁碟機（1 個 9.1 GB Ultra 2 Fast Wide 加上 1 個 7133 SSA Rack 具有 4 個 9.1 GB SSA）	2 GB

Trust Authority 從屬站軟硬體基本要求

IBM 建議以下列工作站配置使用瀏覽器登記表格及用來執行 Trust Authority 從屬站應用程式。

- 下列實體機器設定：
  - 至少 166 MHz Intel 486 處理器，具有 32 MB 記憶體，（建議爲 200 MHz Intel Pentium 處理器，至少 64 MB 記憶體）
  - 圖形卡
  - VGA 影像顯示，或更好
  - 滑鼠或滑鼠相容指標裝置
- 下列其中一種作業系統：
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT，版本 4.0
- 下列其中一種 Web 瀏覽器：
  - Netscape Navigator 或 Netscape Communicator，版本 3.0 或更新版
  - Microsoft Internet Explorer，版本 4.0 或更新版，啓用 Java。

IBM KeyWorks Toolkit 及 IBM SecureWay Trust Authority 互動

請勿將 IBM KeyWorks Toolkit 安裝在和 IBM SecureWay Trust Authority 相同的伺服器上。

第15章 工具箱安裝基本要求及注意事項

FirstSecure 工具箱是一組 API，可協助您的電子商業發展安全的應用程式。

- 授權服務
- 憑證及管理服務
- 目錄服務
- 安全 SOCKETS 層次通信協定服務
- KeyWorks 加密及信任管理服務
  - IBM Key Recovery Service Provider 1.1.3.0 API。IBM Key Recovery Service Provider 可回復加密的資訊。
  - IBM Key Recovery Server 1.1.3.0。IBM Key Recovery Server 1.1.3.0 是一支應用程式，在接到獲授權的要求時，可在沒有金鑰、遺失或損壞的情況下回復加密的資訊。

    這兩個工具集提供標準介面，可讓應用程式用來啓動關鍵的安全服務及安全產品公司可插入其工具集的標準介面。標準介面是以一般資料安全架構（CDSA） 爲基礎。這些工具集提供 Windows NT、Solaris 及 AIX 版。

工具箱軟硬體基本要求

工具箱的硬體基本條件顯示在表13。

表 13. 工具箱的硬體基本條件

平台	磁碟空間	記憶體
版本 4.0, Service Pack 5	2 - 4 GB	64 MB
AIX 4.3.2	9.1 GB	1 GB
Sun Solaris, 版本 2.6 具有 May 1999 Fix Pak	4.2 GB	128 MB

表 14. 工具箱元件產品的硬體基本條件

工具集	機型	磁碟空間	記憶體
IBM KeyWorks Toolkit	可支援產品在以下環境執行的硬體： Windows NT 版本 4.0, Service Pack 5 或更新版 Windows 95 AIX 4.2 或更新版 Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	可支援產品在以下環境執行的硬體： Windows NT 版本 4.0, Service Pack 5 或更新版 Windows 95 AIX 4.2 或更新版 Sun Solaris	50 MB	32 MB

工具箱元件產品的軟體基本要求顯示在以下表格中。

表 15. 工具箱元件產品的軟體基本要求

工具箱元件	Microsoft Windows 平台		AIX	Solaris
	從屬站	伺服器	伺服器	伺服器
IBM KeyWorks Toolkit	Windows NT 版本 4.0, Service Pack 5 或更新版 Windows 95	Windows NT 版本 4.0, Service Pack 5 或更新版 Windows 95	AIX 4.2 或更新版[1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT 版本 4.0, Service Pack 5 或更新版[2] Windows 95	Windows NT 版本 4.0, Service Pack 5 或更新版	AIX 4.2 或更新版	Sun Solaris
附註： 1. 亦支援 AIX 從屬站。 2. 此外也需要 IBM KeyWorks Toolkit。				

IBM KeyWorks Toolkit 1.1

IBM KeyWorks Toolkit 1.1 提供應用程式開發者一個開放並且可擴充的標準方法，存取不同作業環境內的加密及其它安全功能。

IBM KeyWorks Toolkit 提供標準介面 (API)，讓應用程式用來啓動關鍵的加密、信任與安全服務，及安全產品公司的附加模組可作爲和工具集的介面。這些標準介面都是以「一般資料安全架構」(CDSA) 爲基礎，這是來自 Open Group 的標準，最初由 Intel™ Corporation 開發，後來 IBM 將其延伸入 KeyWorks Toolkit。使用標準介面時：

- 您的公司可以選擇最適合的加密及信任施行方式，而不需要變更使用安全服務的應用程式。
- 可提高應用程式及中介軟體程式設計師的生產力。

IBM KeyWorks Toolkit 在應用程式與作爲類別的中介軟體之間，及加密功能與服務提供者之間提供一個隔離層。工具集中包含一個組織架構及「服務提供者」plug-in 模組。

對於應用程式而言，組織架構提供功能豐富的「一般安全服務管理程式」(CSSM) API（Intel Corporation 的 CDSA）。 IBM 延伸 CSSM API 功能，加入金鑰回復功能。如果您使用 IBM KeyWorks Toolkit，您的應用程式可以：

- 加密及解密資訊

- 針對多種目的驗證數位簽章
- 從目錄擷取憑證及憑證廢止清單
- 建立金鑰回復欄位，作爲金鑰回復與加密備份使用
- 根據使用者指示系統設計者及程式設計師建立的基準，決定憑證是否可靠

一般而言，企業或 OEM 會以容許在 CSSM 組織架構上使用 CSSM API 的方式，將 IBM KeyWorks Toolkit 及 IBM Key Recovery Service Provider Toolkit 與應用程式和中介軟體整合。此整合中的產品是一組伺服器與從屬站的執行時間應用程式及中介軟體，這些伺服器與從屬站會分散在一或多個作業環境中。 FirstSecure 的其它元素會依靠 IBM KeyWorks Toolkit 進行所有加密服務及信任政策作業。

使用 IBM KeyWorks Toolkit 進行整合者，需有在加密設計與程式設計及中介軟體與組織架構方面具有廣博經驗的系統工程師與程式設計師可提供協助，或可取得具有此種經驗的契約整合者或 OEM 的協助。

對於服務提供者而言，此組織架構提供標準「服務提供者介面」，即 Open Group 的 CDSA。 IBM 已強化 SPI，加入金鑰回復功能。

IBM KeyWorks Toolkit (SDK) 包括 plug-in 服務提供者模組，可支援開放標準及專有公開金鑰憑證。這些模組包括 PKCS#11、RSA Data Security 的 BSAFE 加密功能、 X.509V3 憑證、Entrust 與 Verisign 的信任政策，及 Lightweight Directory Access Protocol （LDAP）。此組織架構提供無縫式整合由獨立的服務提供者模組提供的加密、信任及安全功能。

IBM KeyWorks Toolkit 可提供關鍵管理功能，包括：

- 防止略過 KeyWorks 支援程序中的關鍵步驟保護
- 在使用之前，驗證服務提供者模組的 plug-in 模組未被變更
- 服務提供者 plug-in 模組只透過組織架構使用
- 支援國家別及加密法別的加密與信任政策用法

IBM KeyWorks Toolkit 提供您的公司下列優點：

- 可讓您變更或取代服務提供者模組，而不需要重新撰寫應用程式及中介軟體
- 提供無縫式支援硬體加密及數位簽章
- 支援 LDAP 目錄及 DSA 簽章標準
- 不要求使用任何特定的憑證管理中心

有關 IBM KeyWorks Toolkit 的其餘資訊位在 *IBM KeyWorks Toolkit 開發人員手冊*一書中。

IBM KeyWorks Toolkit 及 IBM SecureWay Trust Authority 互動

請勿將 IBM KeyWorks Toolkit 安裝在和 IBM SecureWay Trust Authority 相同的伺服器上。

IBM Key Recovery Service Provider Toolkit 1.1

IBM Key Recovery Service Provider 1.1.3.0 是以工具集格式提供，是一個「服務提供者」模組，它使用 IBM KeyWorks Toolkit 提供的標準功能。 IBM Key Recovery Service Provider 可回復儲存的及傳輸的加密資訊，不需要先收集和認證私密金鑰與建立加密單一點的弱點。

由於 IBM Key Recovery Service Provider 使用由 IBM KeyWorks Toolkit 提供的標準功能，金鑰回復功能可使用在不同的加密供應商、來自各個憑證管理中心的標準憑證、來自 Verisign 及 Entrust 的信任政策及任何可由 LDAP 存取的目錄。IBM Key Recovery Service Provider 會根據與往來雙方的通信相關的階段作業，建立金鑰回復資訊。

有關 IBM Key Recovery Service Provider 的其餘資訊位在*金鑰回復伺服器安裝與用法手冊*中，此書隨附在 FirstSecure 文件包中。

第16章 FirstSecure 隨附的文件

FirstSecure 中內含的每一個元件產品都有提供其本身的文件。本章提供有關每一個 FirstSecure 元件產品隨附的文件資訊。

SecureWay FirstSecure、SecureWay Policy Director 及 SecureWay Boundary Server 有隨附媒體包及文件包。媒體包中包含產品 CD，可用來安裝內含的元件產品，並且部份 CD 中也包含線上文件。文件包中包含其隨附的元件產品硬本書籍。 第84頁的『FirstSecure 文件包』列出文件包的內容。

Policy Director

以下文件隨附於 Policy Director 元件產品中。

IBM SecureWay Policy Director Up and Running
說明如何安裝及架構 IBM SecureWay Policy Director。

IBM SecureWay Policy Director Administration Guide
說明如何管理 IBM SecureWay Policy Director。此書以 PDF 格式提供。

IBM SecureWay Policy Director Programming Guide and Reference
說明如何撰寫 IBM SecureWay Policy Director 程式。此書以 PDF 格式提供。

產品 readme
此資訊型在此 Web 網址取得：www.ibm.com/software/security/policy

SecureWay Boundary Server

以下書籍說明 SecureWay Boundary Server 的元件產品、其基本要求及它們之間的互動。

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running
說明 SecureWay Boundary Server 元件產品的硬本書籍。

下節說明 SecureWay Boundary Server 元件產品隨附的文件。

IBM SecureWay Firewall

所有 IBM Firewall 文件均以軟本提供。IBM Firewall 提供下列文件：

IBM SecureWay Firewall for AIX Setup and Installation
安裝及設置 IBM SecureWay Firewall for AIX 的指示。

IBM SecureWay Firewall for Windows NT Setup and Installation
安裝及設置 IBM SecureWay Firewall for Windows NT 的指示。

IBM SecureWay Firewall for AIX User's Guide
安裝及設置 IBM SecureWay Firewall for Windows NT 的指示。

IBM SecureWay Firewall for Windows NT User's Guide
有關使用 IBM Firewall for Windows NT 的資訊。

IBM SecureWay Firewall for Windows NT Reference
包含關於使用 IBM Firewall for Windows NT 的參考資訊。

IBM SecureWay Firewall for AIX Reference
包含關於使用 IBM Firewall for AIX 的參考資訊。

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
包含判斷問題的指示。

IBM SecureWay Firewall VPN Client User's Guide
說明如何設定及使用虛擬專用網路。

MIMEsweeper

MIMEsweeper 提供下列文件：

MIMEsweeper 管理手冊
包含「版本注意事項」，其後是供管理者參考的資訊，包括規劃及安裝資訊。

本書在產品 CD 上以 HTML 格式提供。您可以使用 Web 瀏覽器，在線上檢視檔案 \DOC\MANUAL.HTM。

MIMEsweeper 版本注意事項
包含已更新的文件，包括安裝資訊及在線上檢視文件的指示。

本書在產品 CD 上以 HTML 格式提供。您可以使用 Web 瀏覽器，在線上檢視檔案 \DOC\RELNOTES.HTM。

MIMEsweeper 配置編輯程式說明
包含有關編輯 MIMEsweeper 配置檔的資訊。

此文件在產品 CD 上以 HTML 格式提供。

SurfinGate

SurfinGate 提供下列軟本文件：

SurfinGate 安裝手冊

有關在 Windows NT 上安裝及架構 SurfinGate 4.05 元件的資訊。在產品 CD 上有一份 *SurfinGate 安裝手冊* 的 PDF 版本，檔名爲：\docs\install.pdf。

SurfinGate 使用者指南

有關規劃及使用 SurfinGate 的資訊。在產品 CD 上有一份 *SurfinGate 使用者指南*的 PDF 版本，檔名爲：\docs\manual.pdf。

SurfinGate 4.05 for Windows NT 版本注意事項

有關 SurfinGate 4.05 的資訊，包括系統需求及產品限制。在產品 CD 上有一份 *SurfinGate 4.05 for Windows NT 版本注意事項*的 PDF 版本，檔名爲：\docs\relnotes.pdf。

SurfinGate for Windows NT/UNIX Solaris 版本注意事項，附錄 A

討論 SurfinGate 的變更之線上文件。此文件位在產品 CD 上，檔名爲：\docs\rnappen.pdf。

免入侵

下說明免入侵元件產品隨附的文件。

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security, 版本 1.1 以 .pdf 格式提供下列文件：

Tivoli Cross-Site for Security Installation

此文件提供安裝作業的明細基本要求並引導您經過每一個安裝步驟。

Tivoli Cross-Site for Security User's Guide

此文件提供產品概觀、使用主控台及執行作業的指示、參考資料（如指令行介面）、配置檔及名詞解釋。您可以從產品 CD-ROM 上存取此文件。

Norton AntiVirus

Norton AntiVirus 包括 FirstSecure 中支援的下列元件文件。除了 contents.txt 檔案外，所有文件在 Norton AntiVirus CD 上都是以 PDF 格式提供。 contents.txt 檔在產品 CD 上是 ASCII 格式。

Norton AntiVirus Solution Release 3.04 CD 文件內容

Norton AntiVirus Solution Release 3.04 CD 檔案 \contents.txt 列出 CD 上包含的所有文件。

管理解決方案:

Norton AntiVirus Solution Implementation Guide
請參閱產品 CD 上的 \docs\admin\navimp.pdf。

Norton AntiVirus Command-Line Scanner
請參閱產品 CD 上的 \docs\navc\navcugd.pdf。

Emergency Rescue Disk creation
請參閱產品 CD 上的 \navc\readme.txt。

伺服器解決方案:

Norton AntiVirus for Windows NT Server Administrator's Guide
請參閱產品 CD 上的 \docs\admin\navnts50.pdf。

Norton AntiVirus for NetWare User's Guide
請參閱產品 CD 上的 \docs\NAVNLM\NVN4.pdf。

Norton AntiVirus for Lotus Notes Installation Guide
請參閱產品 CD 上的 \docs\NAVNOTES\NAVNOTES.pdf。

Norton AntiVirus for Lotus Notes Installation Guide
請參閱產品 CD 上的 \docs\NAVNOTES\NAVNOTES.pdf。

Norton AntiVirus for OS/2 Lotus Notes Installation Guide
請參閱產品 CD 上的 \docs\NOTESOS2\NOTESOS2.pdf。

Norton AntiVirus for Microsoft Exchange Installation Guide
請參閱產品 CD 上的 \docs\NAVXCHNG\NAVXCHNG.pdf。

閘道解決方案:

Norton AntiVirus for Internet Email Gateway User's Guide
請參閱產品 CD 上的 \docs\navieg\navieg.pdf。

Norton AntiVirus for Firewalls Administrator's Guide
請參閱產品 CD 上的 \docs\navfw\navfw.pdf。

桌上管理程式解決方案:

Norton AntiVirus User's Guide for Windows 3.1/DOS
請參閱產品 CD 上的 \docs\navwks\nav4dusr.pdf。

Norton AntiVirus Reference Guide for Windows 3.1/DOS
請參閱產品 CD 上的 \docs\navwks\nav4dref.pdf。

Norton AntiVirus for Windows 95/98 User's Guide
請參閱產品 CD 上的 \docs\navwks\nav98usr.pdf。

Norton AntiVirus for Windows 95/98 Reference Guide
請參閱產品 CD 上的 \docs\navwks\nav98ref.pdf。

Norton AntiVirus for Windows NT User's Guide
請參閱產品 CD 上的 \docs\navwks\nav5nusr.pdf。

Norton AntiVirus for Windows NT Reference Guide
請參閱產品 CD 上的 \docs\navwks\nav5nref.pdf。

Norton AntiVirus v4.0 User's Guide for Windows NT
請參閱產品 CD 上的 \docs\351\navntugd.pdf。

Norton AntiVirus v4.0 Reference Guide for Windows NT
請參閱產品 CD 上的 \docs\351\navntref.pdf。

Norton AntiVirus User's Guide for OS/2
請參閱產品 CD 上的 \docs\navos2\navos2ug.pdf。

Norton AntiVirus Distribution Guide for OS/2
請參閱產品 CD 上的 \docs\navos2\navos2dg.pdf。

Norton AntiVirus for Macintosh User's Guide
請參閱產品 CD 上的 \docs\navmac\navmac.pdf。

Norton AntiVirus Solution Release 3.04 CD 上的白皮書: 此 CD 在目錄 \sarc 中包含白皮書。所有白皮書都是 .pdf 格式。

Norton AntiVirus Solution Release 3.04 CD 上的視訊: 此 CD 亦包含視訊。如果要檢視視訊，您必須具有媒體播放程式或其它可播放 .AVI 檔案的程式。視訊位在下列檔案中：

SARC \sarc\sarc.avi

關於病毒
\sarc\aboutvir.avi

Norton AntiVirus： 導遊指南
\navtour\guided\demo32.exe

Norton AntiVirus 提出警示時如何回應
\navtour\alert\demo32.exe

Norton 系統中央一遊
\nsctour\setup.exe

或者，直接從 CD 執行

\nsctour\demo32.exe

有關其它導遊的資訊位在檔案 \ncstour\readme.txt 中

Trust Authority

IBM SecureWay Trust Authority 產品文件在 *Trust Authority 文件* CD-ROM 上是以可攜式文件格式 （PDF） 及 HTML 格式提供。其中許多資訊都已翻譯成 Trust Authority 支援的語言。如需取得如何存取您需要的語言之出版品，請參閱產品中的 *Readme* 檔。 *Readme* 檔的最新版本位在 IBM SecureWay Trust Authority 網站的 Library 頁面，其網址爲： http://www.ibm.com/software/security/trust/library

Trust Authority 書庫包括下列文件：

IBM SecureWay Trust Authority 更新與執行
此書是該產品概觀。其中列出產品基本要求（包括安裝程序），並提供有關如何存取每一個產品元件的線上說明資訊。本書除了可在文件 CD-ROM 上取得外，也以硬本格式隨產品一起配送。

IBM SecureWay Trust Authority 系統管理手冊
本書包含有關管理 Trust Authority 系統的一般資訊。其中包括啓動及停止伺服器的程序、變更密碼、管理憑證管理中心、執行審核及執行資料完整性檢查。

IBM SecureWay Trust Authority 配置手冊
本書包含有關如何使用安裝精靈架構 Trust Authority 系統的資訊。在檢視精靈的線上說明時，您可以存取此指南的 HTML 版本。

IBM SecureWay Trust Authority RA桌面手冊
本書包含有關如何使用 RA 桌面 管理憑證的整個生命週期的資訊。在檢視桌上管理程式的線上說明時，您可以存取此指南的 HTML 版本。

IBM SecureWay Trust Authority 使用手冊
本書包含有關如何取得憑證的資訊。其中提供如何使用 Trust Authority 登記表格，申請瀏覽器、伺服器及裝置的憑證之程序。同時也說明使用者應如何預先登記 PKIX 憑證，及如何使用 Trust Authority 從屬站儲存與管理 PKIX 憑證。在檢視從屬站的線上說明時，您可以存取此指南的 HTML 版本。

工具箱

下節說明工具箱元件產品隨附的文件

工具箱 API

所有工具箱文件都可在以下網站取得：
www.ibm.com/software/security/firstsecure/library。包含下列文件：

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference
提供 API 及 iKeyman 的概觀。定義每一個 API、其語法及用法。

IBM SecureWay Directory Client SDK Programming Reference
包括各種 LDAP 範例從屬站程式及一個 LDAP 從屬站檔案庫，提供存取 LDAP 伺服器的應用程式。支援 C 及 Java。

IBM SecureWay Policy Director Programming Guide and Reference
定義每一個 API、其語法及用法。

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide
提供安裝指示及基本要求資訊。

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
提供程式設計師有關使用 IBM SecureWay 多平台 X.509 公開金鑰基礎建設 (PKI)（亦稱爲 PKIX）開發應用程式的資訊。包括產品概觀、撰寫各個 PKIX 元件的程式之指示及 PKIX API 的說明。

IBM KeyWorks Toolkit

在隨附於 IBM KeyWorks Toolkit 產品 CD 上提供的所有文件都是線上 PDF 格式。其中的文件如下：

IBM KeyWorks Toolkit Developer's Guide
顯示工具集的概觀。同時亦解釋如何將工具集整合至應用程式中及包含一支範例應用程式。

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
定義應用程式開發者用來存取由組織架構及服務提供者模組提供的安全服務之介面。

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
說明所有工具集服務提供者模組共同的特性。此文件應和個別的「服務提供者介面規格」配合使用，以建置服務提供者模組。

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
定義加密服務提供者模組必須符合的介面，才能透過工具集存取。

IBM Key Recovery Service Provider Interface (KRSPI) Specification
定義金鑰回復服務提供者模組必須相容的介面，才能透過工具集存取。

IBM KeyWorks Toolkit Trust Policy Interface Specification
定義政策制定者（如憑證管理中心、憑證發出者及政策制定應用程式開發者）必須符合的介面，才能以模式或應用程式特定政策延伸工具集。

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
定義憑證檔案庫開發者必須符合的介面，才能提供特定格式的憑證操作服務給各種工具集應用程式及信任政策模組。

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
定義檔案庫開發者必須符合的介面，才能提供特定格式或非特定格式的憑證持續儲存體。

IBM Key Recovery Service Provider

以下文件以 PDF 格式隨附於 IBM Key Recovery Service Provider 產品 CD 上：

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide 提供有關金鑰回復概念的基本瞭解、爲組織設置金鑰回復解決方案的指引及安裝、架構與操作 IBM Key Recovery Server 的程序。

安全紅皮書

下列由 IBM International Technical Support Organization （ITSO）開發的紅皮書，涵蓋與安全相關的產品及處理程序。這些書可在 www.us.ibm.com/redbooks 取得。

- *Understanding the IBM SecureWay FirstSecure Framework*
- *IBM eNetwork Firewall 高可用性*

文件包

IBM SecureWay FirstSecure 提供下列文件包。

FirstSecure 文件包

FirstSecure 文件包包含下列書籍：

- FirstSecure 授權資訊
- *IBM SecureWay FirstSecure 規劃與整合*
- *IBM SecureWay Policy Director Up and Running*
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*
- *IBM SecureWay Trust Authority 更新與執行*
- *Tivoli Cross-Site for Security Installation*

Policy Director 文件包

Policy Director 文件包包含下列書籍：

- Policy Director 授權資訊

- *IBM SecureWay Policy Director Up and Running*

SecureWay Boundary Server 文件包

SecureWay Boundary Server 文件包包含下列書籍：

- SecureWay Boundary Server 授權資訊
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*

第4篇 附錄與後記

附錄. 注意事項

本資訊是針對 IBM 在美國所提供之產與服務開發出來的。 而在其他國家中，IBM 不見得有提供本書中所提的各項產品、服務或功能。 要知道在您所在所在地區是否可用到這些產品與服務時，請向當地的 IBM 服務代表查詢。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。 只要未侵犯 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.

若要查詢有關二位元組（DBCS）資訊的特許權限事宜，請聯絡您國家的 IBM 智慧財產部門，或者用書面方式寄到：

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

下列段落若與該國之法律條款抵觸，即視為不適用： IBM 僅以 『現狀』 提供本書，而不提供任何明示或默示之保證（包括但不限於可售性或符合特定效用的保證） 若有些地區在某些交易上並不允許排除上述保證，則該排除無效。

本書中可能會有技術上或排版印刷上的訛誤。因此，IBM 會定期修訂；並將修訂後的資訊納入新版中。同時，IBM 得隨時改進並（或）變動本資訊中所提及的產品及（或）程式。

資料中提供的非 IBM 網站僅供用戶參考方便，絕不代表爲那些網站背書。那些網站上的內容並非本 IBM 產品內容的一部份，用戶使用該網站時應自行承擔風險。

IBM 可能使用或散佈您提供的任何資料，然因合理得宜，可不須對您負責。

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：

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於雙方之「IBM 客戶合約」、「IBM 國際程式授權合約」（或任何同等合約）條款，提供本資訊中所述的授權程式與其所有適用的授權資料。

這裡提到的任何性能資料均限定在一控制環境下。因此從其它操作環境所取得的結果可能差異很大。我們可能已對發展層次系統採取某些措施，但不保證這些措施與一般現有的系統相同。再者，某些措施可能是推斷而來，與實際結果可能有異。 本文件的用戶應查證所屬環境是否適用這些資料。

關於非 IBM 產品的資料是來自該產品供應商、公開說明或其它公開來源。 IBM 並未測試那些產品，所以無法確認性能準確度、相容性或任何其它與非 IBM 產品有關的索賠。有關非 IBM 產品的性能問題應直接洽詢該產品供應商。

所有關於 IBM 未來的方向或企圖可能未經通知逕行修正或撤回，僅代表目標和方針。

所有列出的 IBM 價格只是 IBM 目前的建議售價，可能未經通知逕行變更。經銷商的價格可能有所差異。

本資訊只供規劃之用。在交付所說明的產品之前，此處所提供之資訊有可能改變。

商標

下列詞彙是 International Business Machines 公司在美國和其他國家的商標：

AIX
AIX/6000
DB2
DB2 Universal Database
eNetwork
Global Sign-On

GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Intel 及 Pentium 是 Intel Corporation 在美國及其它國家的商標或註冊商標。

Java 及所有和 Java 相關的商標與標誌，是 Sun Microsystems, Inc. 在美國和其他國家的商標或註冊商標。

Lotus、Lotus Notes、Domino 及 cc:Mail 是 Lotus Development Corporation 在美國及/或其它國家的商標。

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

Tivoli 是 Tivoli Systems Inc. 在美國及/或其它國家的商標。

UNIX 是 X/Open Company Limited 在美國及其它國家獨家授權的註冊商標。

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

此名詞解釋定義本書使用的術語及縮寫中，可能是新名詞或您可能會感興趣的不常見術語。它包括來自下列書籍的術語及定義：

- IBM Dictionary of Computing，New York：McGraw-Hill，1994。
- The American National Standard Dictionary for Information Systems， ANSI X3.172-1990，American National Standards Institute (ANSI)，1990。
- The Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1996.

.

四劃

不可否認性（non-repudiation）. 使用數位私密金鑰來避免文件的簽名者錯誤地拒絕簽名它。

內容過濾（Content filtering）. 解開傳輸物件讀取其內容，以判斷該傳輸是否符合特定的內容標準。

公開金鑰（public key）. 在公開/私密金鑰對中，可讓其他人使用的金鑰。此金鑰可將交易導向至金鑰的擁有者或驗證數位簽章。以公開金鑰加密的資料只能以對應的私密金鑰解密。*亦請參閱*公開/私密金鑰對。

公開/私密金鑰對（public/private key pair）. 公開/私密配對金鑰是金鑰配對加密法概念（由 Diffie 及 Hellman 在 1976 年所提，用來解決金鑰管理問題）的一部份。在它們的概念中，每一個人會取得一對金鑰，其中一個稱爲公開金鑰，而另一個稱爲私密金鑰。當私密金鑰保密時，則每一個人的公開金鑰都是公開的。傳送者及接收者不需要共用機密資訊：所有通信只牽涉到公開金鑰，而私密金鑰永遠不會傳輸或共用。 相較於竊聽或洩密，它不再需要相信某些通信頻道是安全的。唯一的基本要求是公開金鑰必須以可靠的（經過鑑定）方法（例如，放在可靠的目錄中），建立和其使用者的關聯。任何一個人都可使用公用資訊，來傳送機密的訊息。不過，訊息只能使用只有接受者擁有的私密金鑰解密。因此，金鑰配對加密法不僅可用在資料隱私（加密）上，也可用在身份驗證（數位簽章）上。

分散式計算環境（Distributed Computing Environment，DCE）. 一些服務及工具，支援在異質計算環境中建立、使用及維護分散式應用程式。

心跳（heartbeat）. 從某個程式至管理程式的一種通信，其目的是要確認活動；該程式旨在通知管理程式它仍在作用中，正在執行其作業。

五劃

主體（principal）. 在 DCE 中，可透過 DCE 安全機制與其它實體進行安全通信的實體。主體可以是使用者、伺服器或電腦。

代理程式（agent）. 在 Tivoli Cross-Site for Security 中的一個智慧型 IP 封包監視程式，可在不同的網路層次檢查封包是否有不正常情況，並且追蹤已建立連線的狀態與統計值。

加密（encrypt）. 將資訊亂數化，使得只有知道適當解密字碼者可以透過解密程序取得原始資訊。

巨集炸彈（macro bomb）. 一組儲存的指令順序，傳送給其他使用者造成不良結果。

六劃

企業內網路（intranet）. 企業內部的網路，通常位於防火牆內。它是網際網路的衍生網路，使用和網際網路相似的技術。就技術上而言，企業內網路只

是網際網路的延伸。HTML（用來以圖形方式顯示資訊的電腦語言）及 HTTP（在網際網路上移動超本文檔案的通信協定）是其中的部份共同點。

企業外網路（extranet）。 它是網際網路的衍生網路，使用類似的技術。許多公司都開始應用 Web 發佈、電子商務、訊息傳輸及群組軟體方式，擴大對客戶、協力廠商及內部員工的互動範圍。

存取控制列示（access control list）。 一種用來限制特定資源只能給獲授權的使用者使用的機制。

存取控制（Access control）。 在電腦安全系統中，確定電腦系統上的資源只能由獲授權的使用者以授權的方式存取的處理程序。

安全 Socket 層次（Secure Sockets Layer、SSL）。 (1) 一種 IETF 標準通信的通信協定，具有內建的安全性服務，並且儘可能對一般使用者透明化。它提供數位化的安全通信通道。 (2) 啓用 SSL 的伺服器通常從和標準 HTTP 要求不同的連接埠接受 SSL 連線要求。 SSL 建立的階段作業中，只需要進行一次交握動作。在交握完成之後，通信即被加密。訊息完整性檢查會一直繼續到 SSL 階段作業過期爲止。

七劃

伺服器（server）。 (1) 在網路中提供機能給其他工作站（例如，檔案伺服器）的資料工作站。 (2) 在 TCP/IP 中，指網路中負責處理另一個站台的系統要求的系統，稱爲主從架構。

身份驗證（authentication）。 用以決定通信方之身份的可靠程序。

防火牆（firewall）。 一套系統或系統組合，可在不同網路之間實施界限分隔。

八劃

事件（incident）。 在 Tivoli Cross-Site for Security 中，可能是要侵襲系統的一種可疑活動。

物件申請分配管理系統（object request broker）。 在物件導向程式設計中，作爲中介身份的隱藏式軟體，使物件可以交換要求與回應。

九劃

保險庫（vault）。 保險庫使用加密方式保護資訊不致洩露給未獲授權者，如系統管理者及其它保險庫的擁有者。它同時也使用數位簽章方式預防受竄改，及以數位憑證保護和不明對象通信時的安全性。此外也使用加密、簽章及憑證安全地傳輸資訊至其它保險庫。

宣告名稱儲存區（namespace）。 和目錄相關，可讓使用者存取的外部名稱結構。

十一劃

常駐程式（daemon）。 在 AIX 中一種持續存在，等候伺服要求的程式。

從屬站（Client）。 (1) 一種功能單元，可從伺服器取得共用的服務。 (2) 對其它電腦或程式要求服務的電腦或程式。

授權（Authorization）。 決定使用者可執行哪些活動類型的處理程序。授權處理通常會在身份驗證之後發生。

通用資源指位器（Universal Resource Locator）。 全球資訊網通信中使用的命名慣例，其中的 Web 物件路徑會以服務名稱開頭，接下來是組織名稱、路徑及檔名，例如，http://www.ibm.com/software/security/firstsecure。

通道（Channel）。 信號可延之傳送的路徑。

十二劃

虛擬專用網路（virtual private network）。 一種採用網際網路而非電話線來建立遠端連線的專用資料網路。由於使用者是透過「網際網路服務提供者」（ISP）來存取企業網路資源，而不是透過電話公司，因此組織可以大幅地減少遠端存取的成本。

VPN 也能加強資料交換的安全性。 在傳統的防火牆技術中，訊息內容可以加密，但是來源及目的地位址則不能。在 VPN 技術中，使用者可以建立通道連線，其中的整個資訊封包（內容及標頭）都是加密與封裝的。

十三劃

傳輸控制通信協定/網際網路通信協定（Transmission Control Protocol/Internet Protocol）. 一組支援區域及廣域網路之對等式連結性功能的通信協定。

閘道（gateway）. 一套系統，可讓不相容的網路或應用程式彼此通信。

電子商務（e-commerce）. 處理商業交易。包括在網際網路上購買及銷售物品與服務（對象爲客戶、供應商、廠商等）。它是電子商業的主要元素。

電子商業 (e-business). 透過網路及電腦進行商業交易。包括購買和銷售貨品與服務，也包括經由數位通信的轉帳。

電腦駭客（hacker）. 嘗試存取本身未取得適當授權的機器或系統的電腦使用者。電腦駭客通常在沒有許可權的情況下試圖使用電腦資源。

電路層閘道（Circuit-level gateway）. 在防火牆系統中，將從屬站要求透過防火牆重新導向至需要的伺服器之 proxy 伺服器。

十四劃

實作服務（Implementation Services）. 由 IBM 提供的現場安裝支援。

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

網址過濾（network address filtering）. 檢查進入或送出電子郵件的位址，驗證接受者或傳送者是否可能接收的處理程序。

網際網路（Internet）. 世界性的網路集成，提供電腦之間的電子連線。它可讓電腦經由軟體裝置（如電子郵件或 Web 瀏覽器）彼此通信。例如，某些大學院校具有網路系統，這些網路系統鏈結其他類似的網路，即形成網際網路。

輕裝備目錄存取通訊協定（Lightweight Directory Access Protocol）. 在 IBM SecureWay Directory 中，LDAP 提供方法，可在一個集中位置維護目錄資訊，執行儲存、更新、擷取及交換作業。

遠端程序呼叫（remote procedure call）. (1) 從屬站用來向伺服器要求執行一項程序呼叫的機能。此機能包括一個檔案庫程序及及一個外部資料表示。 (2) 從屬站要求傳送至位在其它節點的服務提供者。

十五劃

審核追蹤（audit trail）. 一種邏輯路徑形式的資料，鏈結一系列的事件順序。審核追蹤可用來追蹤交易或給定活動的歷程。例如，它可追蹤客戶帳戶中的活動。

數位式憑證（Digital certificate）. 由具公信力的第三者簽發給個人或實體的電子式證明。憑證包含它所證明的實體資訊。

十六劃

憑證管理中心（certificate authority）. 一個實體、軟體應用程式或人員，負責遵循組織的安全政策並分派憑證格式的安全電子身份識別。憑證管理中心負責處理有關簽發、重訂與廢止憑證要求。

整合式開發環境（integrated development environment）. 供應用程式開發使用的程式，可讓您用來撰寫應用程式碼、以不同岔斷點執行並且取得程式錯誤診斷協助。

機動程式碼（mobile code）. 有關在攜帶型電腦上執行的計算，其使用者爲經常在多個位置之間移動並且使用不同類型的網路連接（例如，撥號式、LAN 或無線電）。

十七劃

應用程式介面（application program interface）. 一種功能介面，可讓以高階語言寫成的應用程式使用特定的功能。

檔案轉送通信協定（File Transfer Protocol，FTP）. 網際網路中的一種主從架構通信協定，可用來在電腦之間轉送檔案。

A

ACL. 存取控制列示。

ActiveX. 在 Microsoft 程式設計中，一組物件導向的技術及術語。

Apache 伺服器（Apache server）. 一組可供自由取用的 Web 伺服器軟體。

API. 應用程式設計介面。

Applet. 以 Java 撰寫的電腦程式，在和 Java 相容的瀏覽器上執行，如 Netscape Navigator。亦稱爲 Java Applet。

B

Bloodhound. 在 Norton AntiVirus 中，追蹤病毒的元件。

C

cell. 在 DCE 中的使用者、系統及資源群組，通常具有共同的目的，並且共用安全、管理及命名界限。 Cell 中包含共用一個共同目的的使用者、機器及資源，它們對彼此的信任層次高於對 Cell 以外的其它使用者、機器及資源。

Cell 目錄服務（Cell directory service，CDS）. 分散式計算環境 （DCE） 的一個元件，負責管理在 DCE cell 中有關資源的資訊資料庫。

D

DCE. 分散式計算環境 （DCE）。

I

IDE. 整合式開發環境。

IPSec. 由 IETF 發展的一套「網際網路通信協定安全」標準。 IPSec 是網路層通信協定，其設計目標是要提供密碼化的安全服務，可彈性地支援身份驗證、完整性、存取控制及是等組合。由於其極強的鑑別特性，此產品已被許多 VPN 產品的供應商採用作爲建立網際網路上安全的點對點連線的通信協定。

ISV. 獨立軟體供應商。

J

Java. 由 Sun Microsystems 公司所發展的一組可感應網路，未針對特定平台的電腦技術。Java 環境是由 Java OS、不同平台的「虛擬機器」、物件導向的 Java 程式設計語言，及數個類別程式庫所組成。

JavaScript. 一種類似 Java 的 script 語言，由 Netscape 發展，在 Netscape 瀏覽器中使用。

K

Kerberos. 一種鑑定要求電腦的服務之安全方法。Kerberos 是由麻省理工學院的 Athena Project 發展出來的。在希臘神話中，Kerberos 是守護冥府的一條三頭狗。 Kerberos 系統可讓使用者向鑑別處理程序要求加密的通行證，此通行證接著可用來向伺服器要求特定的服務。使用者的密碼並不需要透過網路傳遞。

L

LDAP. 全文爲 「Lightweight Directory Access Protocol」，意指「輕裝備目錄存取通訊協定」。

M

MPEG. 由「移動圖像專用群組」開發的標準，用來壓縮及儲存數位形式的影像動畫與動畫。

O

OEM. 委托製造代工。

P

plug-in. 可作爲 Web 瀏覽器的一部份使用的程式。

Proxy 伺服器（proxy server）. 介於要求存取的電腦（A）與被存取的電腦 （B） 之間的中繼站。因此，如果一般使用者向電腦 A 要求資源，則這個要求會導向到 Proxy 伺服器。 Proxy 伺服器會提出該要求，並從電腦 B 取得回應後，再將回應轉遞給一般使用者。 Proxy 伺服器有助於從防火牆內存取全球資訊網。

R

RPC. 在 DCE 中，指遠端程序呼叫。

S

SecurID 記號（SecurID token）. 來自 Security Dynamics 的 ACE/Server 鑑別方法，包括一個使用者 ID 及一個 SecurID 記號。當您在遠端登入時，會從 SecurID 記號取得您的密碼。密碼每 60 秒會變更一次並且只能使用一次。因此即使有人在開放式網路上截取您的密碼，該密碼也不能作爲額外使用。

sock 伺服器（socks server）. 一個電路層閘道，在非安全網路中，提供安全的單向連線，透過防火牆至伺服器應用程式。

SOCKS 通信協定（SOCKS protocol）. 可讓位在安全網路中的應用程式透過防火牆經由 sock 伺服器進行通信的通信協定。

spam. 非經請求電子的郵件，通常會傳送給多位接收者。

T

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」。

telnet. 在網際網路通信協定組中，提供遠端終端機連線服務的通信協定。此通信協定讓某主電腦上的使用者可登入遠端主電腦，並且其互動方式如同是該主電腦的直接連接終端機使用者。

U

URL. 通用資源指位器。

V

VPN. 全文爲「Virtual Private Network」，意指「虛擬專用網路」。

W

Web 伺服器（Web server）. 一種伺服器程式，負責回應瀏覽器程式提出的資訊資源要求。

Web 物件（Web object）. 可透過 Web 瀏覽器使用的資料。Web 物件可以是網頁、網頁的一部份、檔案、影像、目錄、CGI 程式或 Java applet。

Web 應用程式（Web application）. 設計目標爲透過全球資訊網存取的應用程式。

Web 瀏覽器（Web browser）. 在桌上型 PC 上執行的從屬站軟體，可讓使用者瀏覽「全球資訊網」或本端頁面。它是一個擷取工具，可提供對 Web 及 Internet 上可用的大量超媒體資料集合進行廣泛的存取。範例如 Netscape Navigator 及 Microsoft Internet Explorer。*亦請參閱*伺服器。

worm. 一種有害處的電腦病毒。

X

X.509. 一種被廣泛接受的憑證標準，其設計目標旨在支援安全管理，及跨越安全網際網路分送經數位方式簽章的 PKI 憑證。 X.509 憑證定義資料結構，其中納入用來分送由具公信力的第三者，以數位式簽名的公開金鑰程序。

特殊字元

IntraVerse 伺服器（ItraVerse server）. 在 IntraVerse 中，位在網路上的一套系統，其中包含 IntraVerse 伺服器軟體並且可和在 NetSEAT 從屬站軟體上執行的所有主電腦系統通信。 IntraVerse 伺服器是指執行產品相關程式的一套系統或系統組合。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔十三劃〕

〔十四劃〕

A

D

F

H

I

M

N

P

S

T

V

W

IBM SecureWay FirstScure
規劃與整合
版本 2

SC40-0503-00

讀者意見表

折疊線

台北市敦化南路一段二號十二樓

中華民國國際商業機器股份有限公司 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: CT7EHTC

Printed in Singapore

CT7EHTC

SC40-0503-00