虛擬私有網路之應用

文、圖／邱文志

摘　要

現在企業組織活動已不再侷限於某一國家或某一地點，故透過網際網路來傳輸企業位於不同據點的資訊，變得勢在必行。但是利用網際網路來傳輸企業內部的重要資訊，其保密性、安全性及資料完整性備受考驗，因而發展出在網際網路上建構虛擬私有網路(VPN)的技術。

虛擬私有網路應用通道技術、密碼技術、身分認證及密鑰管理等技術，在公眾網路中建立起私有網路通道，除能大幅降低企業網路建設費用外，提供企業員工，能以安全的模式，從遠端連結到企業內部存取資料，或分公司和總部間、企業與企業間建立虛擬私有網路通道，爲企業資料傳送、網路連線提供省錢、方便、安全的方法，創造更大的效益。

現在企業組織活動已不再侷限於某一國家或某一地點，從事商業活動，往往是全球化，跨國界的在世界各地設立子公司、分公司與辦事處，其彼此間或和總公司間，往往需有資訊交換與資料分享，若是以建置專線的方式來傳遞訊息，將耗費龐大的網路基礎建置費用，而且企業跨國界的租用專線亦是困難重重，且不符經濟效益。

自從網際網路興起，挾其只需向當地網路服務公司(Internet Service Provider, ISP)註冊，即可將資料傳送到世界各地任何地方、任何企業，不需自行架設專屬網路，因其方便、省錢、省時，故透過網際網路來傳輸企業的資訊，變得勢在必行，網際網路的加值應用也到處可得。

但是網際網路畢竟是一公眾網路，任何人均可透過ISP來取得服務，利用其來傳輸企業內部的重要資訊，很容易被不相關的第三者竊取，其保密性、安全性及資料完整性備受考驗，因而發展出在網際網路上建構虛擬私有網路(Virtual Private Network, VPN)的技術。

何謂虛擬私有網路

對於「虛擬私有網路」(VPN)的定義，有許多種的說法，以下列舉二種定義：

Charlie Scott認爲，所謂的VPN，就是在公眾網路上模擬一個私有網路。之所以稱爲虛擬是因爲它必須使用虛擬的連線，這是一種暫時性的連線，通訊兩端之間沒有固定的實體連線，這連線本身其實是一堆透過Internet來回轉送的封包。這種安全的虛擬連線可以建立在兩台機器之間，或一台機器對一個網路或是兩個網路之間。

Ruixi Yuan認爲一個VPN的觀念應包括兩個部份：其一爲一個虛擬網路是附加在隨處存在的網際網路上，其次是爲一個私有的網路，提供私密的通訊網路且爲使用者專用。

綜合上述的定義及參考相關的說法，所謂VPN，是在公眾網路，建立一私有網路，且在公眾網路中須具有資料保密、身分認證及保持傳送封包之

完整性的功能。

虛擬私有網路的沿革

為了解決資料在Internet傳輸的安全性，而發展的VPN其發展史可概分為下列三個階段：

1.萌芽期：1998

提供應用的VPN產品，以虛擬私有撥接網路(Virtual Private Dial-up Network, VPDN)為主，主要用於員工出差時可以透過撥接網路和企業總部建立連線，節省通信費用，本署安檢所（站）即利用現有的VPN線路撥接至署本部資訊機房連線，使用安檢資訊系統。

2.成長期：1999-2000

VPN的應用已擴展到企業分支機構和總部的連線(Branch Office VPNs)，除節省成本外，更具彈性、易用性、安全性的功能被重視，如本署的各地區巡防局，在海巡網路建置VPN連線，增加其安全性。

3.成熟期：2001迄今

VPN的應用已擴展到企業和企業間的連線(Extranet VPNs)，服務品質(Quality of Service, QoS)、服務層級保證機制(Service Level Agreements,SLAs)、標準目錄(Standard Base Directory)及安全基礎建設(Security Infrastructures)受到重視，如本署可針對安檢情傳系統、PKI/CA系統身分鑑別定義較高的服務等級、對於連線網際網路定義較低的服務等級。

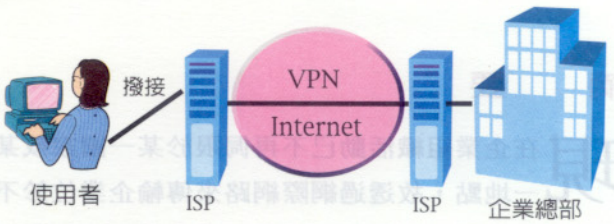
虛擬私有網路的應用

企業應用虛擬私有網路，常因需求資料分享者的型態不同而有不同的建置模式，常見有下列三種模式：

1. 虛擬私有撥接網路(VPDN)通道的建立

VPDN通道的建立，通常需和點對點通信協定(Point-to-Point Protocol, PPP)搭配，遠端使用者利用PPP撥接至ISP的遠端存取伺器(Remote Access Server, RAS)和ISP建立連線，再透過Internet或ISP骨幹網路，和伺服器端建立起通道(如圖1)，通常此通道僅個人使用，使用者需於電腦安裝VPN使用者端(Client)軟體。

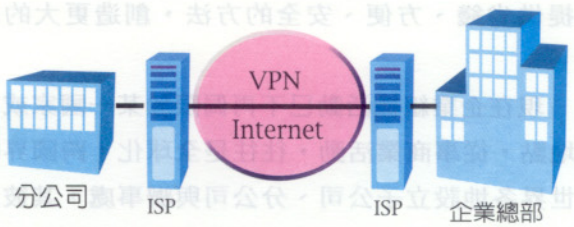
圖1 個人使用VPDN連線模式



2. 站對站(Site To Site)通道的建立

通常是分支機構以專線和當地ISP連線，再透過Internet或ISP骨幹網路，和企業總部伺服器端建立起通道，一般兩端均設有虛擬私有網路閘道器(VPN Gateway)，由兩個VPN Gateway建立起連線通道，可提供分支機構內多人同時使用此一通道（如圖2)。

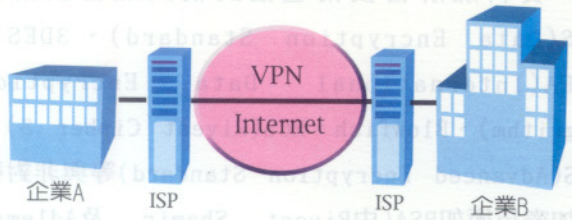
圖2 分公司與總部VPN連線模式



3. 跨企業網路(Extranet)通道建立

其建置方式和站對站通道的建立相似，由兩端的VPN Gateway建立起連線通道（如圖3）；不同的是，企業各自管理自己的Intranet網路，不像站對站的方式分支機構和總部同屬於一企業內部網路，分支機構的網路位址通常受到總部的管理。

圖3 企業間VPN連線模式



所以企業使用虛擬私有網路，應具有下列原因：

1.基於網路建置的考量

企業要和分散在各地的據點、業務往來的上下游企業及客戶，以專線建立完整的網路是困難重重的。

2.基於成本效益的考量

就算可以完成以專線建立的網路連線，其所花費的龐大金錢亦不符合成本效益。

3.基於安全機制的考量

將資料透過Internet傳送其安全性的問題，往往受到質疑，必需經由安全機制較完善的VPN來加強。

虛擬私有網路使用的技術

圖4 VPN採用技術

VPN採用通道技術、密碼技術、身分認證及密鑰管理等技術，在原有網路建立虛擬通道，並保護傳輸資料的安全性，且必須符合下列條件：

1. 機密性(Confidentiality)：防止非法使用者閱讀或拷貝資料內容。

2. 完整性(Integrity)：確定傳輸的過程資料沒有被竄改過。

3. 身分認證(Authentication)：確定使用者的身分。

4. 存取控制(Access Control)：限制使用者對資料的存取行爲。

爲達成上述條件，必須在資料傳輸的雙方加入許多額外的程序，例如建立私有通道、資料的加密、雜湊演算法的驗證、電子簽章等程序，以保障資料的完整性與私密性。以下說明虛擬私有網路的安全作法：

通道的安全作法

VPN在通道協定的安全服務主要如下：

1.PPTP(Point-to-Point Tunnel Protocol)

採用一般性路徑選擇封裝（Generic Routing Encapsulation, GRE）來封裝資料在網路上傳輸，用點對點協定(PPP)的驗證機制如密碼驗證協定(Password Authentication Protocol, PAP)及查問式握手驗證協定）(Challeng Handshake Authentication Protocol, CHAP）作身分驗證。

2.L2TP(Layer Two Tunneling Protocol)

仍用PPP的驗證機制如PAP及CHAP作身分驗證，和PPTP不同的是他可以支援IPsec的使用。

3.IPsec(Internet Protocol Security)

IETF(Internet Engineering Task Force)組織針對IP制訂了一系列的協定，稱爲IPsec，IPsec架構下主要：

(1)安全協定(Security protocol)

增加了兩個Header給IP封包作爲認證及加密之用，其中一個稱爲AH(Authentication Header)，是將資料經由單向雜湊函數作認證，常用的演算法有訊息摘要(Message Digital 5, MD5)雜湊訊息驗證代碼(Hash Message Authentication Codes,

HMAC)及私密雜湊演算法(Secure Hash Algorithm 1, SHA-1)。另一個稱爲ESP(Encapsulating Security Payload)，可用來作資料的加密或認證，AH和ESP是分開獨立的個體，可以利用目前已知的演算法來作，並不限制其種類。

(2)安全關係(Security Associations, SA)

IPsec爲使兩個設備在交換受保護的資料時，它們要使用何種加密方法要先達成共識，這種對等設備間的協議稱爲安全關係(SA)，當雙方開始要建立連線通訊時，彼此必須協商出一組共通遵守的參數，收送雙方都要遵守此一組參數的規範，例如指定所用的加密演算法，共享會話密鑰(Session Key)或是確認何時必須重新交換key等，這些協議出來的參數就會被存在SA中。

(3)管理資料庫

爲了使資料傳輸時更爲方便，所以需要一些機制來管理SA，用來管理是否允許建立連線(包含Inbound and Outbound traffic)的資料庫稱爲安全政策資料庫(Security Policy Database, SPD)。用來管理連線後SA的行爲的資料庫，稱爲安全協議資料庫(Security Association Database, SAD)。

(4)密鑰管理

所有的金鑰都必須進行交換，以使雙方能安全的通信，常用於處理IPsec中的金鑰管理有二類，一爲人工作業，另一爲網路安全關係密鑰管理協定(Internet Security Association and Key Management Protocol, ISAKMP)，ISAKMP協定制訂了一套程序與封包格式來處理連線前確認建立連線對方的身分是否屬實、建立並管理連線時所需要用到的key值、管理並選擇產生key值的演算法。

其他安全作法

在通道技術中除IPsec有完整的安全服務定義外，其他的通道協定並無完善的安全機制，以下列出VPN可運用的安全機制：

1.密碼技術(Cryptography)

資料加解密技術包括對稱式加密技術如DES(Data Encryption Standard)、3DES、IDEA(International Data Encryption Algrithm)、Blowfish、RC5(Rivest Cipher 5)、AES(Advanced Encryption Standard)等與非對稱式加密技術如RSA(由Rivest, Shamir, 及Adleman所提出)。

2.身分認證技術(Authentication)

(1)雙方認證：PPP(如PAP、CHAP)、RADIUS(Remote Access Dial In User Service)、S/KEY。

(2)三方認證：公開金鑰基礎建設(Public Key Infrastructure, PKI)、Kerberos。

(3)設備認證：Gateway-to-Gateway、Client-to-Gateway。

3.密鑰管理(Key management)

認證中心(Certification Authority, CA)、分享密鑰(Shared Secret Key)、ISAKMP、IKE(Internet Key Exchange)。

4.存取控制(Access Control)

入口存取控制政策(Inbound access control policy)、出口存取控制政策(Outbound access control policy)、群取存取控制政策(Group-base access control policy)、屬性存取控制策政(Attributes access control policy)。

設備的安全功能

根據VPNC(Virtual Private Network Consortium)網站，在2002年4月公布的廠商VPN設備安全機制功能表(如表1)，其中IPsec、3DES的技術各家廠商均有提供，而IKE、IKE X.509大多數廠商有提供，然而已被廣泛使用的憑證管理(CA)技術，所提供的廠商並不多見。

表1VPN設備功能表

	IPsec	L2TP/IPsec	PPTP/RC4	IKE	IKE X.509	3DES	CA
Alcatel	◎			◎	◎	◎	
Asita	◎			◎	◎	◎	
Avaya	◎			◎	◎	◎	
Check Point	◎			◎	◎	◎	◎
Cisco	◎	◎		◎	◎	◎	
CoSine	◎	◎	◎	◎	◎	◎	
Cryptek	◎					◎	
CyberGuard	◎			◎	◎	◎	
Cylink	◎			◎	◎	◎	
DigiSAFE	◎			◎	◎	◎	
Enterasys	◎	◎		◎		◎	
F-Secure	◎			◎	◎	◎	
Hi/fn	◎			◎	◎	◎	
Intel	◎			◎	◎	◎	◎
Intoto	◎	◎	◎	◎	◎	◎	
Microsoft	◎	◎	◎		◎	◎	◎
NetScreen	◎	◎		◎	◎	◎	
Nokia	◎	◎	◎		◎	◎	◎
Nortel	◎	◎	◎	◎	◎	◎	
Philips	◎			◎	◎	◎	
Quarry	◎	◎		◎	◎	◎	
RedCreek	◎				◎	◎	
SafeNet	◎	◎		◎	◎	◎	
SecGo	◎			◎	◎	◎	◎
SSH	◎	◎		◎	◎	◎	◎
Stonesoft	◎			◎	◎	◎	◎
V-ONE	◎					◎	
Wind River	◎	◎				◎	
Wipro	◎	◎		◎		◎	
Zeus	◎			◎	◎	◎	

本署使用虛擬私有網路情形

一般VPN的建置可分爲專線型VPN及租用型VPN，專線型由企業自行構建VPN，海巡網路就是屬這類型；租用型則由網路服務公司構建VPN。專線型VPN既然是自行租用專線，費用是固定，又是專屬的網路，外人無法入侵，那爲什麼還要使用VPN？其重點並不在於省錢及防外賊而是用來保證使用頻寬及防內賊，如企業有需即時傳送及敏感性資料即可用VPN來定義他的優先權及對資料加密傳送。

但不管使用那一種類型，要一個連線單位或個人，來維護VPN的通道或VPN Gateway的相關設定，均需要網路專業人員，造成很大的困擾，以海巡網路爲例（如圖5）。

若是任兩節點間均要構成VPN連線(Fully Mesh)，其共有37個節點，必須要建立個的虛擬通道數666個(T=n*(n-1)/2=37*36/2=666)，若是任兩部電腦間均要構成VPN連線(Fully Mesh)，將超過2000個節點，要建立個的虛擬通道數將達到二百萬個(T=n*(n-1)/2=2000*1999/2=1,999,000)。要管理這麼龐大的通道數，不但困難且容易出錯，而且電腦在作路徑選擇要花費相當多的時間，造成連線速度減緩，其次VPN連線本身又需對資料加（解）密，身分認證，又要花費時間，故整體效益會大打折扣。

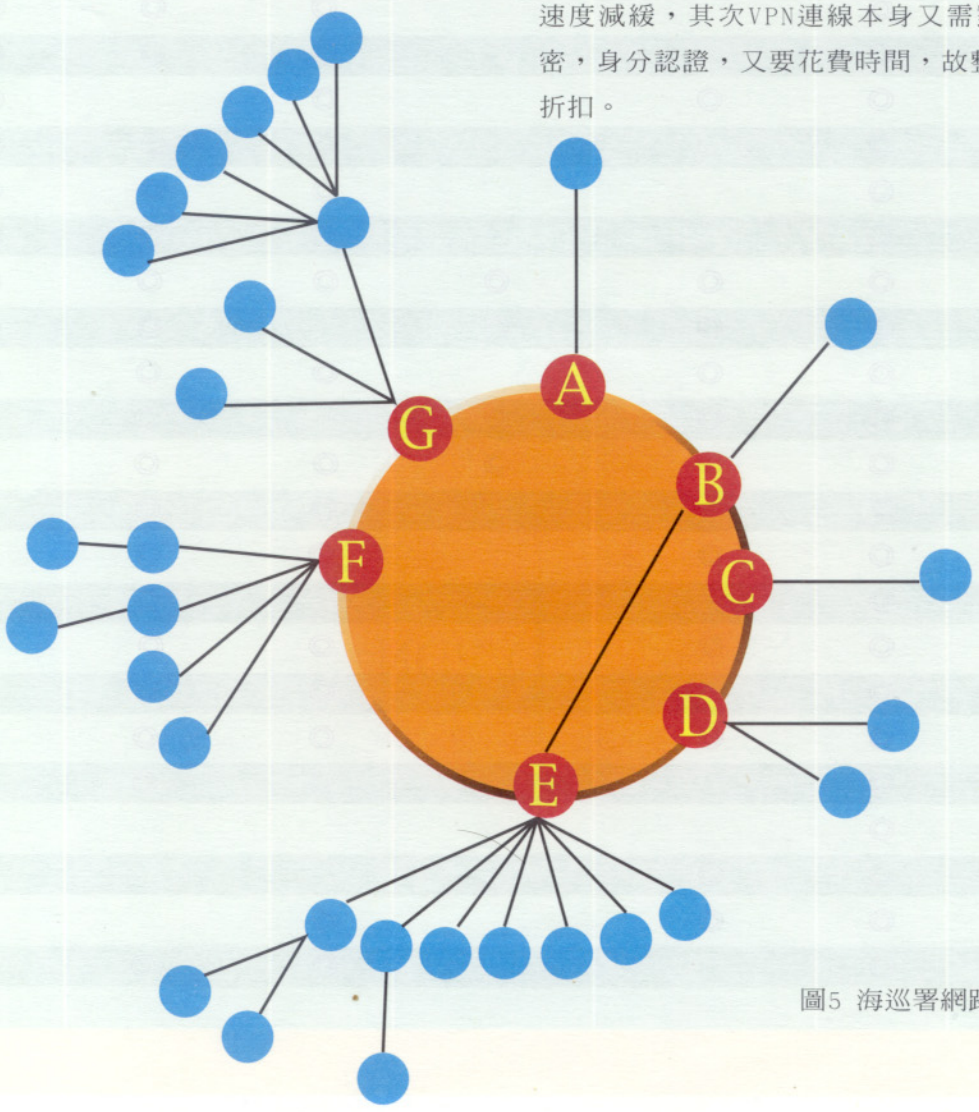


圖5 海巡署網路架構圖

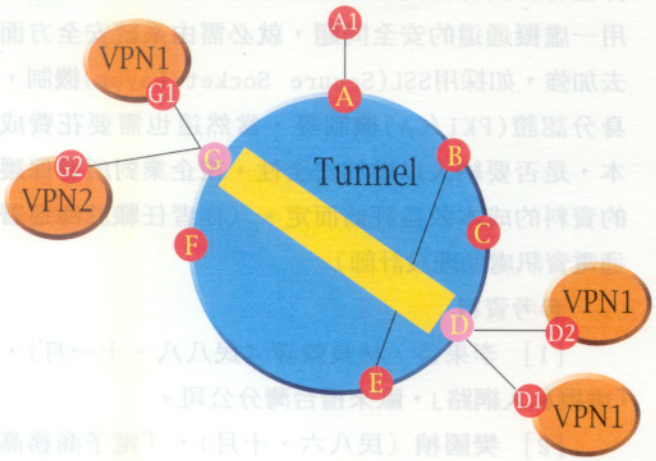


圖6 骨幹VPN示意圖

所以VPN連線的使用很少由端點使用者至端點使用者設定連線，大都採用於重要節點設立VPN連線，如海巡網路在骨幹設立VPN連線（如圖6），只有7個節點（A-G），只需建立21個(T=n*(n-1)/2=7*6/2=21)虛擬通道數，這和原有的上千個上百萬個虛擬通道數差距甚大。

實例說明

本實例是以使用本署海巡資訊應用系統爲例（如圖7），說明下屬單位地區巡防局及安檢所應用不同的網路連線的安全作法，及其採用PKI/CA安全

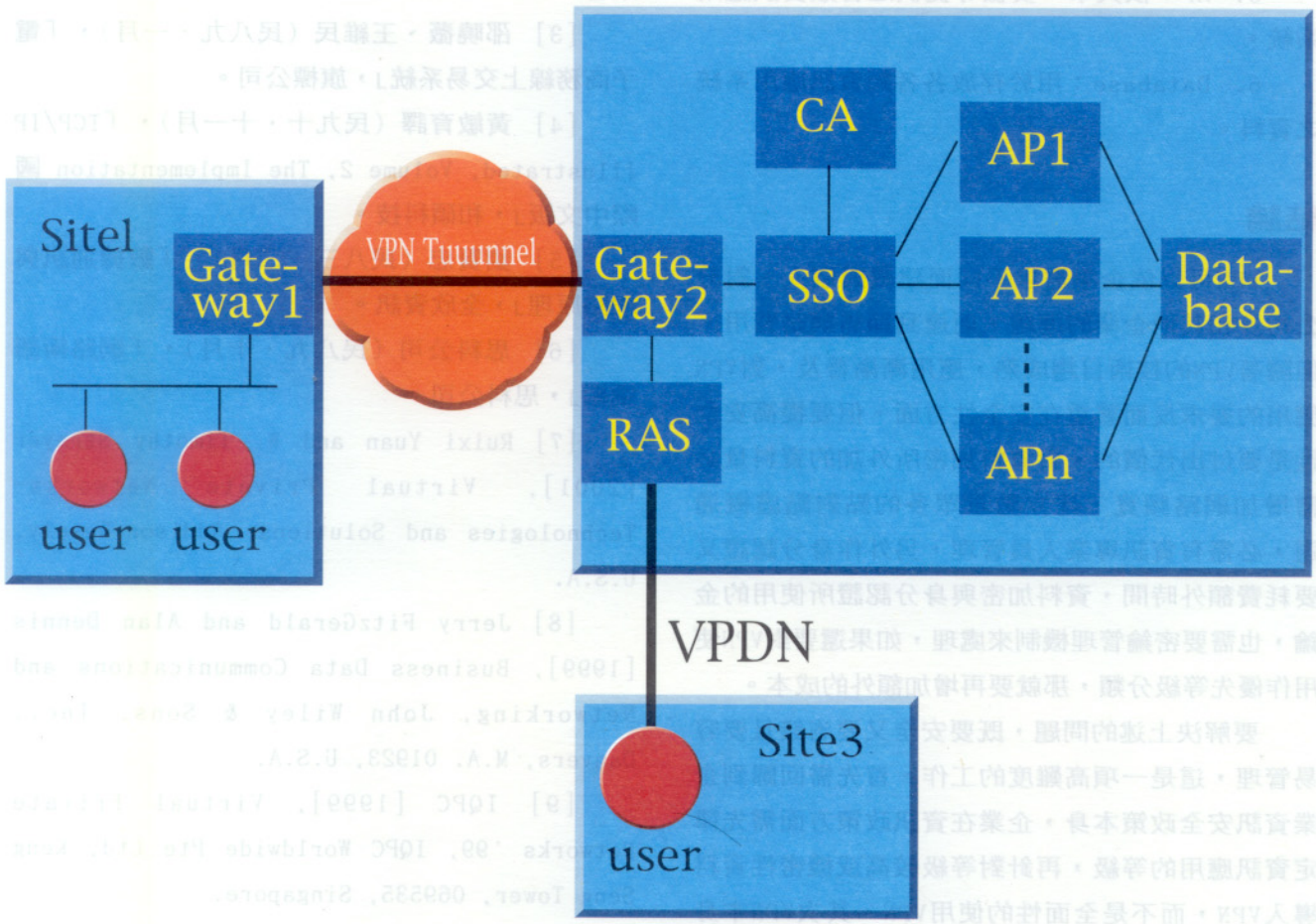


圖7 海巡資訊系統網路連線圖

機制的身分認證方法。

說明：

1. Gateway1和Gateway2：爲VPN Gateway，用於連接地區巡防局(Site1)，和署部(Site2)間的網路，提供虛擬私有通道服務。

2. VPDN：利用RAS提供安檢所(Site3)撥接連線至署部(Site2)的虛擬私有撥接網路服務。

3. CA：憑證管理中心(CA)，用於核發個人、伺服器的電子憑證，公布憑證。

4. SSO：單一簽入(Single Sign On)伺服器，提供使用者身分認證，依使用者權限之不同，而進入不同的應用系統。

5. AP：依人事、安檢等提供之各類資訊應用系統。

6. Database：用於存放各各類資訊應用系統之資料。

結論

VPN可以依企業需求不同而建置對個人、對分公司及和其他企業的連線，而達到節省網路費用。但隨著VPN的技術日趨成熟，應用漸漸普及，對VPN應用的要求反而著重在安全性方面，但要提高安全性是要付出代價的，對資料加密所外加的資料量必需增加網路頻寬，建立數量眾多的點對點虛擬通道，必需有資訊專業人員管理，另外作身分認證又要耗費額外時間，資料加密與身分認證所使用的金鑰，也需要密鑰管理機制來處理，如果還要對VPN使用作優先等級分類，那就要再增加額外的成本。

要解決上述的問題，既要安全又要省錢且要容易管理，這是一項高難度的工作，首先需回歸到企業資訊安全政策本身，企業在資訊政策方面需先律定資訊應用的等級，再針對等級較高或機密性資料導入VPN，而不是全面性的使用VPN。其次VPN本身屬網路安全方面的應用，若爲了減少管理成本，選擇在骨幹與骨幹間建立虛擬通道，所衍生的多人共用一虛擬通道的安全問題，就必需由系統安全方面去加強，如採用SSL(Secure Socket Layer)機制，身分認證(PKI/CA)機制等，當然這也需要花費成本，是否要納入以增加安全性，視企業對所要保護的資料的成本效益評估而定。（作者任職於海巡署通電資訊處助理設計師）

參考資料

[1] 李果益、林長毅譯（民八八・十一月），「虛擬私人網路」，歐來禮台灣分公司。

[2] 樊國楨（民八六・十月），「電子商務高階安全防護－公開金鑰密碼資訊系統安全原理」，資策會。

[3] 邵曉薇、王維民（民八九・一月），「電子商務線上交易系統」，旗標公司。

[4] 黃敏育譯（民九十・十一月），「TCP/IP Illustrated, Volume 2, The Implementation 國際中文版」，和碩科技。

[5] 劉賢忠（民八三・二月），「數據通訊與網路原理」，全欣資訊。

[6] 思科公司（民八九・十月），「網路術語彙編」，思科公司。

[7] Ruixi Yuan and W. Timothy Strayer [2001], Virtual Private Networks-Technologies and Solutions, Addison-Wesely, U.S.A.

[8] Jerry FitzGerald and Alan Dennis [1999], Business Data Communications and Networking, John Wiley & Sons, Inc., Danvers, M.A. 01923, U.S.A.

[9] IQPC [1999], Virtual Private Networks '99, IQPC Worldwide Pte Ltd, Keng Seng Tower, 069535, Singapore.

[10] W. Simpson, "The Point-to-Point

Protocol"(PPP), RFC1661, July 1994.

[11] A. Valencia, et al., "Cisco Layer Two Forwarding Protocol" (L2F), RFC2341, May 1998.

[12] K. Hamzeh, et al., "Point-to-Point Tunneling Protocol", (PPTP), RFC2637, July 1999.

[13] S. Hanks, T. Li, D. Farinacci, and P. Traina, "Generic Routing Encapsulation", (GRE), RFC1701, October 1994.

[14] W. Townsley, et al., "Layer Two Tunneling Protocol"(L2TP), RFC2661, August 1999.

[15] S. Kent, et al., "Security Architecture for the Internet Protocol", RFC2401, November 1998.

[16] S. Kent, and R. Atkinson, "IP Authentication Header", RFC2402, November 1998.

[17] S. Kent, and R. Atkinson, "IP Encapsulation Security Payload(ESP)", RFC2406, November 1998.

[18] http://www.cisco.com/

[19]http://vpnc.org/features-chart.html.