行政院國家科學委員會專題研究計畫成果報告
利用虛擬私有網路進行電子商務—技術面、管理面、與應用面上之研究

Electronic Commerce on the Virtual Private Network - Technology, Management, and Application Issues

計畫編號：NSC 89-2416-H-009-013
執行期限：88 年 8 月 1 日至 89 年 7 月 31 日

主持人：羅濟群　　國立交通大學資訊管理研究所
計畫參與人員：莊秉文　　國立交通大學資訊管理研究所

一、中文摘要

商業資訊的公開與企業內私有資訊的安全，是企業組織發展電子商務的重要課題，而虛擬私有網路技術正提供了企業私有資訊安全問題的解決方案。本研究計劃旨在探討企業建構虛擬私有網路上技術面的相關課題，並歸納出整體性的虛擬私有網路架構，做為企業利用虛擬私有網路進行電子商務時的參考。

關鍵詞：虛擬私有網路、電子商務

Abstract

With the advent of the Internet, the Electronic Commerce (EC) becomes a reality. Openness creates security threats to cooperator's confidential information. The Virtual Private Network (VPN) provides a good solution to the security of business information. According to business requirement, we will an VPN architecture for business to use.

Keywords:virtual private network, electronic commerce

二、計畫緣由與目的

隨著網際網路技術的成熟發展與資訊技術的普及，電子商務已成為目前企業組織在電腦資訊技術應用上的主要目的，而商業資訊的流通與公開，便是企業組織發展電子商務的重要課題。然而，商業資訊的公開與企業內私有資訊的安全，實為相互抵觸的兩面，也是企業發展電子商務急待解決的問題。

本研究計劃的目的，在於探討以網際網路為基礎之虛擬私有網路，從而提出一個用來支援企業進行電子商務的虛擬私有網路架構。本年度乃針對技術面進行研究，內容包括對網路安全機制的研究，虛擬私有網路建置相關的傳輸協定研究，以及企業如何在虛擬私有網路環境下應用相關資訊服務功能，最後提出一套適當的虛擬私有網路架構，做為企業組織建構虛擬私有網路時的參考，以期取得在商業訊息流通、公開，與企業資訊安全的平衡點，發揮電子商務上的最大效益。

三、結果與討論

本研究計劃主要規劃為三年期，在第一年(本年度)的研究計劃中, 我們規劃探討企業組織利用虛擬私有網路進行電子商務

時，與技術面相關的議題研究，並已獲得顯著的研究成果。首先，我們針對企業組織進行電子商務的各種相關模式與資訊安全需求加以探討，然後再針對這些安全需求，探討虛擬私有網路的相關技術加以解決；依據這些研究與探討後的結果，提出一套以網際網路為基礎的虛擬私有網路架構，做為企業組織利用虛擬私有網路進行電子商務時的參考。

(一)電子商務的分類與安全需求

Kalakota & Whinston [1997]將電子商務分成了三種不同的應用：

1. 企業組織間的電子商務：即企業與企業間的電子商務(B2B)，可以促進企業間的商業應用更加便利。
2. 企業內部的電子商務：即組織內的電子商務，可以幫助企業傳遞內部訊息，並且將組織內各種重要的功能整合。
3. 顧客與企業間的電子商務：顧客與企業間的電子商務(B2C)，以電子傳送技術來輔助顧客對於公司的交易。

確保交易安全性可說是電子商務最重要的課題，保證電子商務的交易過程安全，才能夠提高使用者的意願。針對交易過程的安全性加以探討，我們可約略歸納出企業組織進行電子商務時，相關的安全需求包括：

1. 私密性(confidentiality)：能夠保證特定資訊的隱密性。
2. 身份驗證(authentication)：能夠保證通訊對方的身份。
3. 資料真確性(data integrity)：能夠保證所儲存的或傳送的資料未被修改。
4. 不可抵賴性(non-repudiation)：能夠使通訊雙方不可否認其曾經參與的資訊溝通行為。
5. 存取控管(access control)：能夠決定進入者可以存取特定資訊的權限。

表 1 不同型態電子商務的安全需求

應用	私密性	身份驗證	資料真確性	不可抵賴性	存取控管
企業間	極重要	極重要	極重要	極重要	極重要
企業內	極重要	極重要	極重要	非必要	極重要
顧客	極重要	極重要	極重要	極重要	非必要

在不同的電子商務應用之下，著重不同的安全需求。我們已針對這些不同的應用與安全需求加以探討，表 1 列出不同型態電子商務所對應的安全需求。

(二)虛擬私有網路技術與安全機制

所謂虛擬私有網路(virtual private network, VPN)，就是在公眾數據網路上建立屬於自己的私有數據網路。虛擬私有網路主要的需求，包括企業內部網路對外節點要有適合需求的頻寬，以便對網際網路進行訊息存取，也可能需要搭配防火牆系統或路由器，當公司內部的私有資訊要透過網際網路傳給其它公司內部網路時，所要傳輸的資訊必定經過一定程度的資訊安全保障，即使用適當的安全機制，並可能透過觀念上具安全性的通道(secure tunnel)來傳輸資料。對於非私有而可公開的訊息則可以直接丟到網際網路上傳遞。

我們針對現行的技術加以探討，可歸納出虛擬私有網路主要的應用方式可分為下面數種：

1. 遠端存取(Remote Access)：使用遠端存取的模式，需要在企業內部與客戶端加裝對應的虛擬私有網路軟體，當使用者撥接進入 ISP 伺服器後，透過網際網路或 ISP 骨幹網路，建立通道連回企業組織內部網路。
2. 站對站(Site-to-Site)：站對站的虛擬私有網路主要是針對由分支機構連往組織總部的應用方式，分支機構透過網際網路或 ISP 骨幹網路建立通道來傳送資料到組織總部，而不必再負擔各分支機構連回總部的長程專線。

3. 商際網路(Extranet)：這種應用方式的基本概念就是利用虛擬私有網路的存取控制與身份驗證等等服務，以決定進入者有沒有權限可以存取特定的資訊。外界人士可以透過網際網路或 ISP 骨幹網路上建立的通道連到企業組織防火牆，但防火牆內部則由虛擬私有網路的存取控制服務來管理，以保證企業組織內部的資訊安全。
4. 整合式：以企業組織建置虛擬私有網路的觀點來看，企業組織內部資料的存取，依各個單位而有不同的權限，因此虛擬私有網路所提供的加密、身份驗證以及存取控制等服務，即可將各個不同的單位分成不同的群組或等級，而各個群組或等級各有不同的資料存取權限。如此一來，對於企業組織內各個不同單位的資料安全有較佳的管理。

虛擬私有網路運用並整合了許多資訊安全上的技術與機制，根據功能來區分，虛擬私有網路主要採用下面四項技術：

1. 通道建置技術(tunneling)：通道建置技術是為了將私有數據網路的資料在公眾數據網路上傳輸，所發展出來的一種資料封裝方式(encapsulation)。現有的通道建置協定主要有 IPSec、PPTP 及 L2TP 等三種，IPSec 為第三層的通道建置技術，專門為網際網路所設計，不但符合現有 IPv4 的環境，同時也是 IPv6 的標準。PPTP 與 L2TP 均為第二層的通道建置技術，適合具有多種傳輸協定的環境。IPSec、PPTP、L2TP 三者最大的不同在於，若是運用 IPSec 的技術，使用者可以同時使用網際網路與虛擬私有網路的多點(multi-point)傳輸功能，而 PPTP 及 L2TP 只能執行點對點虛擬私有網路的功能，也較難以執行目前網際網路上的應用。
2. 加密技術(encryption)：為確保私有之資料於傳輸過程中，不會被其他人瀏覽竊取或篡改，可將封包在傳輸過程中先行加密，當封包傳送到目的地後，再將封包解密。加密技術可概分為對稱式密碼學(如 DES、RC2)與非對稱式密碼學(如 RSA)兩類，而在 IPSec 通道建置技術中的 ESP 機制便可將資訊封裝加密，以達到私密性。
3. 金匙管理技術(key management)：金匙管理乃針對金匙生命週期加以規劃，以確保金匙的安全，避免遭到竊取、破壞或偽造。金匙管理機制的核心大多是對稱式加解密技術與非對稱式加解密技術的混合體，現行的機制包括 SKIP、ISAKMP/Oakley 與 IKE。
4. 驗證技術(authentication)：驗證技術的應用可分為身份驗證、訊息驗證、與設備驗證等。身份驗證常用的機制有密碼、智慧卡(smart card)；訊息驗證常使用雜湊函數；而設備驗證則需仰賴由憑證中心(certificate authority, CA)所發出之 X.509 電子證書(certificate)。

(三)虛擬私有網路與電子商務相關性分析

在電子商務的應用中，針對不同的安全需求，虛擬私有網路都有相關的安全技術可以滿足(見表 2)。此外，在探討以虛擬私有網路安全機制來支援電子商務時，不同的虛擬私有網路應用方式與不同型態的電子商務亦有其相關性，茲分述於下：

表 2 虛擬私有網路所能滿足的安全需求

安全需求	虛擬私有網路安全技術
私密性	加解密技術、通道建置技術
身份驗證	身份驗證技術、通道建置技術、金匙管理技術
資料真確性	通道建置技術、雜湊函數
不可抵賴性	身份驗證技術、通道建置技術、金匙管理技術
存取控管	身份驗證技術、金匙管理技術

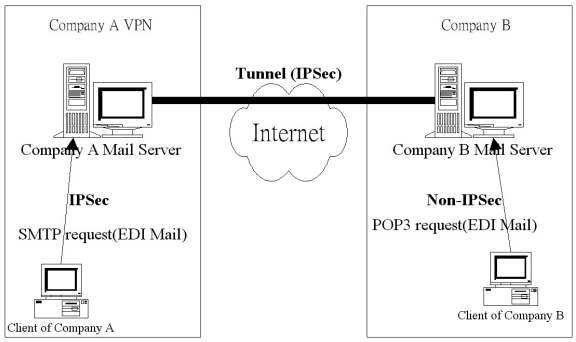

圖 1 利用 VPN 支援 B2B 電子商務系統架構圖

1. 企業與企業間以商際網路配合：商際網路應用方式可利用虛擬私有網路的存取控制與身份驗證等服務，以決定進入者有沒有權限可以存取特定的資訊。企業與企業間的合作、聯盟或是上下游的訂購下單等，都可以商際網路的虛擬私有網路來進行。我們可以 IPSec 相關協定為基礎達成此需求(見圖 1)。
2. 企業內以整合方式配合：站對站的應用方式可以提供企業內部總公司與分公司之間的商務資訊交換的安全保障。而遠端存取的方式可使在企業組織外活動的行動工作人員在需要時，透過撥接方式進入公司內部網路。此處的系統架構將以 IPSec 為基礎，再搭配目前在 L2TP 中與 IPSec 整合的方式為較佳的解決方案。
3. 顧客與企業間的應用：顧客與企業間的電子商務，虛擬私有網路並不那麼適宜提供支援。因為虛擬私有網路適用於通訊雙方先有一定的規範或配合。不過商家也可以設法與顧客取得協議，做為爾後溝通的基礎。針對具有協議的顧客使用安全機制，一般顧客則使用不具安全性的傳輸模式(見圖 2)。

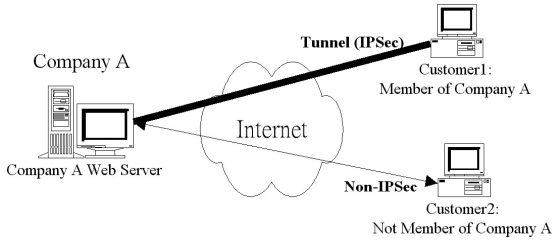

圖 2 利用 VPN 支援 B2C 電子商務系統架構圖

(四)結論

經由對相關文件、傳輸技術與協定、安全機制等的研究，並根據我們進行系統實作與測試的結果，企業組織若利用虛擬私有網路來進行電子商務，將可以同時顧及資訊公開性與安全性的問題。企業首先應對其組織的電子商務模式進行需求分析，然後再由這些需求，對應到能滿足這些需求的虛擬私有網路技術。

我們認為以 IPSec 協定為基礎來建構虛擬私有網路是現行較好的解決方案；由於 IPSec 協定與網際網路的相容性最高，不但可與 IKE 金匙管理協定、L2TP 協定、防火牆系統等相互配合，並且運用的方式也頗具多樣化，理論上將能夠適用於大多數企業的電子商務需求。

四、計畫成果自評

目前國內對於虛擬私有網路的相關研究，多半集中於網路安全技術的研發，缺乏整體的思考與探討。本研究針對虛擬私有網路技術進行的整體性的探討，提出具建設性的問題與解決方案，無論在學術或實務上都具有肯定性的參考價值；如同本計畫初期的規劃，我們已歸納出適當的虛擬私有網路系統架構。不過相關網路安全技術仍在發展，有許多細部與非技術性的問題有待探討，這將是我們與國內其他研究人員所該繼續努力的方向。

五、參考文獻

[1] R. Kalakota, A. B. Whinston, “Electronic Commerce – A Manager’s Guide”, *Addison Wesley*, 1997
[2] R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, 1998
[3] W. Stallings, “Cryptography and Network Security – principles and practice”, *Prentice Hall*, 1999
[4] ***資訊安全通訊***, **第五卷第三期**, 1999
[5] **郭雅惠**, “**以虛擬私有網路的安全機制支援電子商務之研究**”, ***交通大學資訊管理研究所碩士論文***, 2000