南　華　大　學

資 訊 管 理 學 系

碩 士 論 文

防 火 牆 結 合 虛 擬 私 有 網 路 技 術 應 用 於 企 業 內 部 網 路 通 訊 安 全

A method to improve the security of intranet network by combining firewall with virtual private network

研 究 生：張 逸 為

指導教授：王 昌 斌 博士

中華民國　九十六　年　六　月　十五　日

南 華 大 學

資訊管理研究所

碩 士 學 位 論 文

防火牆結合虛擬私有網路技術應用於企業內部網路通訊安全

研究生：張逸彥

經考試合格特此證明

口試委員：謝[illegible]

郭宏林

[illegible]

指導教授：[illegible]

系主任（所長）：資訊管理學系 系主任吳光閔

口試日期：中華民國 96 年 6 月 15 日

誌　　謝

首先誠摯的感謝指導教授王昌斌博士，老師悉心的教導促使得以一窺網路安全領域的深奧，不時地討論並指點正確方向，使我在這些年中獲益匪淺，老師對學問的嚴謹更是我輩學習的典範。

感謝南榮圖資處全體同仁大力協助，因為有你們的體諒及幫忙，使得求學過程更為順遂。亮光同學不厭其煩的指出我研究中的缺失，總能在迷惘時為之解惑。感謝友訊科技公司張育誠先生提供設備以供研究之用。當然也不能忘記實驗室的蔡政宇學弟，您的幫忙及關心我銘感在心。另外，女朋友在背後默默地支持更是我前進的動力，感謝她的體諒、包容與生活上的鼓勵，永銘吾心。

最後，謹以此文獻給我摯愛的父親，雖您無法親眼目睹我完成學業，仍盼望能與您分享這份喜悅。

防火牆結合虛擬私有網路技術應用於企業內部網路通訊安全

學生：張 逸 為　　指導教授：王 昌 斌 博士

南　華　大　學　資訊管理學系碩士班

摘　　要

近年來資訊管理意識抬頭，企業為達高效率而大力投入資訊及網路化應用來藉以提高企業競爭力。在資訊化普及運用後，隨即面臨資訊安全防護艱鉅考驗，為確保資訊資產安全，往往需投入大量資源，包括設備與人力，來防堵來自網際網路（Internet）的入侵和攻擊。然而來自企業內部網路（Intranet）仍是資訊安全更值得重視之安全問題，尤其在網路速度及存取權限的先天優勢下，讓保密資訊易於內部網路傳輸時遭受竊取，使資訊安全大打折扣。

防火牆（Firewall）是一種硬體或軟體形式的網路防護機制，常應用於管控企業內外部網路的資訊傳遞，藉由適當設定可以有效的阻擋外部網路非法存取企業內部資源，同時亦可有效控管內部網路使用網際網路資源。如何以最簡易及節省資源之方式來加強防火牆內部之安全控管是一個值得注意之問題。

虛擬私人網路（Virtual private network, VPN）是一種採用加密隧道的連線技術，可運用在企業彼此間網路連結，達到資訊傳遞安全需求。

透過此種連線方式，使用公開網際網路連線時，仍可保有如專線連接的安全性與保密性。由於虛擬私人網路連線時亦可採用不加密方式，但該連線存有資訊被盜取風險，不適用於一些敏感資訊之傳輸。目前許多企業所使用的虛擬私有網路技術，仍存有安全性不足、跨平台性較差及設置不易等問題。

本研究旨在探討在不改變現有規劃下，以有限資源加強內部網路通訊安全。在避免建置繁雜與高可用性考量下，本研究以穩定性較佳的嵌入式系統（Embedded system）實際模擬設置易於安裝部署之虛擬私人網路，並結合防火牆安全控管，提供企業改善內部網路通訊安全一個參考方法。

關鍵字：防火牆、虛擬私有網路、嵌入式系統

A method to improve the security of intranet network by combining firewall with virtual private network

Student：Yi-Wei Chnag Advisors：Dr. Chang-Bin Wang.

Department of Information Management
The M.I.M. Program
Nan-Hua University

ABSTRACT

Because of the raising consciousness of information management in recent years, enterprise for high efficiency of reaching but great input information and network to should be used for and used to raise enterprise's competitiveness. In order to guarantee information security, ample resources, including equipment and human resources, must be put after the application of information and network. However the security problems come from Intranet are more serious than come form Internet because of the congenital advantage the network bandwidth and privilege.

Firewall, a kind of hardware or the software implementations, is the protection mechanism to ensure the valid information transmission of Internet by suitable policy. Information transmission insides firework is usually weak in security management, therefore it is interesting research topic by using simple implementations to managing the information transmission insides firework.

The virtual private network (VPN), a secure data transmission by using the encrypted tunnel technology, can be used in order to get secure communication between enterprises. The information security and privacy can be guaranteed by using VPN in Internet. Transposition transmission can

be adopted in VPN, but it is not suitable for the transmission of some sensitive information. Nowadays there are still many problems of security and implementation in many enterprise applications of VPN.

In this research, we focus on the implementation to enhancing the intranet security without changing construct. Our implementation is designed by VPN in embedded systems and is combined the management of firewall. The implementation is an efficient solution to improve the security in intranet.
Keywords: Firewall, virtual private network (VPN), embedded system.

目　錄

表　　目　　錄

圖　　目　　錄

第一章 緒論

第一節 研究背景

網際網路發展至今，顛覆人們傳統生活及企業營運模式，透過網際網路可無限制區域、時間、設備和人員，進行購買、查詢、傳遞訊息與影音互動等行為，更成為企業快速取得資訊的重要命脈，在如此多元化的網路應用下，資訊安全問題也相對地備受關注，CERT/CC 的報告中指出全球資訊安全事件，在 2001 年為 52,658 件，2002 年 82,094 件，2003 年更提高到 137,529 件[27]，這種情況下造成企業界極大的損失，圖 1 是由 CERT/CC 網站的統計數據所彙製之資訊安全事件成長趨勢圖。另外，在美國 CSI/FBI 電腦犯罪與安全調查中，電腦資料被非法存取的損失單一事件平均為 85,621 美元，資訊安全所造成的總損失為 52,494,290 美元[28]，由此可見，建立網路安全的管理機制，已是當下的網路安全防護不容乎視的執行工作。

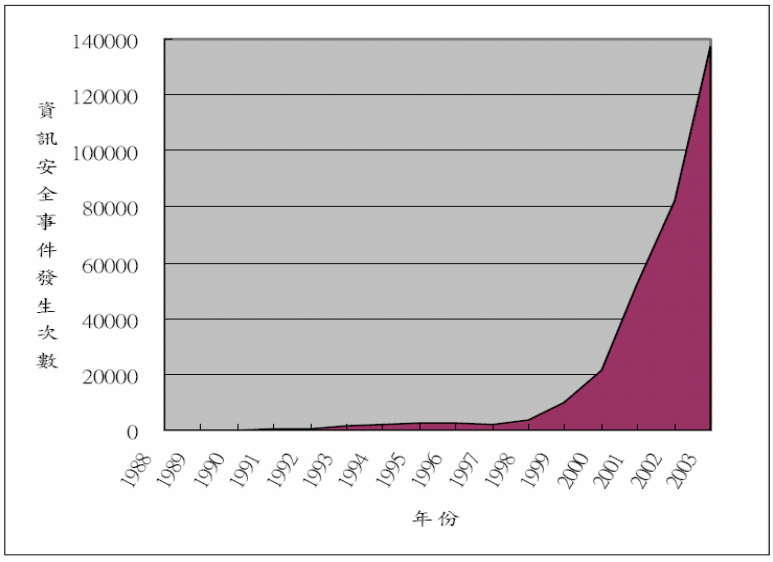

圖 1. 資訊安全事件成長趨勢圖

資料來源：整理自 CERT/CC 網站的統計數據所彙製[27]

第二節 研究動機

多數資訊安全防護機制，仍針對外部網路與內部網路連線間之安全防護動作，事實上企業區域網路中資訊傳輸隱藏著資安危機，藉由高速頻寬、存取權限高以及網路區域劃分明顯等特性，企業區域網路所傳遞機密資訊，隨時有被竊聽、攔截可能，成為企業內部資訊安全之隱憂。在各界採取資訊安全防護措施中，以防火牆（Firewall）與虛擬私有網路（Virtual Private Network, VPN）應用最為廣泛，防火牆常配置於企業內部網路（Intranet）與外部網路（Internet）之間，進行網路連線管控，但即使企業將伺服器與使用者網段分隔，當使用者通過內部網路存取企業資源時，資訊安全事件即可能發生。

虛擬私有網路是近年來網際網路應用中最常被用來建置資訊安全通道之技術，自 2004 年起其市場規模逐漸被開啟，是個相當受注目的應用趨勢，因為虛擬私有網路利用公用網路取代專線連接企業的區域網路，不僅大幅降低建制成本，也提高了未來擴充的便利性。朱澔偉研究虛擬私有網路全球市場現況預測中發現至 2008 年預估整體營收將達 4 百萬美元，且未來整體市場呈現逐年成長之趨勢，預估在 2008 年全球寬頻基礎建設更趨完善，市場需求將會被大量開啟，但目前廣受企業青睞的虛擬私有網路技術，仍存有缺乏足夠安全性與技術過於複雜不易使用等問題[34]。

第三節 研究目的

藉由防火牆與虛擬私有網路技術，透過網路存取權限、身分確認與加密通訊機制之協助，可有效控管網路資源存取維護網路安全，然而企業區域網路中通訊安全亦需要這些防護技術來協助，但在虛擬私有網路應用技術上，存有與防火牆整合性差、設定手續過於繁複和不易跨平台等缺點，故在管理上來說必須具備足夠的專業知識才有辦法

勝任。

因此本研究係使用較容易設置的虛擬網路技術，搭配應用彈性佳之軟體式防火牆進行建置。由於虛擬私有網路技術可建立一個加密的連線通道，讓資訊傳遞時即使被監聽或攔截亦無法判讀，因此可彌補資料傳輸時所欠缺的安全性。使用虛擬私有網路技術結合防火牆規則控管下便可達到區域網路安全需求。本研究分別採用四種作業系統平台 Windows、Linux、FreeBSD 及 Pfsense 搭配防火牆與虛擬私有網路軟體進行效能評估，篩選出效能最佳之作業系統平台進而將之建為嵌入式系統，提供一個低成本高效能防火牆結合虛擬私有網路技術方法，以改善企業內部網路通訊安全。

第四節 研究架構

本論文共分五章，各章內容摘要說明如下：

第一章:說明本研究的研究背景與動機,並敘述本研究之主要目的。

第二章：探討與本研究相關之文獻，包括防火牆、虛擬私有網路、嵌入式系統和網路竊聽。

第三章：依據相關理論基礎，透過防火牆結合虛擬私有網路技術，建置出企業區域網路通訊安全之方法。

第四章：針對第三章所發展出的相關架構,探討其安全性以及效能分析。

第五章：總結本論文之成果，並提出相關建議。

第五節 研究流程

本研究先以文獻探討與資料蒐集之方式，對於防火牆、虛擬私有網路、嵌入式系統和網路竊聽等概念進行相關探討，以分析建構防火

牆結合虛擬私有網路系統之相關技術所面臨的問題，並確立本研究的研究流程，建立系統開發方法，作為整體發展的步驟。再以實作進行該整合系統應用於企業區域網路，結合頻寬需求及網路安全之評估與分析，進而驗證所提出構想之安全性及可行性，以達到本研究完整架構及結論，流程圖如圖 2 所示。

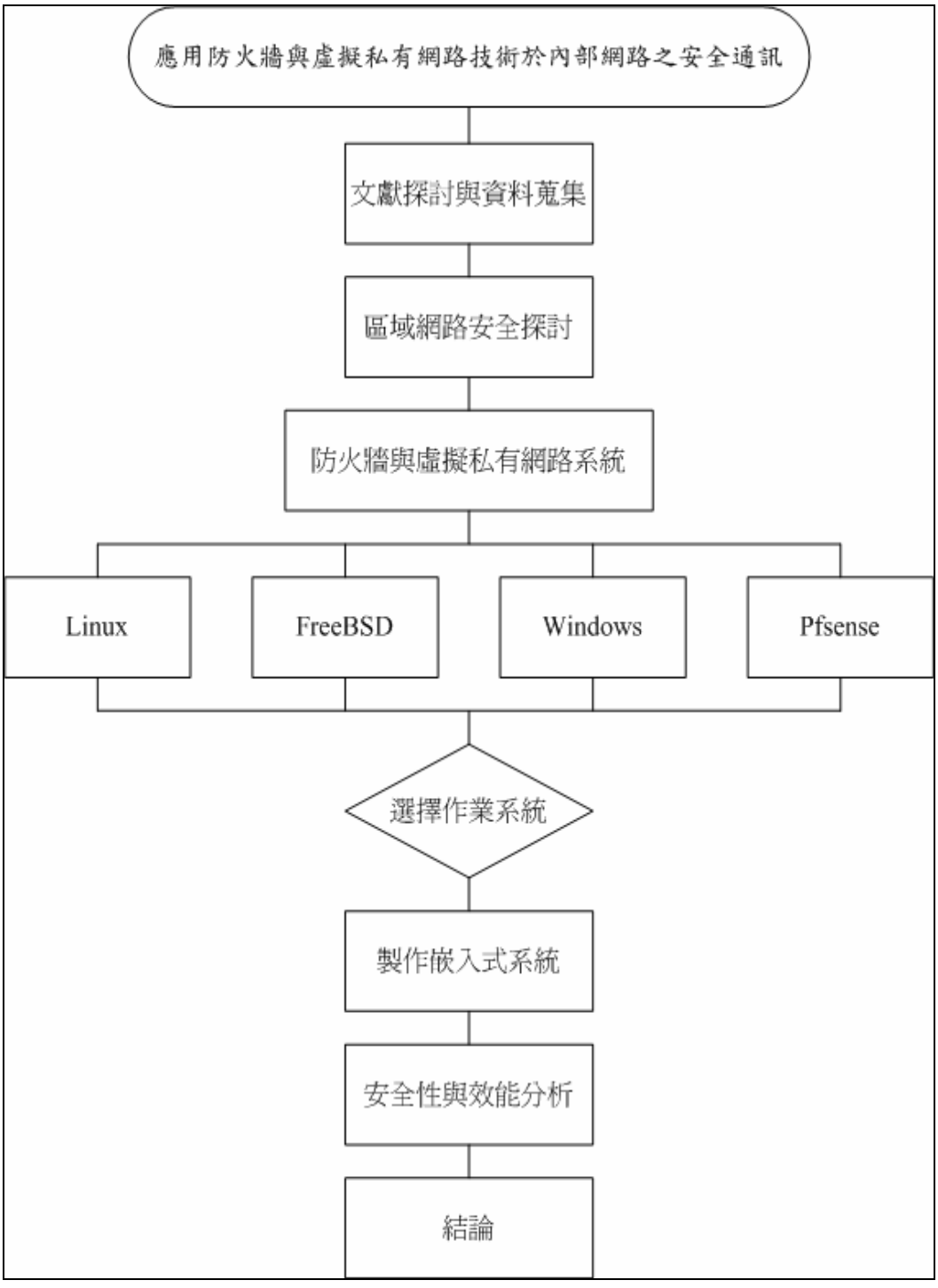

圖 2. 研究流程圖

第二章 文獻探討

本研究主要在探討如何使用防火牆結合虛擬私有網路技術，以達企業區域網路間之通訊安全，因此本章進行防火牆、虛擬私有網路、嵌入式系統及網路竊聽等相關文獻分析蒐集與探討。本章內容分為四個部份，首先對企業應用在區域網路防護機制進行探討，再針對造成區域網路資訊安全漏洞原因進行分析，並參考嵌入系統製作方法，最後對防火牆結合虛擬私有網路相關研究加以整理分析，作為本研究的概念架構與理論基礎之依據。

第一節 防火牆

壹、何謂防火牆

蔡國棟於網路生活雜誌中指出防火牆是一套能夠在兩個或兩個以上的網路之間，明顯區隔出一條界線的電腦軟硬體裝置的組合[15]。理論上，當網路間有安全上的考量時即可裝設防火牆，但一般而言，防火牆大多架設於網際網路與組織內部網路之間，成為內部受信任的網路與外部不受信任的網路之間的區隔通口。D. Brent Chapman & Elizabeth D. Zwicky 將防火牆定義為：是一個用以被保護的網路與網際網路之間或與其他網路之間的控制連線措施[18]。

網路防火牆可區隔不同安全等級的網路，並提供各個網路間的控管功能。防火牆可提供雙向的安全管理機制，不僅能防止外界的入侵，也可以限制內部主機對外的通訊。具體的來說，它只允許一些特定的資料通過，不論是從外面進入內部網路亦或是內部網路傳輸到外界的資料，都必須經過防火牆的確認手續才能放行，而這些確認手續是由一些事先設定的安全規則和政策來完成的[3]。

貳、防火牆的種類

夏雲浩認為防火牆的分類有封包過濾（packet filtering）、迴路通訊閘（circuit gateways）、及應用程式通訊閘（application gateways）等三種[8]。Robert Zalenski 認為因應不同的資訊安全需求，防火牆已演變成下列資料中所提到的六種模式，這些技術通常採用混合型的技術呈現[12][22]。

一、Application-based firewall

一套可以設定允許存取或是拒絕存取網路資源的軟體，提供了紀錄檔以供查詢連線狀態，也提供了使用者層級的認證，但是它不提供 internal 與 external 之間的連線控制，相對於 packet filter，需要付出較高的成本，也不支援所有可能的連線。

二、Packet filtering

是最容易建置的防火牆，路由器就可以做為封包過濾的功能，經由一部設備就可以保護整個網路，它透過 IP 位址、子網路遮罩、TCP 或是 UDP 埠等條件作為允許或是拒絕存取網路，所以用戶端不需要做任何設定或是安裝軟體，可使用許多的硬體或是軟體來達成。

三、Stateful-inspection

Packet filter 技術的加強版，同樣運作於網路層與傳輸層，提供低成本與高流量輸出，packet filtering 檢測各別封包的內容，但 stateful-inspection 檢測多重封包流的屬性，可由上一個封包流來決定下一個封包流的通行與否，另外 packet filtering 使用 static packet filter，放行的通訊協定是永久開放，stateful-inspection 採用 dynamic packet filter，可以在必要時才會開放通訊協定，且在使用後馬上關閉通訊協定，較不易被駭客

攻擊。

四、Proxy

一部介於內部網路與網際網路之間的伺服器，對於進入的資料，proxy 將接收到的資料轉進企業內部網路的使用者，對於外出的資料，proxy 則代替使用者發送資料到網際網路，proxy 提供高階的管理、良好的紀錄功能、極佳的快取與使用者認證機制，缺點是設定較為複雜、有潛在的效能瓶頸、無法應用於所有的程式、不同的服務和不同的主機與使用者可能需要安裝額外的程式等。

五、NAT

允許一個網路或多個網路經由一個或多個 IP 連接到網際網路，NAT 本身不提供任何安全，但是它可以將企業內部網路隱藏成單一點連接到網際網路，不過在不連接網際網路時它不會將位址做轉換的動作，NAT 會影響加解密與認證機制，也會影響 packet filter。

六、VPN

提供加解密與資料完整性保護，在經由大眾網路時仍然能夠確保像私有網路的環境，但需要付出效能降低的成本，也可能產生新安全性問題。

參、防火牆的架構

葉輝煌引述 Robert Zalenski 的資料中現今的防火牆架構可分為下列幾種[12][22]：

一、Single box

最簡單的防火牆架構，一個擁有防火牆運作的單一的物件，優點是由於只有一個單一物件，容易做出正確設定，但相

對的缺點就是所有的安全都依賴這個物件，且缺乏備援的線路，不過由於架構簡單，很容易就可以知道架構弱點並加以防制，由於 single box 價格便宜且容易理解，非常適合小型網路使用。

二、Screening router

一套擁有 packet filtering 系統的 screening router，它可以保護整個網路的安全，它也是最低的成本，缺點是缺乏彈性，另外對於允許通行或是拒絕通行的協定，只能針對 port 的編號去做檢查，無法針對 port 的實際內容檢查，且無法達到深層防禦，因此一但路由器的過濾妥協，則將沒有其它的安全保護。

三、Dual-homed host

一部至少擁有兩張網路卡的電腦，它能夠如同 router 一樣將 IP 封包由一個網路轉送到另一個網路，但是防火牆裡面與外面是無法完全互相通行，它需要經由高階的控制，來設防火牆裡面與外面的通行協定，由於提供高階的控制，因此需要較多的資源，相較於設備型的 packet filtering，它的效能會比設備型的差一些，它也有單點失誤危機，因此必須要明確的設定它的安全性。

四、Screened host

一部位於路由器後方內部網路的主機，當外部網路要流入內部網路時，必須先經由這部主機過濾，一般是採用 packet filter 方式，這部主機也可以稱為堡壘主機，用來屏障外部網路對內部網路的威脅。

五、Screened subnet

Screened host 的進階版，有別於 screened host，screened

subnet 針對堡壘主機再切割出一的網段，讓堡壘主機處於既不是外部網路也不是內部網路，而是獨立的一個網路，以增加安全性。

六、Architectures with multiple screened subnet

Screened subnet 的進階版，主要是運用在需要有不同安全性的環境，針對不同的安全性而切割更多的 screenedsubnet，在這環境中有內部路由器與外部路由器，兩部路由器之間採用一部或多部 dual-homed host 或 bastion host 連結。

七、Variations

結合上述技術所構成的環境，可以是非常富有彈性的組合，例如由多部堡壘主機結合多部內部路由器與多部外部路由器所組成。

八、Terminal servers and modem pools

當使用數據機作為存取內部網路資源時，要將 modem 整合到內部網路，如果沒有整合入內部網路，則必須開啟防火牆的規則，將造成駭客有入侵的管道，當使用 modem 作為存取外部網路資源時，要將數據機置於外部網路，以防止內部網路受到駭客的威脅。

九、Internal firewalls

防火牆通常是架構於外部網路與內部網路之間，可是在某些情況下可架設內部防火牆，例如用來隔絕測試主機、保護重要主機資料等。

自文獻得知防火牆為目前網際網路主要之防護機制，並隨著多元化入侵手法，防禦措施也呈現以複合技術進行安全管制，提供各種網路架構安全需求。

第二節 虛擬私有網路

壹、虛擬私有網路定義

在傳統的網路架構上，連接兩個私有網路大都使用專線，專線是一條獨立封閉的線路，可以保持私有網路的隱密性，可是專線的價格昂貴，尤其遠距專線，若能利用網際網路來建置私有網路的連線，將可大幅增加便利性、降低費用，且保有私有網路的安全性，這種網路稱為虛擬私有網路（Virtual Private Network，簡稱 VPN）[17]。

虛擬私有網路的觀念是應用隧道（tunneling）技術在公用網路（public networks）上邏輯性地區分多個虛擬的私有網路，以提供網路傳輸時之安全性及服務品質保障。由於虛擬私有網路是建構在公眾網路上，因此在建立虛擬私有網路之隧道時，若一次給足所要求的頻寬，則可能因使用量不高而浪費頻寬，反而降低整體公眾網路的鏈路使用率及系統可容納之使用者數量。但若配置予虛擬私有網路的頻寬過低，則將增加虛擬私有網路上連線被拒之機率[2]。

貳、虛擬私有網路起源

隨著企業經營型態的轉變與拓展，從一開始單一公司營運方式演變成數各區域性的經銷據點，每個據點會有屬於自己的內部網路，為達安全及私密性，公司間資訊傳遞便大量使用專線，透過這樣的方式，一旦企業分公司據點繁多，或者彼此距離遙遠，傳遞資訊的費用是相當可觀的支出。另外，員工因業務需求常透過不定點的外部網路存取公司內部資源，此種情況下，使用專線變的不再可行，於是有了虛擬私有網路的需求，該連線方式讓員工可以透過大眾網路，傳輸公司內部資料，並且可以確保這樣的傳輸過程，如同使用專線一樣地安全[17]。

叁、虛擬私有網路安全技術

構成虛擬私有網路安全技術要件，主要是傳輸中採用加密隧道連線，加密皆透過金鑰進行，因此如何保護金鑰避免遭竊或暴力破解，即是另一個衍生的安全問題，常見的因應方案為縮短金鑰有效時限，也就是在短時間內持續更換金鑰，如此一來即使欲破解金鑰，就須在短暫的時間內完成，並且得在金鑰更換之前，該機制下可避免金鑰被破解的可能性[29]。圖 3 為兩個不同區域網路開始建立虛擬私有網路加密隧道的步驟，首先進行雙方認證，接著比對雙方採用加密的方式，最後進行金鑰交換完成後即建立起加密的安全隧道，在隧道中傳遞的資料均已加密，即使被竊聽也無法判讀所傳遞的資訊[19]。

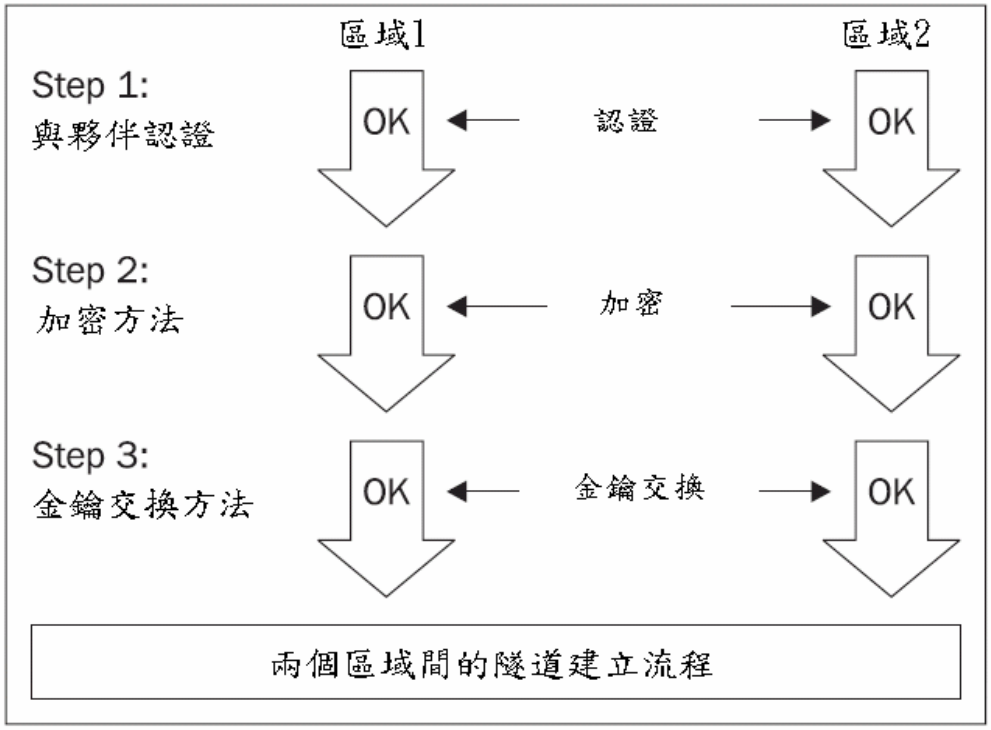

圖 3.虛擬私有網路建立隧道流程
資料來源：翻譯自OPENVPN [19]

肆、虛擬私有網路架構

葉輝煌[12]針對虛擬私有網路作詳細的整理，分述如下：

一、依照網路架構主要可分為三類：

（一）、Host-to-Host

用於兩部單一的資訊設備要做安全性的通訊，這兩部資訊設備可以位於公眾網路或是私有網路，這兩部資訊設備以外的設備都無法識別兩者間傳遞的資料(如圖4)。

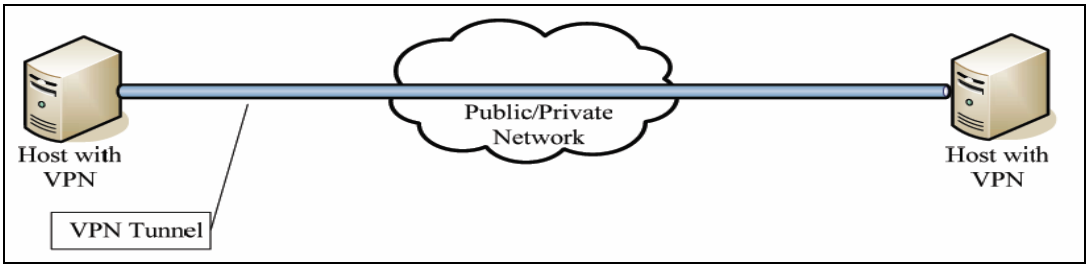

圖4. Host-to-Host VPN 示意圖

資料來源：動態IP網路中實行IPSec VPN [12]

（二）、Host-to-Gateway

用於一個單一資訊設備要存取一個私有網路的資源，在以往員工一旦外出出差，就無法存取公司資源或是極有限度的存取公司資源，可是透過虛擬私有網路就可以讓員工如同身處公司內部可以存取任何資源(如圖5)。

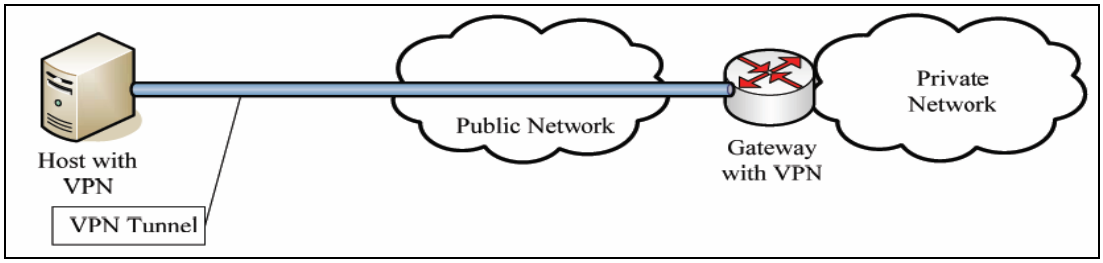

圖5. Host-to-Gateway VPN 示意圖

資料來源：動態IP網路中實行IPSec VPN [12]

（三）、Gateway-to-Gateway

通常用於兩個私人網路相互連接，像是總公司與分公司之間的連線，透過虛擬私有網路，總公司與分公司

之間猶如有一條專線連接，可以進行各種服務的連線，也可以用於總公司與協力廠商之間的相互連線（如圖6）。

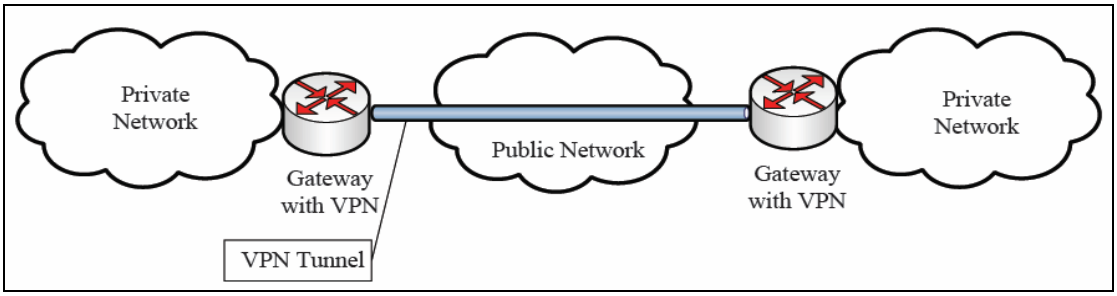

圖6. Gateway-to-Gateway VPN 示意圖

資料來源：動態IP網路中實行IPSec VPN [12]

伍、虛擬私有網路種類

目前常見的虛擬私有網路協定有 PPTP、L2TP、IPSec 與 SSL 四種[11] [12]：

一、PPTP：

是 PPP（Point to Point Protocol）的擴充，屬於 OSI 第二層的通道協定，支持該協定的公司包括 Microsoft、Ascend Communications、3Com/Primary Access、ECI Telematics 和 US Robotics 等。該協定會把網路協定的 datagram 放進 IP 封包，包裝好的封包看起來就像正常的 IP 封包一樣，所有遇到該封包的路由器或機器都會把它視為一個 IP 封包，以一般正常 IP 封包的方式來處理它。其優點在於它可讓許多不同的協定透過 IP 網路（如 Internet）來傳送，而由於 Microsoft 的作業系統內建支援 PPTP 協定，因此對一般使用者而言較具便利性。PPTP 的缺點是安全問題，PPTP 所使用的編碼技術並非很好，認證功能也不佳，因此對於極機密的資料傳送較不適合，Microsoft 使用 MPPE 及 EAP 協定以改進驗證及加密功能，運作圖如圖 7 所示。

PPTP 的運作原理簡述如下：

（一）、資料由第三層送至第二層的 PPTP driver 加密。

（二）、由第二層的 PPTP driver 回送至第三層重新封裝。

（三）、定址後依正常程序送至第一層傳輸。

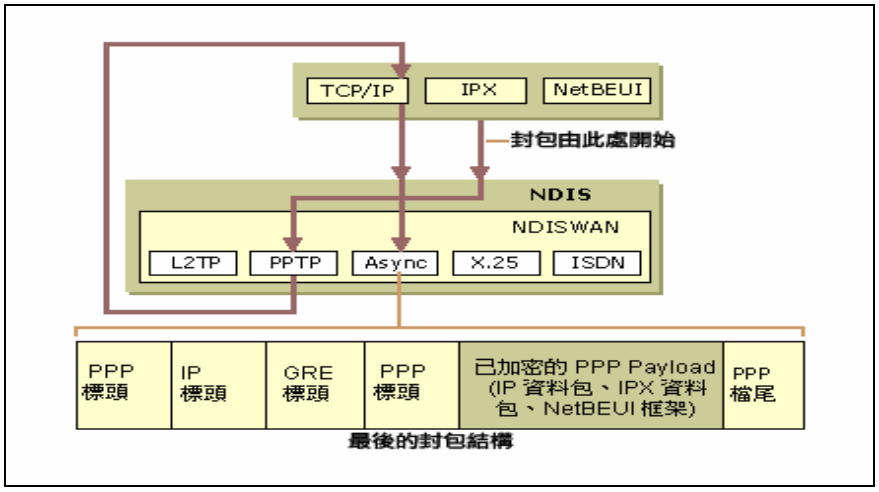

圖7. PPTP運作原理

資料來源：Microsoft TechNet，虛擬私人網路 [31]

PPTP 封包結構：

（一）、 首先使用 PPP 的標頭封裝已加密的 PPP 資料來建立 PPP 的框架，然後再以 GRE（Generic Routing Encapsulation）標頭封裝 PPP 的框架，所得的有效傳輸單元（payload）再以含有傳輸來源和目的地 IP 位址的 IP 標頭加以封裝。

（二）、 此 IP 資料包會再以資料連結通訊層的標頭和檔尾予以封裝。資料連結通訊層的標頭和檔尾會隨著所選用不同的技術類別而有所差異。

當透過 Ethernet 網路傳送 IP 資料包時，就會使用 Ethernet 的標頭和檔尾進行資料包的封裝；如果是經由類比式的電話線傳輸資料包的話，則會使用 PPP 的標頭和檔尾進行封裝，以此類推。當封包到達其目的地時，就會反向除去各個封裝層，

首先會除去資料連結通訊層的標頭和檔尾，然後依序除去 IP、GRE 以及 PPP 的標頭，最後再進行 PPP 資料的解密。

PPTP 的使用者驗證方式採用 PPP 的驗證方式，以微軟系統支援方式分為以下幾種：

（一）、PAP 非加密式驗證（明文傳送使用者名稱與密碼），當用戶端不支援其他驗證方式時用，安全性低。

（二）、SPAP 針對 Shiva 公司 Lan Rover 軟體用戶端提供加密式驗證，為雙向、可逆的加密。

（三）、CHAP 使用 MD5（Message-Digest Algorithm 5）交涉加密驗證，可於不同作業系統間提供加密式驗證。

（四）、MS-CHAP V1 由微軟於 CHAP 架構上發展，主要為提供 Windows 95 以上用戶端加密式驗證。MS-CHAP V2 提供 Windows 2000 以上用戶端。

（五）、EAP 延伸驗證通訊協定，支援較多驗證機制，如智慧卡的公開金鑰驗證、憑證等。比其他驗證方法（如 CHAP）提供了較多的安全性以避免暴力攻擊及密碼字典猜測。

PPTP 的加密方式，有以下幾種:

（一）、MPPE（Microsoft 點對點加密）以 RSA/RC4 進行資料加密。

（二）、微軟只有採用 MS-CHAP V1/V2 或 EAP-TLS 的驗證方式才能用 MPPE 進行資料加密。

（三）、MPPE 會在以 PPP 為標準的撥號連線或 PPTP VPN 連線中加密資料。其支援加強型（128 位元的機碼）及標準型（40 位元的機碼）的 MPPE 加密配置。

（四）、MPPE 提供 PPTP 連線及通道伺服器間資料的安全性。

二、L2TP（Layer 2 Tunneling Protocol）

L2TP 是結合 Layer-2 Forwarding（L2F）和 PPTP 的協定，L2F 通道協定是由 Cisco 在 1996 年提出，1997 年 Micorosoft 和 Cisco 公司把 PPTP 協定和 L2F 協定的優點結合在一起，形成了 L2TP 協定。

L2TP 能將任何 TCP/IP、IPX/SPX 或 NetBEUI 的數據組合加密，建立點對點通訊協定（PPP）訊框，並將 PPP 訊框封裝經非同步傳輸模式（ATM）、X.25、Frame relay、IP network 網路建立的隧道傳送。L2TP 本身不提供任何加密方法，當資料需要保密時，就要使用其他的加密機制，如 IPSec 加密機制，而 IETF（Internet Engineering Task Force）組織考慮 ISPec 已經日漸成熟因此將 IPSec 協定作為 L2TP 通道提供安全保護的加密機制，所以 L2TP 搭配 IPSec（L2TP/IPSec），採用使用者層級的 PPP 驗證方法和 IPSec，以憑證和資料驗證、整合性和加密，來進行電腦層級的驗證，運作圖如圖 8 所示。

以下針對 L2TP 運作做一說明：

（一）、當 L2TP 進行時，資料由第三層送至 L2TP Driver。

（二）、L2TP Driver 將資料的數據組合，建立點對點通訊協定（PPP）訊框。

（三）、送至 IPSec 進行加密處理。

（四）、加密處理送至第三層由 TCP/IP 封裝。

（五）、產生完整 L2TP/IPSec 封包向下層送出。

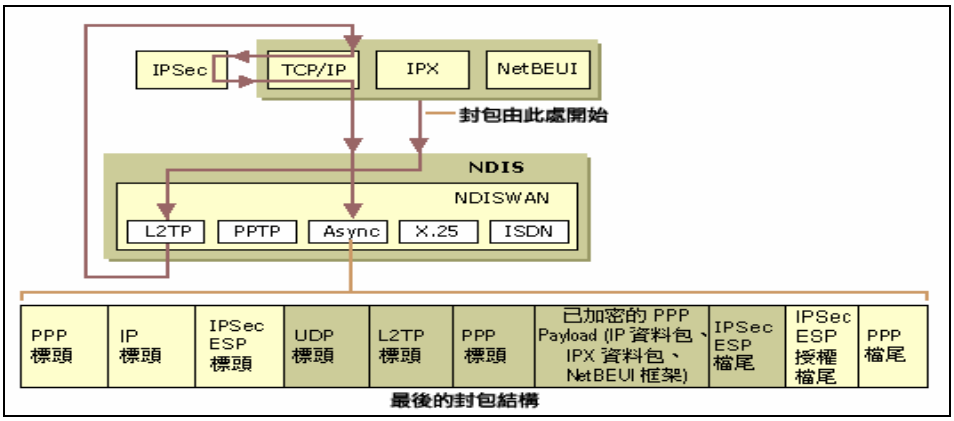

圖8. L2TP運作原理

資料來源：Microsoft TechNet，虛擬私人網路 [31]

由 L2TP 封包可以看到整個封包比 PPTP 複雜，它加上 IPSec 中 ESP 協定，這是 L2TP 本身不提供的，加密機制是由 IPSec 進行。此外，封包中有一 UDP Header，表示 L2TP 不同於 PPTP 之 TCP 傳輸，而是採用 UDP 來傳送 L2TP 封裝的 PPP 訊框。

當 L2TP 設定使用 IP 傳輸時，L2TP 可以用來作為 Internet 上的 VPN 通道通訊協定，使用 UDP 1701 與 500 連接埠，並包含維護通道的控制。

部署採用 L2TP 的 VPN 連線，必須以憑證為基礎結構，發出執行 IPSec 驗證所需的憑證。L2TP 的驗證方式分為二階段：電腦驗證及使用者驗證，電腦的驗證是採憑證基礎，當 IPSec 進行安全關聯性的建立同時完成。使用者的驗證方式與 PPTP 相同也是採用 PPP 的驗證。

L2TP 使用 IPSec 來進行資料的加密，分別採用 56-bit DES 及 Triple DES（3DES,168 bit），作為加密方式。

三、IPSec（Internet Protocol Security）

IPSec 是 IETF 所制定的標準，可以提供網際網路、內部網路、外部網路和遠端存取加密及認證等安全保護，是 Ipv6 實作

的標準之一（在 Ipv4 則可選擇）。IPSec 只提供基礎架構，因此容易套入新的演算法，非常具有彈性，另一個優點是具備透通性，使用者不需安裝或更新應用程式即可使用[11]。

在 RFC2401 中完整的定義了 IPSec 架構[24]，它是設計來達到網路層（network layer）中的安全通訊，主要有三個大協定：封裝安全負載（Encapsulation Security Payload, ESP）、認證表頭（Authentication Header, AH）、IKE，其中 ESP 提供認證加密，而 AH 只提供認證動作，通常是使用 MD5、SHA1（Secure Hash Algorithm 1）、HMAC（Hash Message Authentication Code）等演算法來確認使用者身份，IKE 則用來協商密鑰自動交換[9][11]。

IPSec 提供 ESP 和 AH 兩種通訊協定中，AH 提供資料的完整性和身份認證，確保 IP 封包在傳輸過程中未被更改，若封包在傳輸過程中被更改，接收端也會察覺。因此可保證資料完整性，並提供防竄改保護及確保主機驗證。而 ESP 提供與 AH 類似的功能，加入選擇性的資料機密性，將 IP 封包加密再傳輸，即使封包被擷取，也無法解開此封包觀看其內容，圖 9 為 IPSec header 的位置[9][11] [20]。

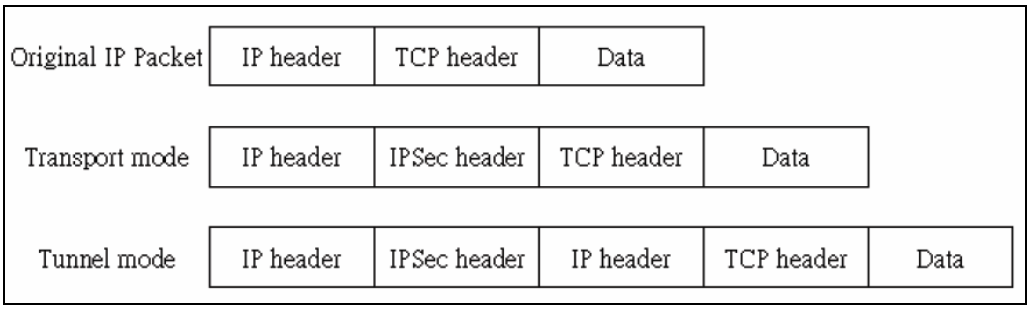

圖9. IPSec header位置
資料來源：動態IP網路中實行IPSec VPN [12]

IPSec 協定尚包括 IKE 協商程序，可爲 IPSec 產生密鑰，其它還包括演算法、密鑰長度、轉碼程式以及演算法專用的資

訊。而協商時常使用的參數則被歸類在一個單獨的文件中，爲 RFC 1407 IPSec OI（Domain of Interpretation），圖 10 是 IPSec DOI 關係圖[20]。

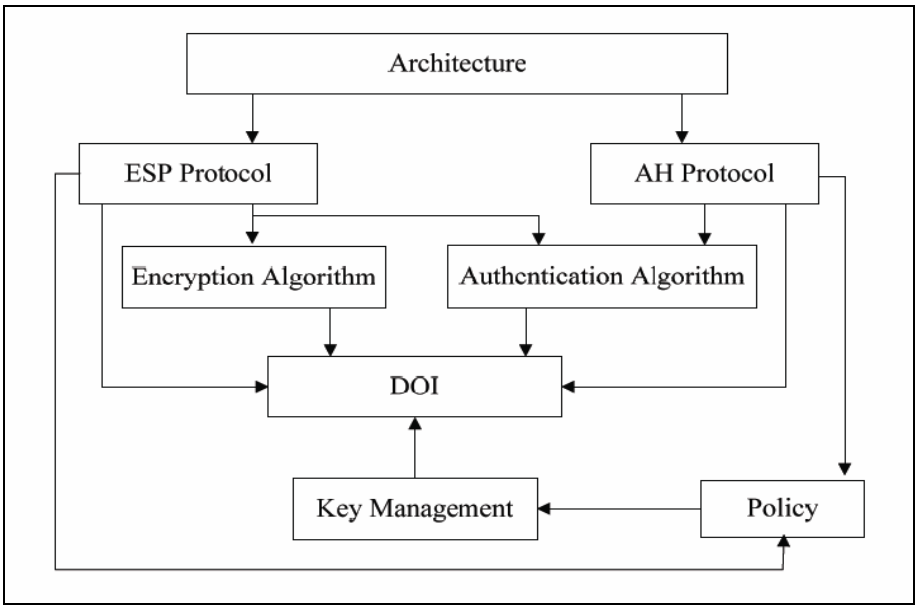

圖10 .IPSec架構圖
資料來源：IPSec: the new security standard for the Internet, intranets, ad virtual private networks [20]

AH 或 ESP 不提供實際的加密演算法來執行上述功能，但可使用現有的加密及驗證演算法。ESP 支援的加密演算法包括 DES-CBC、56 位元 DES 及 3DES。

若不需要較高機密性的傳輸，AH 足以提供驗證及完整性。若為需要高機密性的傳輸，則需要 ESP 及 AH。IPSec 運作有以下模式：

（一）、傳輸模式：

利用 AH 或 ESP 直接對 IP 封包驗證或加密，此模式適合在公司內部網路使用，保護由來源到目的地現有的 IP 封包安全。

（二）、通道模式：

利用 AH 或 ESP 來達成 IP 封包傳輸過程之一致性

或對 IP 封包加密，然後在這個 IP 封包外面再包上一層新的 IP 封包，而這個新的 IP 封包的目的地則指向一個通道端點，而此封包到達目的地後，會先移除外面的 IP 封包，再送到原來封包的目的地。這個傳輸模式主要是用在透過 Internet 傳輸機密資料時使用。

IPSec 運作模式如圖 11 所示：

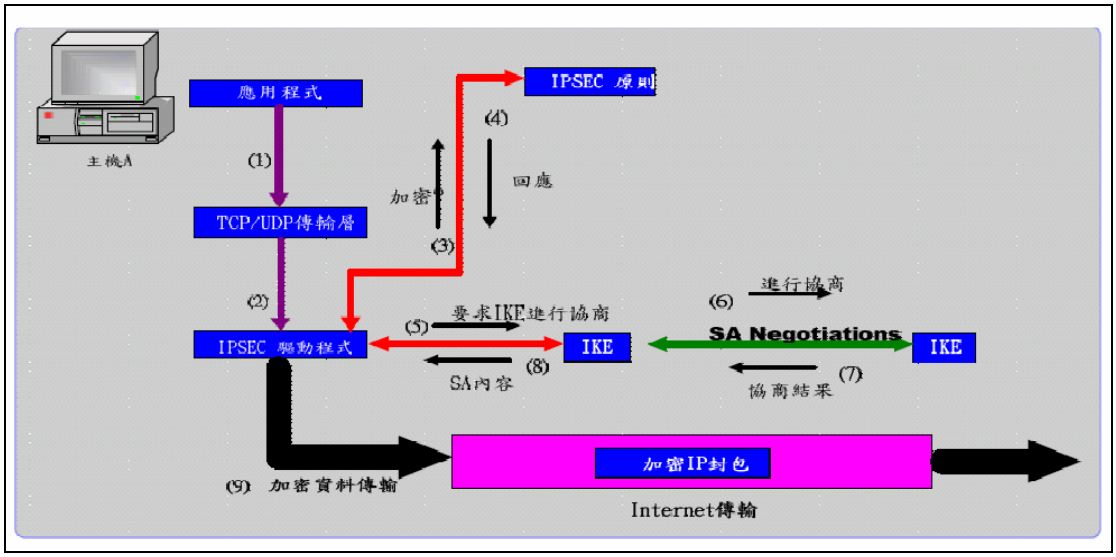

圖11. IPSec運作模式

資料來源：虛擬私有網路技術於無線網路上之通訊安全應用[11]

（一）、 應用程式送出資料至TCP/IP傳輸層。

（二）、 TCP/IP傳輸層送至IPSec驅動程式預備進行加密。

（三）、 由IPSec原則確認加密方式，IPSec要求與對方IKE進行SANegotiations。

（四）、 IKE收到SA後，IPSec依SA內容進行加密，並往下層送出封包經網際網路傳送（此時封包已加密）。

四、SSL（Secure Socket Layer）

SSL 原本是應用於網頁加密的一種技術，近年來 SSL 也被視為是 VPN 的一個新成員，由於 SSL 屬於 OSI 第四層的加密認證技術，IETF 更將 SSL 協定改進後命名為 TLS（Transport

Layer Security），並規範於 RFC 2246[25]，由於用戶端不需要安裝任何程式，用戶端只需要有瀏覽器就可以運作，因此成為非常熱門的技術之一。目前 IPSec 與 SSL 為兩大 VPN 熱門技術，許多的設備廠商都有推出相對應的產品，IPSec 與 SSL 都有其優缺點，以建置、管理方面來看，SSL 比 IPSec 方便很多，可是 SSL 無法達到 Gateway-to-Gateway 虛擬私有網路架構，且由於 SSL 是基於瀏覽器來執行，因此瀏覽器的安全性就間接影響了 SSL 的安全性，兩者可以視環境搭配使用。

在 SSL 虛擬私有網路領域裡 OpenVPN 是項嶄新的技術，透過 OpenSSL 技術的應用，支援 OSI（Open System Interconnection）Layer 7 架構裡的 Layer 2 與 Layer 3 多種不同的通訊協定，改進了傳統 SSL 虛擬私有網路技術只能應用於少許通訊協定缺乏延展性的缺點，以跨平台性而言，也是目前支援性最好的虛擬私有網路軟體。

其他虛擬私有網路之配置於遭遇困難時，往往都轉而採用非標準的解決方案技術，但由於標準不一的狀況下往往使安全性大打折扣，然而 OpenVPN 在安全性與網路架構裡使用模組化設計觀念，大幅擴增程式的延展性，它採用安全性高、穩定度佳的 TLS 機制來進行認證與編碼，同時具有安裝部署較容易，異於 IPSec 虛擬私有網路建置時過於複雜的特性，讓管理人員大幅減輕建置的負擔[16][19][32]。

OpenVPN 的優點：

（一）、Layer 2 and Layer 3 VPN

OpenVPN 支援兩種運作模式，可運作在 OSI Layer 7 網路架構中 Layer 2 或者 Layer 3 下。因此 OpenVPN

的隧道技術能傳送乙太網路訊框，IPX/SPX 或 NetBEUI 封包，異於其他類型的虛擬私有網路技術，常會遭遇無法支援該類型的通訊協定。

（二）、Protecting field workers with the internal firewall

支援漫遊使用者透過 OpenVPN 建立虛擬私有網路隧道，並透過該加密隧道連線存取網路資源，在該模式下移動式電腦同時可獲得企業中央式防火牆防護。此狀態運行時防火牆只需對區域網路設定放行一個網路服務埠即可運作連線。

（三）、OpenVPN connections can be tunneled through almost every firewall

OpenVPN 之隧道技術幾乎可以穿透所有的防火牆，如果架構中需要透過虛擬私有網路通道存取網際網路資源的方案，它便是良好的選擇。

（四）、Proxy support and configurations

OpenVPN 提供代理伺服器支援性，在伺服器端與使用者端能設定使用 TCP 或 UDP 埠的服務來運行。伺服器運作時，OpenVPN 以單純的模式等待使用者連線，使用者端僅須依據伺服器環境設定進行適當的配置。

（五）、Only one Port in the firewall must be opened to allow incoming connections

在 OpenVPN 第二版後，伺服器可採用不同的設定在每一個登入連線設定值上。這種運作模式則允許多種登入連線在這 TCP 與 UDP 服務上。

（六）、Virtual Interfaces allow very specific networking and

firewall rules

在 OpenVPN 的隧道技術裡，由於運作的模式是採用透過虛擬網路介面卡，因此可支援防火牆的存取規則以及 NAT 封包的轉送等功能。

（七）、High flexibility with extensive scripting possibilities

提供排程設定多點連接。這個排程功能可應用於常見的故障復原。

（八）、Transparent, high-performance support for dynamic IPs

在虛擬私有網路的隧道兩端，可使用廉價 ADSL 所配發的動態 IP，並且使用者無須去注意任何一方的 IP 變化。

（九）、No problems with NAT

在 OpenVPN 伺服器與使用者兩端，可以使用企業區域網路中所配置虛擬 IP 位置進行連線。

（十）、Simple Installation on any platform

在使用者與伺服器端均可以很容易安裝建置。尤其是體驗過在不同的架構嘗試設定 IPSec 連線，將會發現 OpenVPN 所謂的建置簡易的意思。

（十一）、Modular Design

模組設計以高度簡潔的架構呈現，在安全性和網路支援各項表現是卓著的。

OpenVPN 加密流程：

首先應用程式將原本傳輸資料轉而傳送至虛擬私有網路產生的虛擬網路卡（tun0），使之接收資料後傳送至 OpenVPN 程式，並進行資料的加密，加密後的資料透過設備真實網路卡傳送至網路上，此時的資料即呈加密狀態，即使被攔截也無法

判讀，資料接收端透過真實網路卡接收已加密資料，進而傳送至 OpenVPN 程式解密還原資料（如圖 12）。

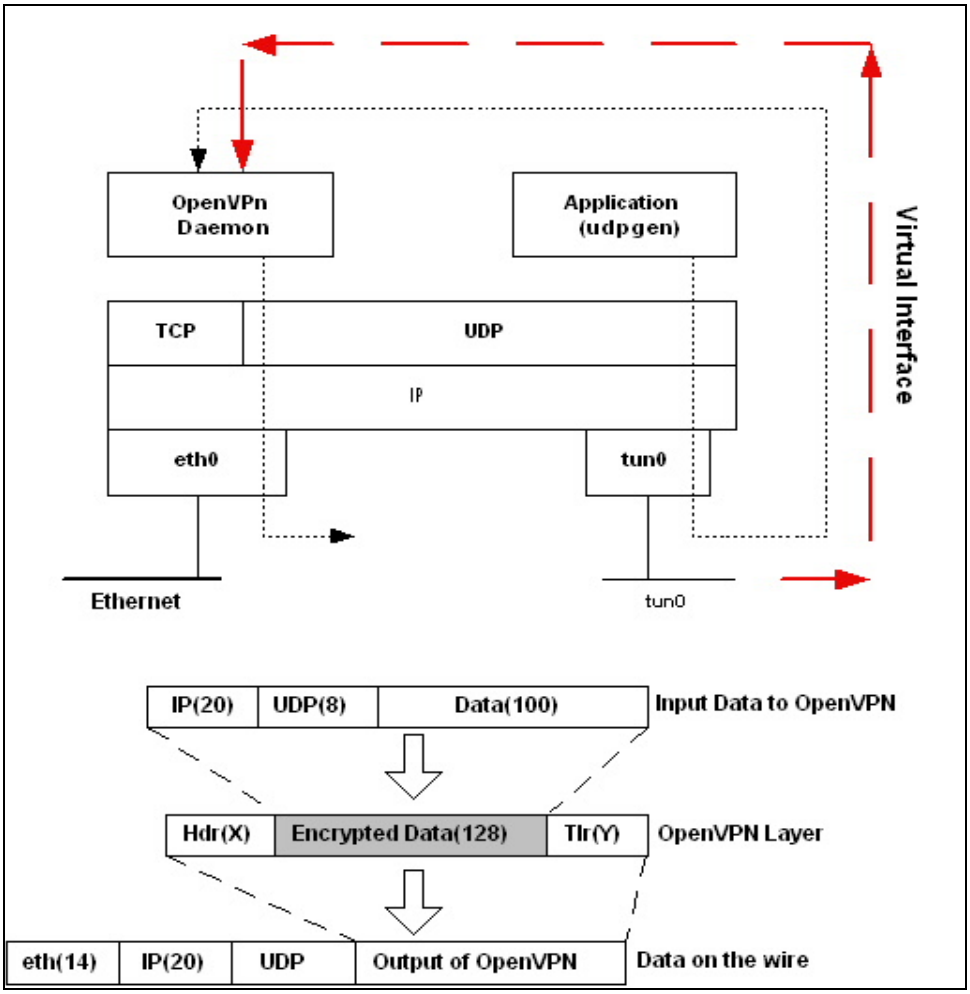

圖12. OpenVPN加密流程圖
資料來源：OPENVPN [19]

OpenVPN 高度的安全協定：

TLS（Transport Layer Security）是 OpenVPN 所採用的安全協定，它與 SSl 都是採用密碼學加密方式，達成身分證明與保護隱私權的目的，專家以保密性（Confidentiality）、認證性（Authentication）、整體性（Integrity）、不可否認性（Nonrepudiation）四個定義描述加密技術扮演的功能，TLS 則透過以下四種方法來達到該加密的功能[6]。

（一）、用數位簽名達到伺服器端的身分驗證和不可否認性。

（二）、用數位簽名達到客戶端的身分驗證和不可否認性。

（三）、運用加密技術滿足資料的保密性。

（四）、用訊息認證碼滿足資料的整體性。

然而 TLS 事實上是被設計用來取代 SSL 的，其版本的定位為 SSL 3.1 版，雖然它們之前只存在一小部份的差異，但仍因 SSL 是屬於網景（Netscape）的封閉性協定，因此技術規範組織（IETF, Internet Engineering Task Force）提出了這個展新的協定。TLS 協定在運作過程會歷經以下三個步驟，達成安全的通訊連線，也為 OpenVPN 進行了第一個資訊安全把關的動作。

（一）、 在用戶及伺服器之間協調，是要採用 TLS 方式還是要指定 SSL 版本（2.0 或 3.0）。這階段就會決定編碼加密的方式，以作為之後協定在交換上的使用。

（二）、 在雙方溝通完編碼加密的方法後，伺服器端要接受驗證，然後用戶才會產生出一把對稱金鑰，以作為之後傳輸資料的使用。至目前為止，整個過程都是在公開金鑰和 X.509 數位憑證之下所完成的，而數位憑證是憑證管理中心（CA, Certificate Authority）所核發出來的，通常交由公正的第三方來判別伺服端的真確性。進行這種單向的驗證是有其必要性的，因為用戶端要知道他正在與合法的伺服器溝通，而非偽裝者-就像一個造假的金融網站，會利用網路釣魚的方式不當獲利。用戶接下來要提供帳號及密碼，或是再進行一連串的驗證。所以，在此種封閉式的環境裡，會有一群已知的用戶保持連線也就是說，裡頭就只存在合法的公司與交易用戶這些

雙向驗證方式可是能提高線上交易的安全性。

（三）、 對稱金鑰是以公開金鑰加密過後再傳給伺服器端的，而公開金鑰裡頭包含由 CA 所驗證通過的數位憑證；所以在建立以及交換對稱金鑰之後，一切的通訊將使用對稱金鑰的演算法進行，而非以前所使用的公開金鑰。原因很簡單，因為對稱金鑰演算法較有效率，較容易計算出所得數值。到現在，所有 client-server 的交易活動均會以此對稱金鑰進行加密，直到連結中斷或金鑰過期為止，故這種方法即是在用戶端和伺服器之間，建立起一個安全連結的通道。

在 TLS 安全議題上，最備受關注在於如何挑選一個好的編碼加密方式，雖然有部份公開及對稱金鑰加密演算法可供在 SSL/TLS 傳輸之中使用，但是 TripleDES，甚至於更好的 AES 演算法，才是最安全、最備受推崇的。若以 DES 為加密演算法，而 MD5 為雜湊函數，就目前所知，已經不再安全了，因此在 OpenVPN 預設的加密方式裡，是以 BlowFish、AES、TripleDES 等加密方式作為安全連線的加密[29]。

OpenVPN 的缺點：

（一）、 與現有的 IPSec 技術不相容。

（二）、 異於 IPSec 技術已廣受設備廠商採用，並搭配其他商業化軟體應用之狀況。

（三）、 目前並無 OpenVPN 被應用在硬體設備的研發方案。

（四）、 該技術尚未被普及，仍有許多人不了解它的存在。

這些缺點意會著，OpenVPN 主要弱點是對缺乏與 IPSec 的

相容性和缺少人們與廠商對它的了解。但這狀況將漸漸會被改變，因為它提供了比其他虛擬私有網路更豐富的應用與解決方案[19]。

OpenVPN 與 IPSec 虛擬私有網路技術的優缺點比較：

表 1. IPSec 與 OpenVPN 優缺點比較表

	IPSec	OpenVPN
優點	標準虛擬私有網路技術。 可裝置於硬體平台。 標準化技術。 許多視窗管理介面。	使用簡單的技術架構。 標準化的網路介面與封包。 支援在使用者權限下運作。 標準化的加密技術。 架構易於設定，採用模組化設計。 簡單易學。 運作時僅需於防火牆上開放一個服務埠。 網路位址運作具有快速恢復連線的技術。 採用 SSL/TLS 工業標準加密等級的技術。 支援流量管制。 運作速度快。 相容於防火牆和代理伺服器。 在 NAT 的環境中仍可運作。 漫遊用戶的支援性良好。
缺點	設定過程複雜。 使用時，修改作業系統核心的必要性。 需要管理人員權限，才可運作。 不同的廠商提出的實施方案，彼此間存有不相容的問題。 複雜的配置過程與技術。 學習較困難，跨入門檻高。 必須在防火牆上開放數個服務埠，才可運作。 在動態 IP 的服務中無法順利提供服務。 技術衍生的安全問題。	與標準化的 IPSec 不相容。 只能在電腦平台執行，但支援眾多自。 由軟體作業系統平台。 是項仍然在研發、成長的新技術。 沒有專屬的視窗管理介面。

資料來源：研究者自行歸納整理

第三節 嵌入式系統

李英瑞認為「嵌入式系統」是一種是以應用為中心，軟、硬體可視需求而被改變，適合應用在功能、可靠性、成本、體積及功耗等綜合性嚴格要求的專用電腦系統[5]。王金龍也提到，嵌入式系統與傳統型電腦設備之差異，為配合特定應用的特殊設計、高效率、產品壽命長、穩定的系統、不易被竊取、高安全性和容易操作等優點[1]。故嵌入式系統是一個客製化的高效率系統，且具高彈性可針對需求變化而有所調整。

而在周樹林調查報告中顯示，綜觀 2002 至 2004 年間，自嵌入式系統應用產值遠超過伺服器應用產值，在嵌入式系統的年複合平均成長率高達 123%，成長幅度明顯超越伺服器，顯示出嵌入式系統在未來的發展性是個非常具有潛力的系統[7]。

李俊德探討嵌入式系統開發產品關鍵因素研究中說明，嵌入式系統一般是燒錄在非揮發性記憶體中，避免系統被更改或遭破壞，但隨著時代改變，小型記憶卡的發達，目前些許嵌入式系統是安裝於 Flash Card 中，具有可隨時更新軟體的優點，又可以克服傳統硬碟裝置容易故障的問題[4]。

壹、Embedded 作業系統的架構和類型

Embedded 系統是一個含有微處理器在內的軟硬體整合為一之裝置或設備，其中軟體部分的 Embedded 作業系統是掌管系統功能發揮的靈魂核心，通常燒錄於非揮發性記憶體中，不允許任意更改或任意重新安裝，但如今隨著小型記憶卡的發達，有些嵌入式系統的 OS 是放置於 Flash Card 之中，如工業電腦最近開發的 NAS 網路儲存設備，就是利用 Embedded Linux 系統開發並將 OS 載入 Flash Card 中，利用 Flash Card 取代傳統的硬碟裝置，即可執行開機並完

成所有的伺服作業，其核心小又具有穩定性加上原本 Linux 強大的網路功能，作為網路儲存設備可謂游刃有餘。而 NAS 只是 Embedded Linux 系統應用的一小部份，舉凡各種工業、商業、軍方、一般消費都可以看見 Embedded Linux 系統的應用如表 2 所示[4]：

表 2.Embedded Linux 系統產品應用的範圍[4]

企業、工控、軍事、網路通訊用		消費用
內嵌式電腦	交通號誌	視訊轉換器
嵌入式主機板	入侵偵測防禦	Set Top Box
嵌入式點腦卡	虛擬私有網路設備	PDA
嵌入式單板電腦	電腦交換機	Smart Phor.e
伺服器		電視遊樂器
網路磁碟機		隨身聽
防火牆		網路分享器
路由器		個人伺服器
精簡型電腦		無線基地台

資料來源：應用 Embedded Linux 系統開發產品關鍵因素之研究—以台灣工業電腦產業例

而典型的 Embedded 作業系統的架構如圖 13 所示，包括最底層硬體溝通的驅動程式（Device Drivers）和韌體（Firmware），再來是微核心的部份（Micro Kernel），系統程式庫（System Libraries）以及中界軟體（Middleware），最上層是預載的應用軟體。而有許多 Embedded OS 公司則開發許多好用的開發工具，使得 Embedded 系統變得更為方便測試或分析，以節省開發軟體的時間和提升軟體的品質。

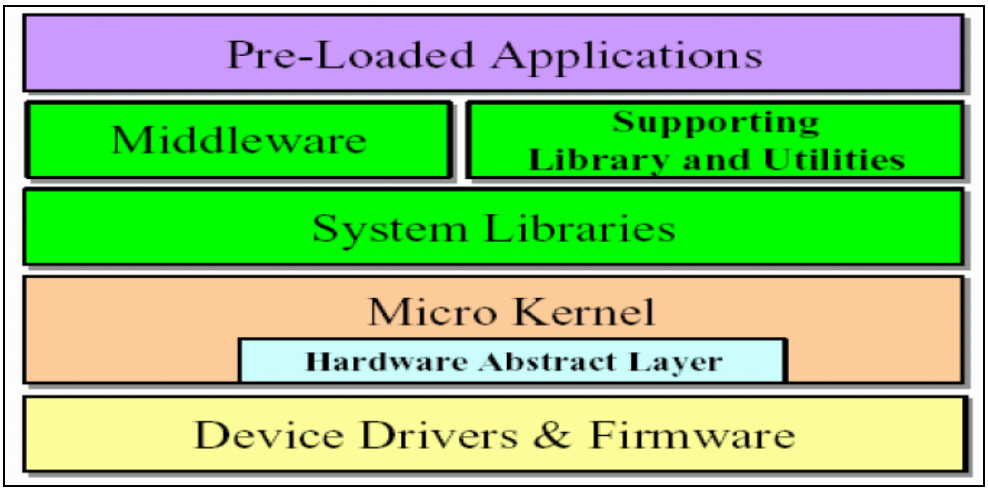

圖 13. Embedded 作業系統架構[36]
資料來源：資策會資訊市場情報中心

Embedded 作業系統又分為即時作業系統（Real Time）和通用作業系統，即時系統是嵌入式系統裡頭非常重要的一環，即時系統常被誤認為是執行速度非常快的系統，事實上不然，所謂即時代表的意義是『即時反應』[35]。一般多人多工作業系統如：Windows、UNIX，系統內部同一時間內僅有一個程式在執行但因為 CPU 執行速度快，所以感覺似乎是同時執行多個程式，無感於城程式為間斷性執行，這是一般所謂的非即時性的作業系統運作模式。即時作業系統乃具有立即反應而且不能讓出資源的特性，這類的應用多半多屬體積小、功能簡單，所以算是種嵌入式系統。QNX 的 QNX OS、Wind River 的 VxWorks 與 Microware 的 OS9、pSOS 等等，都是有名的 Embedded 即時系統公司。這些 Embedded 即時系統的公司也從原來的航太、國防領域將觸角延伸到網路設備、資訊家電等消費性電子產品[4]。

貳、Embedded Linux 系統的特性

在嵌入式系統中 Linux 除了可以應用在伺服器、Cluster 叢集伺服器等，亦適合應用在 Embedded 系統，有以下優點[35]：

一、開放原始碼，模組化設計：

Linux 採用 GPL 授權，除了把原始碼公開以外，任何人都可以自由使用、修改、散佈，而 Linux 核心本身採模組化設計，使用時容易增減功能，藉由這樣的高彈性，可以調校出適合硬體平台的核心。相較於 Linux，Windows 是屬封閉原始碼，故無法得知或修改其核心部份。另外因採用 GPL 授權所以無權利金與保密協定的約束。

二、穩定性高：

Linux 不屬於任何一家公司，但是開發人員卻遍及全世界，每天有無數的人參與改進、除錯及測試，這樣嚴苛的條件造就了穩定度高的 Linux。

三、網路功能強大：

Linux 的架構是參照 UNIX 系統而來，因此承襲了 UNIX 強大的網路功能。

四、跨平台：

Linux 一開始是基於 Intel 386 機器而設計，但是隨著網路的散佈，各式各樣的需求湧現，許多工程師致力於各式平台的移植，造成了 Linux 可以在 x86、MIPS、ARM/Strong-Arm、PowerPC、Motorola 68k、Hitachi SH3/SH4、Transmeta 等平台上運作的盛況。這些平台幾乎涵蓋了所有嵌入式系統所需的 CPU，因此選擇 Linux 可以把更多的硬體平台納入考量的範圍。嵌入式環境不如 x86 PC 那樣單純，所採用的 CPU 架構眾多，使用 Linux 作開發，硬體的選擇性較高。

五、應用軟體眾多：

嵌入式系統所使用的自由軟體具有眾多軟體支援之特色，符合 GPL 開放標準，換句話說，支援軟體如同自由軟體可

免費的使用，這類軟體多半由工程師免費開發，建置時並非以營利為主，因此在無商業公司整合管控下，難免擔保軟體上絕非有 Bug 存在，縱使如此仍有非常多的支援軟體表現傑出。

六、多元化選擇：

企業可自行研發建置所需的嵌入式系統，亦可選擇購買商業版的嵌入式系統，例如著名的 Red hat、Lineo、MontaVista 等。

七、自行開發：

嵌入式系統之程式碼大多屬開放性授權軟體故可自行開發，不僅可成為專屬之系統，且建置成本低。

以上幾點均是嵌入式系統的特性與優點，以技術面來看嵌入式系統的功能具安全性和穩定性，但考量到市場和其它因素時就有所謂的優劣勢分析，劉惠鳳指出採用自由軟體雖然不需支付授權金，但是如果嵌入式系統業者在願意負起某種程度的擔保時，即可收取一定的費用，此種專業服務的提供成為眾家嵌入式系統業者的營利模式之一[14]。其又提到程式開發者的接受度，對於開放原始碼就成為正反兩面的效果，由於開放原始碼程式取得接近零成本，但也因為開放原始碼的原因，使得各家的自由軟體版本以及工具略有不同，相對的程式開發者的程度顯然要高於其它平台（如 Microsoft WinCE），在無統一開發工具下，開發者至少要具備系統核心的知識，才能在不同版本的自由軟體間游刃自如，因此從開發者的調查顯示，採用自由軟體是許多人的選擇，但並不代表廠商最後會選擇嵌入式系統，原因在於對廠商而言授權成本為零，不代表開發成本為零。但嵌入式系統仍以輕薄短小、價格便宜等相當好的競爭立

基。MIC 黃淑琴也表示嵌入式系統承襲了自由軟體的開放原始碼精神與先進的網路支援功能，成為許多嵌入式系統廠商首選的作業系統[36]。許多廠商採用嵌入式系統的主要理由，除了成本考量之外，還有一個很重要的著眼點在於可以運用社群的力量協助開發各式應用，迅速取得各種先進技術，達到 Time to Market 的要求[4]。

第四節 網路竊聽

透過網路所衍生的資訊安全事件，眾多是資訊傳輸時遭受竊取、竄改，封包監聽是網路駭客經常使用了手法，透過該種方式可竊取網路流通中資訊（例如：帳號、密碼），進而完成入侵或竊取資料等動作，使得被害人遭受資產上的損失，遭竊資料可能是個人的金融交易資訊、企業的研發設計圖或客戶名單等，因此網路資訊遭竊所造成的損失往往是讓人始料未及，因此在本節中，將探討網路竊聽使用技巧與區域網路封包傳送方式，以了解企業區域網路架構中隱藏的弱點。

壹、封包擷取

近年透過網路資訊快速的傳送、分享，具有封包監聽的軟體網路比比皆是（例如：Cain、Ethereal、Sniffer 等），網路管理者透過該類工具軟體，可察覺區域網路故障發生之原因，但也因這類型軟體中往往都包含了封包分析工具，使得入侵者易透過軟體取得封包內含資訊，免去封包分析的門檻後網路監聽使用的難度大幅降低，也讓在網路傳遞資訊時增添了不少的危機。

在網路資料中，封包的接收是由網路卡來完成，正常模式下網路卡只會接收下列兩種封包[13]：

一、Ethernet frame 之「目地端硬體位址」與本身 MAC 位址相符的封包。

二、廣播封包。

網路卡尚可以進入另一種模式，稱為「混亂模式（Promiscuous Mode）」，在此模式下網路卡將接收任何通過它的封包；因此，以軟體將網路卡設定為混亂模式，則可以接收所有進入的封包，歸納分析出相關的資訊，此種軟體一般稱為「封包監聽器（Sniffer）」。

Scott M. Ballew 在 Managing IP Network witch Cisco Routers[23] 中提到傳統非交換式的乙太區域網路上，封包是以廣播（Broadcast）的形式在傳送，此種網路拓撲下，任一部電腦只要將網路卡設為混亂模式，就可以監聽到網路上所有傳送的訊息。而交換式乙太區域網路中，資訊設備係以交換器相互連接，交換器內存在一份埠（Port）與介面存取控制位置（Media Access Control Address，MAC）對照表，所有進入交換器內的封包，都會根據 Ethernet frame 之「目地端硬體位址」與對照表比對後，送往指定的埠；在此種網路拓撲下，由於封包並不是以廣播方式傳送，傳統的封包監聽方法將無法作用。

貳、Address Resolution Protocol 運作流程

依據 TCP/IP 協定，當來源端欲送出資料至目地端，在 IP 層處理時，需在資料前加上目地主機 IP 位址後，再往下層送，來源端電腦會檢查本身的 ARP table 中有無目地主機 IP 的 MAC 位址，若有，則將該 IP MAC 位址填入 Ethernet Frame 的「目地端硬體位址」欄位後送出；若否，則以廣播方式發出 ARP Request 封包並接收目地主機所傳回之 ARP Reply 封包，以取得目地主機之 MAC 位址，並將資訊寫入 ARP Table 後，再傳送封包。如果封包目地 IP 位址為不同子網路，則來源端會依上述流程，向路由器（Router）發出 ARP Request，並接收路由器傳回之 ARP Reply 取得路由器之 MAC

位址後，將其填入 Ethernet Frame 之「目地端硬體位址」欄位，然後送出封包（如圖 14）。

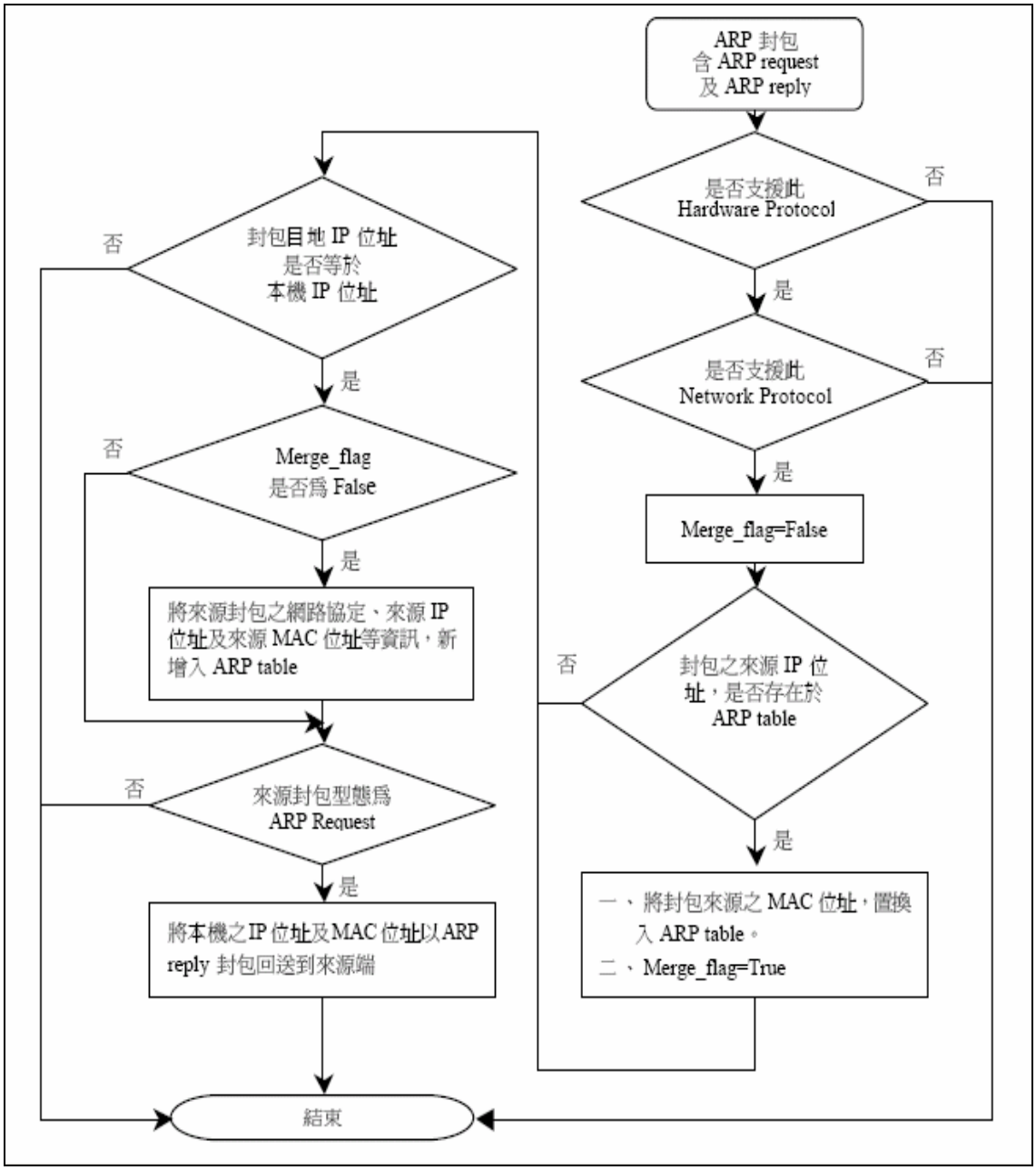

圖 14. ARP 演算法
資料來源：在交換式乙太區域網路中防範封包監聽之研究[13]

參、ARP Table

為了加快位址轉換的處理速度，作業系統會為每張網路卡配置一塊記憶體空間(ARP Cache)，用以存放 ARP Table；一個 ARP Table

包含 index、硬體位址長度、硬體位址、IP 位址及型態等五個欄位；ARP table 內每一筆紀錄稱為一個 entry，每個 ARP entry 具有下列兩種型態（Type）

一、動態（Dynamic）：

動態的 entry，均有存活時間（Life Time）限制，當存活時間到了之後，系統會自動將其刪除[13]。

二、靜態（Static）：

靜態的 entry，無存活時間限制，必需藉助作業系統命令列以 arp -s 指令加入。當本機收到 ARP Reply 或 ARP Request 封包後，會將發送封包者的 IP 與 MAC 位址新增（或修改）填入 ARP Table 內；但實務上，Dynamic 型態的 entries 確是如此，但 Static 型態的 entries 則因作業系統的不同而有不同的作法，並未完全參照 RFC 826 的定義，在劉修仁整理了五種常見的作業系統在收到 ARP 封包時，對於其 ARP table 中之 static entries 是否要置換之作法。可以發現 HP-UX 及 Windows 為「是」，Cisco IOS、Linux、Solaris 則為「否」[13][21]。

肆、ARP 欺騙

電腦在收到 ARP Reply 或 ARP Request 封包時，系統僅檢查 Hardware Protocol 及 Network Protocol 是否與本機相符，就直接去異動 ARP table，並無任何條件的檢查。目前網路上已知的 ARP 欺騙工具軟體，例如 Arpspoof、Arpsniffer 和 Dsniff 等，主要是藉著對某部電腦發送偽造的 ARP Reply 封包，將錯誤的 IP 與 MAC 位址寫入其 ARP Table 中，因而使得其封包轉向，此種方法，一般稱為「ARP 欺騙（ARP spoof）」，透過該方法即可在交換式乙太區域網路中進行監聽到網路上所有傳送的訊息。

經由以上文獻中得知，區域網路中封包藉由 ARP 協定傳輸，但 ARP 傳輸模式中易遭受欺騙，因此網路使用者既使在交換式乙太網路環境中，透過 ARP 欺騙工具軟體亦可輕易的竊聽區域網路所傳遞中資訊，劉修仁提出 ARP 欺騙之防禦方法中，機制防禦時需個別安裝 ARP Defender 區域網路中所有電腦設備，一旦企業規模頗具時，該方案執行上仍遭受相對困難[13]。

第三章 研究設計

本研究設計乃使用防火牆結合虛擬私有網路技術之方法，改善企業內部網路通訊安全，評估 Linux、FreeBSD、Windows 及 Pfsense 四種作業系統與防火牆軟體結合虛擬私有網路技術後的效能表現，並挑選效能表現良好作業系統，進而建置成嵌入式系統，以達高穩定性的系統平台；企業內部網路使用者透過防火牆管制與虛擬私有網路軟體建立加密通道連線，可避免使用者存取資料時洩漏機密，透過該方法可改善區域網路連線缺乏安全性之狀況，同時採用較新 OpenVPN 虛擬私有網路技術，可達降低企業建置成本與減輕網路管理者學習及管理的負擔。

第一節 企業區域網路弱點分析

網際網路技術迅速發展，使得網路應用在企業的範圍越來越普遍，但同時也代表越來越多企業需面對資訊安全的議題，企業內部網路架構中（如圖 15），較被廣泛使用的網路設備為集線器（Hub）與交換式集線器（Switch Hub），兩者具有簡易架設與方便管理等優點，卻因 ARP 之運作特性與 IP 封包格式，讓此種架構下的企業內部網路顯得更加危險。

集線器的運作模式是以廣播方式傳遞封包，此種網路拓撲架構下，任何一台電腦將網路卡設定為混亂模式即可接收區域網路上所有傳送的訊息（如圖 16），然而採用該網路監聽方法，並無進行任何主動式偵測行為，因此竊聽者不易被發現。

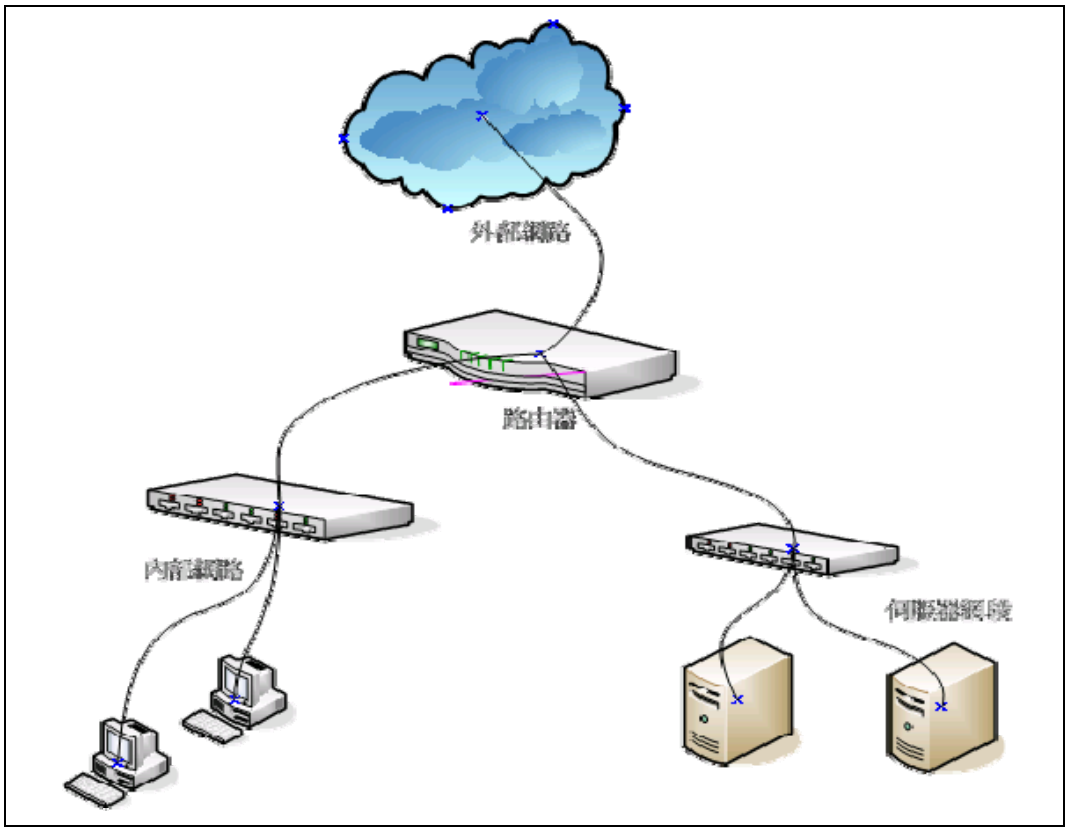

圖 15. 原有企業區域網路架構

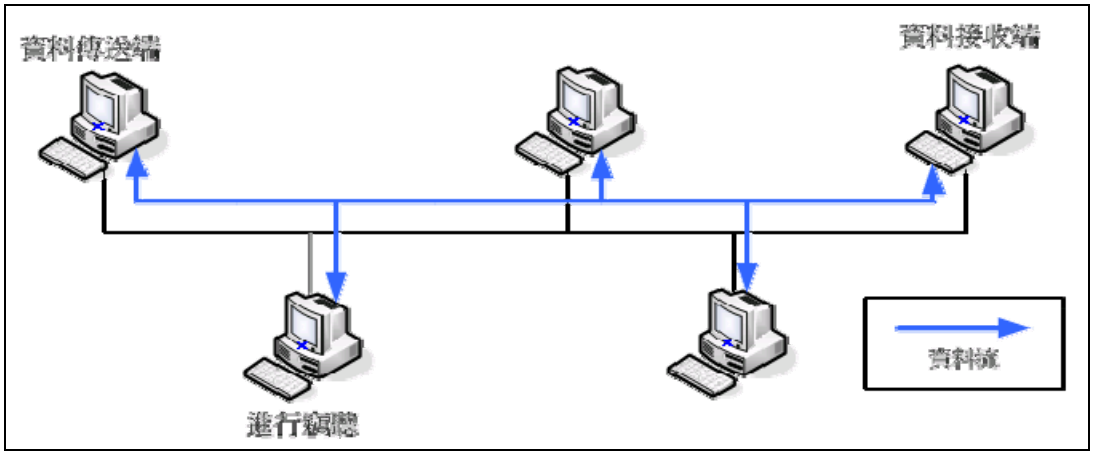

圖 16. 集線器架構下封包竊聽示意圖

電腦透過交換式集線器互相連接，運作時可減少廣播封包的產生，增加網路互相傳遞的速度，這是由於交換器本身中存有一份埠與介面存取控制位置對應表（如圖 17），故當兩台電腦要傳遞資料時，交換器本身亦可得知資料是由哪兩個埠相互傳遞，不需透過廣播封包詢問每一台電腦，也因此大幅改善資料容易遭竊的事件。

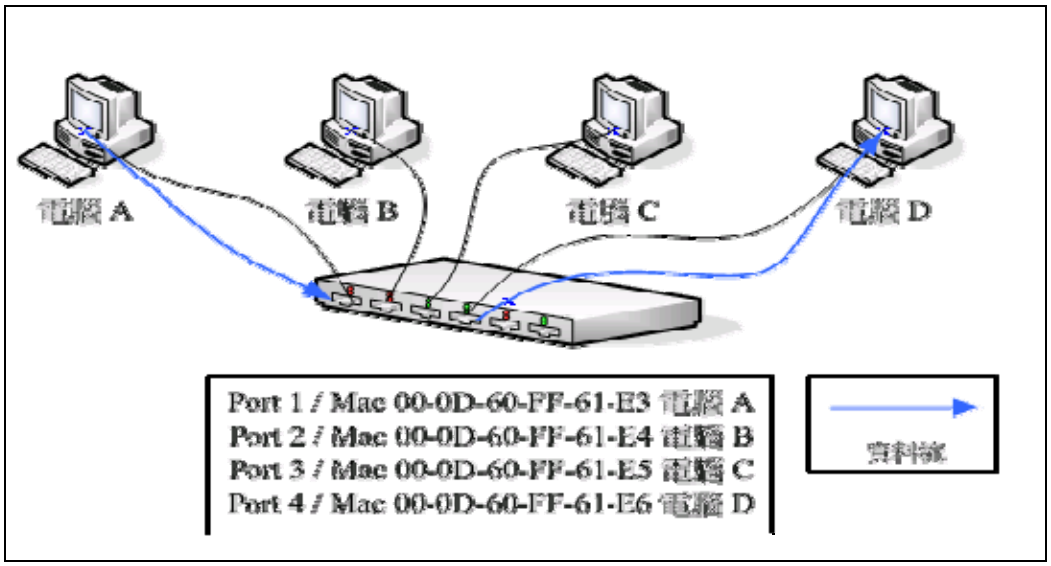

圖 17. 交換式集線器運作模式示意圖

然而在 Arpspoof 工具出現後，交換式即線器所建構之區域網路就不如以往安全，攻擊者可以透過 Arpspoof 軟體對被害者進行 ARP 欺騙，透過這種中間人攻擊法，讓被害人誤認攻擊者的 IP 位置為通訊閘的 IP 位置（如圖 18），使得被害者與伺服器進行連線時自然會通過誤判的通訊閘 IP，因此攻擊者再透過封包監聽軟體，立即可以竊取傳送者的封包資訊，此外攻擊者可以安裝 NAT 軟體讓被害者可持續網路傳輸，使得被害者也不易發現已被竊聽。

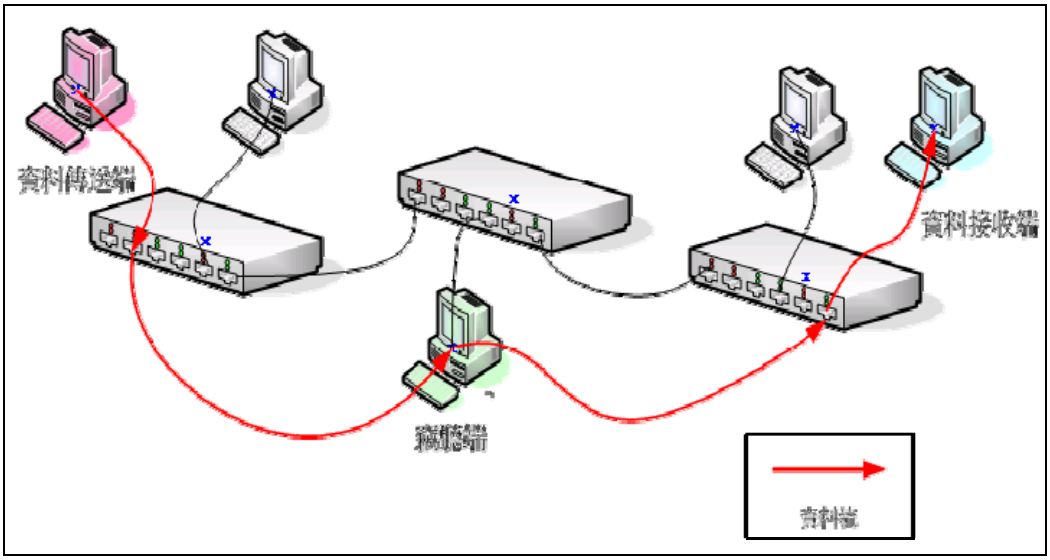

圖 18. ARP 欺騙示意圖

壹、企業內部網路資料竊聽程序分析

一、集線器環境：

（一）、安裝網路竊聽軟體（Cain、Ethereal 等）。

（二）、進行封包監聽。

（三）、分析封包資訊。

二、交換式集線器環境：

（一）、安裝網路竊聽軟體（Cain、Ethereal 等）。

（二）、安裝 NAT（Network Address Translation）軟體。

（三）、進行 Arpspoof。

（四）、進行封包監聽。

（五）、分析封包資訊。

貳、測試設硬體設備

一、一台 LEMEL LM-D16s+ 集線器。

二、一台 SMC 6724AL2 交換式集線器。

三、兩台桌上型多媒體電腦。

在此程序中本研究以集線器與交換式集線器分別模擬不同狀況的內部網路，並以企業前端軟體與 FTP（File Transfer Protocol）連線為例，進行監聽封包。

在集線器的架構下，首先將已經安裝好網路竊聽軟體的網路卡設定成混亂模式（Promiscuous Mode），此模式下網路卡會接收任何通過它的封包；此外另一電腦開啟企業前端軟體並進行登入（如圖 19），當使用者鍵入帳號密碼並送出確認時，資料庫的帳號密碼即被竊取（如圖 20），同樣地其它以明碼傳遞資訊的軟體，在此種狀況下帳號、密碼均會遭竊。

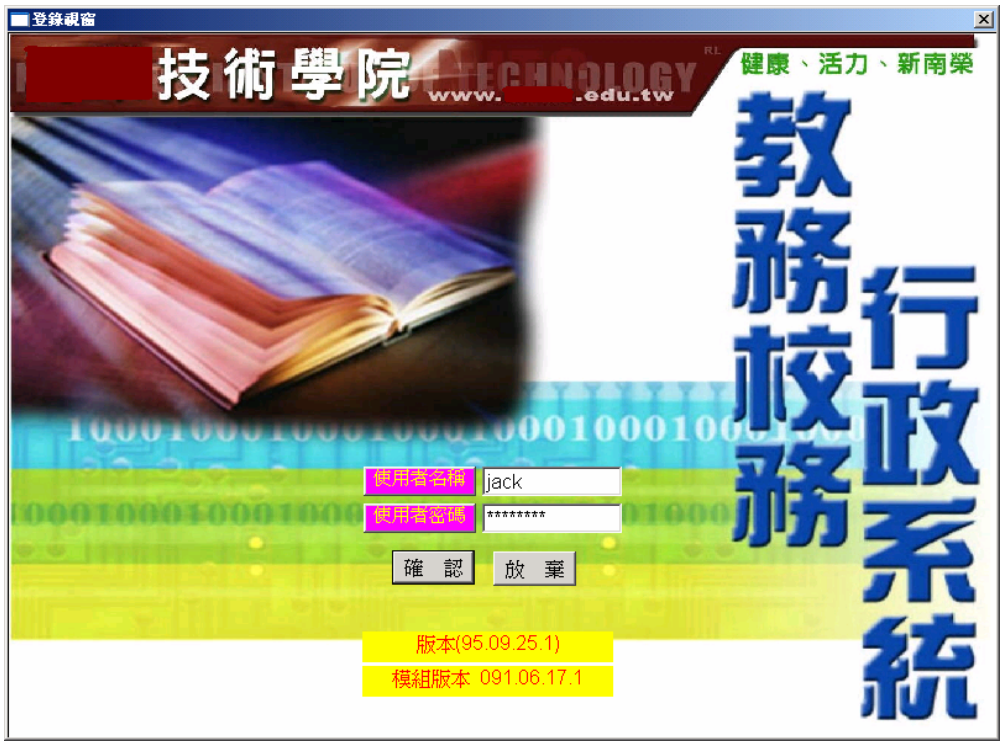

圖 19. 前端軟體登入畫面

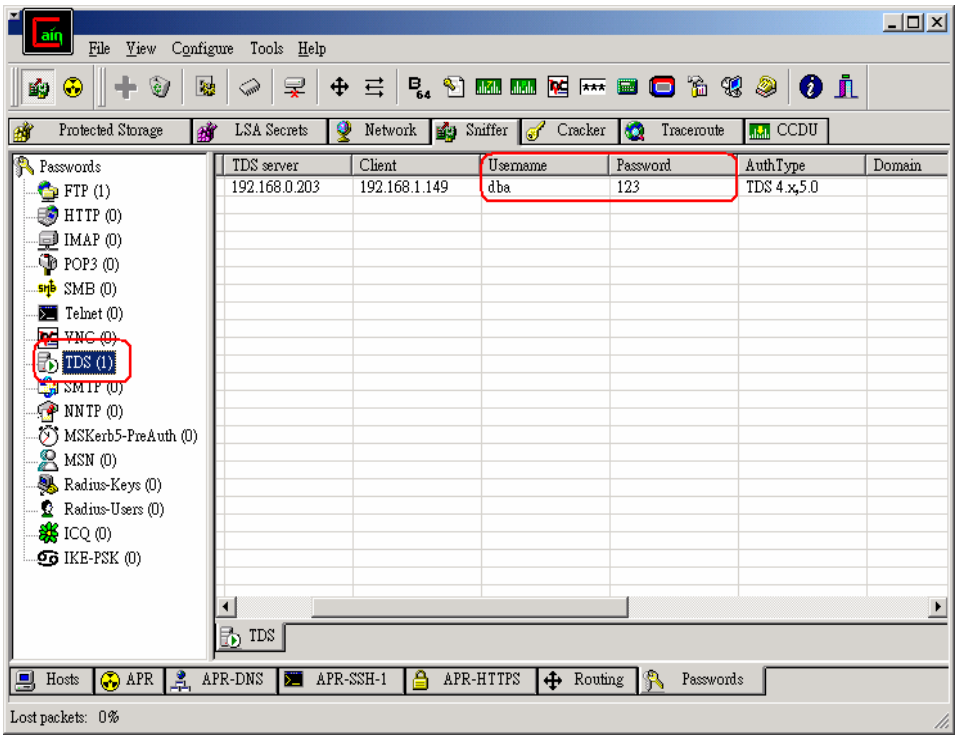

圖 20. 資料庫帳號密碼遭受監聽畫面

在交換式集線器的架構下，差異為需要先透過 Arpspoof 軟體的輔助，在 Windows 作業系統中實際測試 ARP 欺騙，以 Arpspoof 軟體對被害者進行 ARP 廣播，欺騙使用者端通信閘 IP 位置（如圖

21)，讓使用者誤認為竊聽者 IP 位置為通信閘的 IP 位置，當使用者與伺服器連線時，封包則會往攻擊者的電腦傳遞（如圖 22），此時攻擊者再搭配 NAT 軟體的協助，即可讓受害者持續上網不被發現，同時即可達到竊聽資訊之目的。

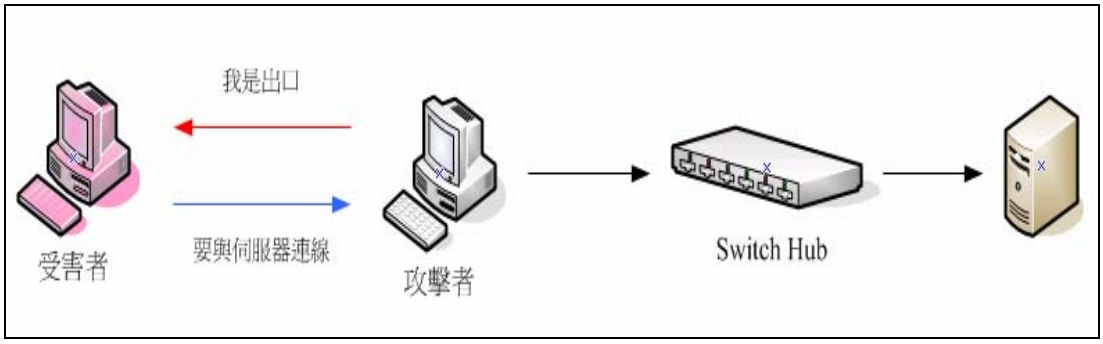

圖 21. 交換式集線器架構下竊聽封包

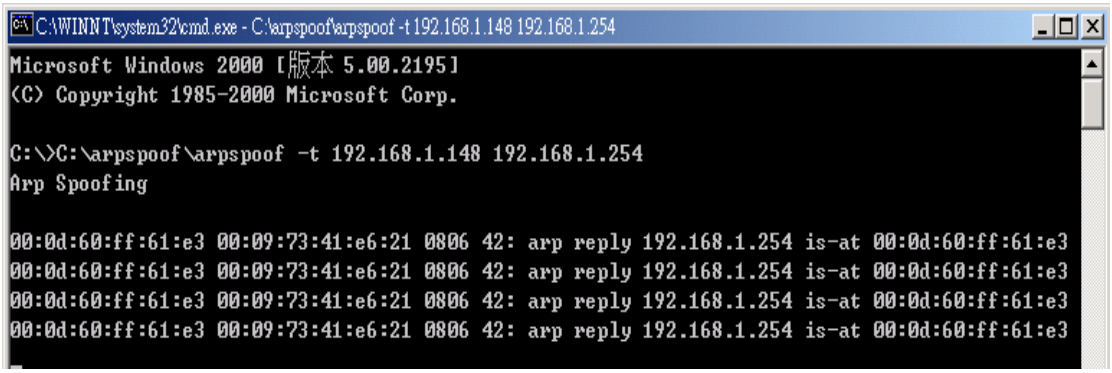

圖 22. Arpspoof 軟體進行欺騙

第二節 防火牆結合虛擬私有網路架構

在本研究架構規劃中，採用防火牆結合虛擬私有網路技術方法（圖 23），主要為改善企業區域網路通訊之安全，並建置高流量的虛擬私有網路平台，以符合區域網路高頻寬傳輸需求，其中虛擬私有網路系統選用跨平台性極佳的 OpenVPN 軟體來進行架設，以符合企業內部類型繁多之作業系統可行性，並與目前廣泛使用的 IPSec 虛擬私有網路技術進行效能差異性評估。

使用該架構模式優點在於 OpenVPN 相較其它虛擬私有網路技術

運作的擴充彈性較高，加密時除支援多種模式特性外，亦可支援硬體式加密晶片輔助，該虛擬私有網路運作時會產生新的虛擬網路介面卡，然而該介面仍可套用原有作業系統平台防火牆規則之定義原則，進行控管流量進出，透過 TLS 協定溝通下更讓 OpenVPN 安全性大幅提升，易於學習之特性更是不同於 IPSec 虛擬私有網路技術。此外防火牆整合下可達到整體性安全規則控管，減輕網管人員管理的複雜度，達到簡易管控存取權限的優點。通訊傳輸上支援完整的 OSI Layer 2 與 Layer 3 模式，因此亦可傳遞 IPX、NetBEU 等多類型通訊協定。在彈性路由設定下，可依需求設定使用者連線後的靜態路由與預設路由，以改善 PPTP 與 L2TP 虛擬私有網路連線後無法使用網路資源狀況。此外亦可在多種作業系統平台上運行，支援的有 Linux、Windows、FreeBSD、Mac OS X 及 Solaris 等作業系統平台；在安全性認證上支援兩種模式，可透過憑證、晶片卡認證連線，或採用一組預先設定密碼。加密彈性較高，預設的加密方式有 Blowfish、AES 與 Triple-DES 等方式，金鑰的大小可隨著需求而變更設定，傳輸通道上不容易遭受攔截進而解讀資訊。支援壓縮連線模式減少資訊傳輸量，加快傳輸時所需時間，此模式適合使用較小頻寬傳輸。在各方面優點集聚狀況下，以致本研究採用 OpenVPN 建構該通訊安全之軟體。

防火牆的選定則採用各作業系統平台內建之防火牆軟體，以達穩定性及降低建置複雜度等需求，雖本研究採用作業系統平台內建之防火牆軟體均非一致，但各作業系統平台搭配防火牆之效能表現仍為本研究效能評選考量之一。

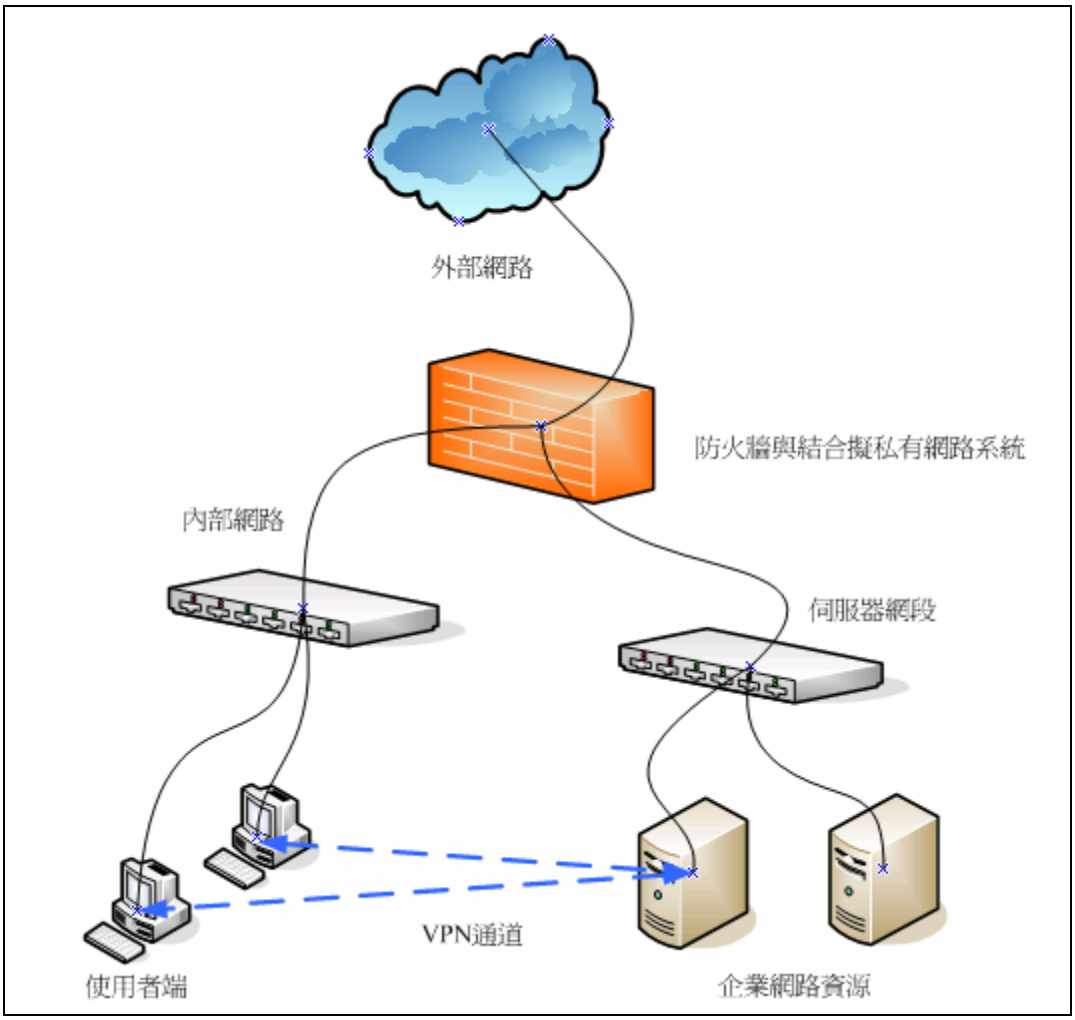

圖 23. 防火牆結合虛擬私有網路架構

第三節 防火牆接合虛擬私有網路系統建置

系統建置以 Linux、FreeBSD、Windows 與 Pfsense 作業系統進行評估，測試各種系統搭配 OpenVPN 的效能與穩定性，在其中挑選出效能表現良好之作業平台，進而建置成嵌入式系統，以尋找出一個既經濟且具備安全的方案，提供給網管人員建置企業虛擬私有網路規劃時之參考，其四種系統規劃如下。

壹、Linux 系統

以 CentOS Server 4.4 搭配 Iptables 防火牆以及 OpenVPN 軟體，建置防火牆結合虛擬私有網路系統，該版本 Linux 具有可媲美穩定

度高之 Red Hat Enterprise Linux，為企業架設 Linux 伺服器的首選[26]。

貳、FreeBSD 系統

以 FreeBSD 6.2 搭配 PF 軟體防火牆以及 OpenVPN 軟體，建置防火牆結合虛擬私有網路系統，FreeBSD 的穩定性高且功能強大，因此許多大型網站都以它為作業平台，其中知名站台就是 YAHOO，於學術網路上亦普遍被應用，且許多大專院校伺服器都是使用它來提供網路服務[30]。

參、Windows 系統

以 Windows2003 R2 搭配 ISA2006 軟體防火牆以及 OpenVPN 軟體，建置防火牆結合虛擬私有網路系統，該系統為最常見的作業系統平台，在伺服器的版本上承襲了簡易視窗操作的特性，是個極易上手的作業系統平台[31]。

肆、嵌入式系統

以 Pfsense1.01 軟體防火牆以及 OpenVPN 軟體，建置防火牆結合虛擬私有網路系統。Pfsense 為一套嵌入式防火牆軟體，內建的功能十分齊全，安裝過程也相當便利，在學術網路中漸漸使用這類系統軟體取代高價的防火牆硬體設備[33]。

伍、硬體規格

在防火牆、伺服器及使用者端均採用相同之硬體設備以確保測試數值之正確性，CPU 等級為 Intel Pentium D 3.0 GHz，記憶體規格為 DDR2 1GB，網路卡規格為 Intel 1000MT，交換器規格為 D-Link DGS3426，其中防火牆平台採用三張網路卡，用以區分伺服器（DMZ）、使用者（Intranet）和網際網路（Internet）等三個網段使用。

在各平台防火牆設定，將企業區域網路劃分為使用者網段與伺服器網段，兩網段連線模式設定成路由模式增加傳輸速度，在測試加密連線時防火牆規則中禁止區網使用者直接對伺服器連線，唯有開放虛擬私有網路 IP 範圍與伺服器連線，該方式可確保所有連線使用者，均與虛擬私有網路進行加密隧道連線以確保數值量測正確性，而透過外部網路存取網際網路資源時，則採用 NAT 模式進行，以模擬企業內部 IP 不足之現況。

虛擬私有網路設定裡，連線時採用 TLS 模式並與憑證方式進行使用者確認及授權，加密分別採用 Blowfish、AES 與 Triple-DES 等方式進行評估比較，配合區域網路高頻寬的傳輸特性，故傳輸時不採用壓縮模式，路由採用靜態路由方式，讓加密連線時仍可存取網際網路資源。

本架構採用交換式集線器均為 1000 Mbps 速度提供服務，以搭配網路卡規格進行傳輸，紀錄傳輸速度時則透過 SNMP 通訊協定與交換式集線器溝通，使用 STG 軟體以每秒記錄傳輸頻寬數值方式，透過集線器設備獲得之頻寬數值，可避免因作業系統軟體差異所呈現數值不正確等狀況。

第四章 系統效能及安全性

本研究利用防火牆結合虛擬私有網路技術，提供企業區域網路資源存取之安全通訊，其中包含了認證、加密及封裝資料方式，以達安全網路環境，然而透過虛擬私有網路存取內部資源時，傳輸速度勢必受到影響，因此針對本研究所建置之架構進行頻寬壓力測試、效能與可靠度分析，以評估使用軟體式防火牆結合虛擬私有網路技術之效能差異及可行性。

第一節 測試指標

系統測試中安全性以封包檢測方式進行驗證，透過監聽軟體（Ethereal）擷取網路傳遞封包，解析封包內容是否包含帳號、密碼等資訊，並分析系統架構改善前後之差異。效能與穩定性測量則以頻寬壓力測試與封包遺失率進行驗證，壓力測試採用大容量檔案經由 FTP 下載測試頻寬，紀錄以交換器介面傳遞頻寬數值為標準，透過該方式可以避免作業系統差異所產生之數值誤差。穩定性測試採用 ICMP 通訊協定，透過虛擬私有網路加密連線後，測試企業內部網路伺服器連線品質，並以回應次數進而計算連通率。

第二節 安全性分析

首先討論有關區域網路資料遭竊的常見原因，再經由實測防火牆結合虛擬私有網路技術整合架構導入後探討其差異。

區域網路傳輸資訊中，構成傳輸安全威脅主要原因，大多為使用明碼傳輸資訊，在此以 FTP 傳輸為例說明，當使用者與 FTP 伺服器完成三向式交握登入過程中將帳號及密碼以明碼方式送出，在集線器所

構成網路環境下，送出的資訊將立即被竊取，而在交換式集線器環境下透過 Arpspoof 軟體進行 MAC 位址欺騙的功能，結果亦是如此。雖有許多常見的通訊協定已支援 SSL 加密方式傳輸，但企業區域網路仍有許多軟體傳輸過程依然採用明碼方式，該類軟體以 Client-Server 架構中前端軟體連接資料庫時所傳遞的資訊居多。

以 Ethereal 軟體模擬監聽企業區域網路封包時，發現使用者前端軟體連接資料庫的封包裡包含了 Login Packet 形態的訊息，其中就以明碼方式記錄著封包傳輸時的帳號、密碼等資訊（如圖 24）。

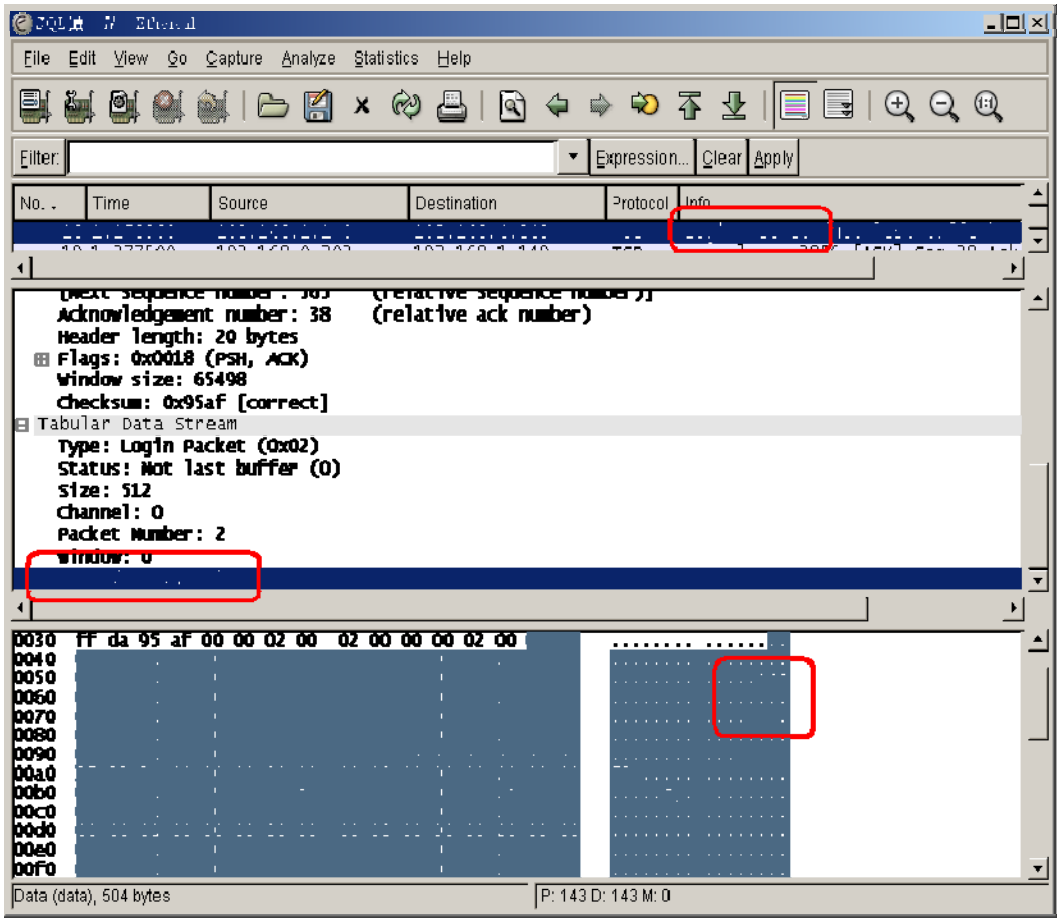

圖 24. 使用 Ethereal 軟體監聽封包

緊接著分析使用防火牆結合虛擬私有網路技術後的架構傳輸資料情形，是否可以改善企業區域網路通訊之安全性，進行實測時使用者端與防火牆先行建立虛擬私有網路加密隧道連線，再進行前端軟體登入步驟，並同樣以監聽軟體進行封包紀錄，然而分析封包資訊中發現

原本的 Login Packet 封包資訊裡面密碼均已加密（如圖 25），雖然該架構下仍無法避免 MAC 位址遭受欺騙攻擊，但可確定即使資訊半途遭受竊聽，在虛擬私有網路加密技術下所傳遞的資訊均呈加密狀態，故可達到資訊安全訴求，因此所採用的加密方式即是該系統安全性的關鍵，如加密時採用安全性不足或已知破解方式的加密方法，傳輸時被擷取的封包仍可能會遭受破解而洩密。

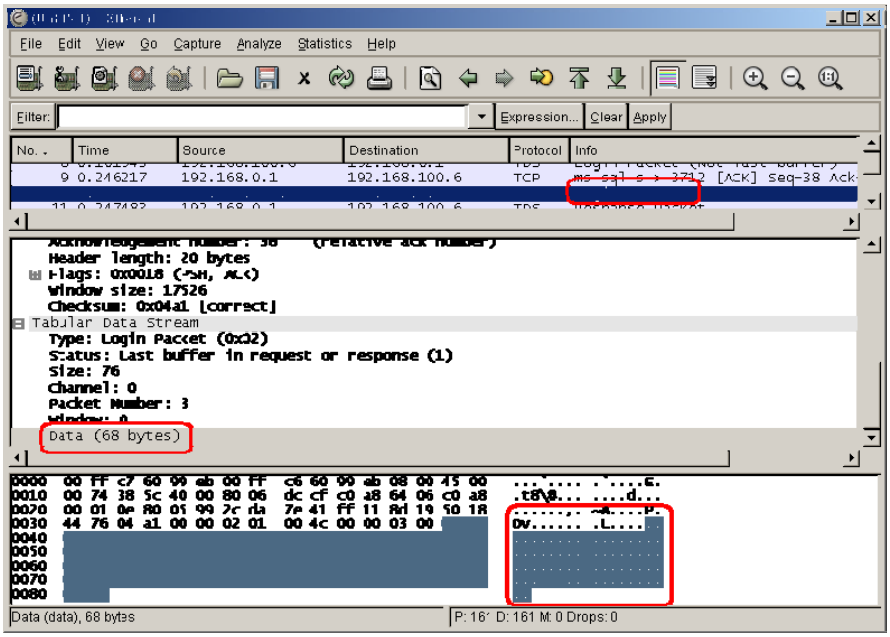

圖 25. 使用虛擬私有網路加密後的封包

第三節　系統效能分析

在討論區域網路封包及虛擬私有網路加密通道傳輸安全後，以實際進行資料傳送方式分析之間差異。一般企業區域網路具有較外部網路頻寬數倍之高特性，因此針對虛擬私有網路連線後測量可承受的最大頻寬，探討該系統架構在不同平台採用各種加密方式的效能表現，以及實行在企業區域網路的可行性。

壹、本研究測試架構概述：

一、頻寬壓力測試

（一）、 在伺服器網段架設 FTP Server，提供使用者端與防

火牆連線並建立虛擬私有網路隧道後進行下載。

（二）、 以約 3GB 的檔案進行下載。

（三）、 於 Windows 平台加以比較 L2PT/IPSec 傳輸速度。

二、加密差異頻寬測試

（一）、 在伺服器網段架設 FTP Server，並以單台使用者與防火牆連線建立虛擬私有網路隧道後進行下載。

（二）、 以約 616MB 檔案進行下載。

（三）、 於 Windows 平台加以比較 L2PT/IPSec 傳輸速度。

三、建置嵌入式系統

挑選出效能表現優異的作業系統平台，進而建置嵌入式系統，以獲得更良好的穩定性。

四、穩定性測試

使用者建立虛擬私有網路連線後，採用每分鐘送出 10 個由小而大的 ICMP ping 封包，針對防火牆 IP 與伺服器網段內伺服器進行連線測試，並以回應數/10*100%等於連通率等方式紀錄繪製 MRTG 圖並且以網頁方式呈現[10]。

五、架構規劃

於伺服器端架設三台 FTP Server 提供下載服務，防火牆結合虛擬私有網路系統（如圖 26），分別以四種不同作業系統平台，個別針對四種不同加密傳輸方式，進行頻寬壓力測試及各種加密後耗損頻寬分析，第（一）項為單純防火牆環境之傳輸，第（二）至（四）項為經過虛擬私有網路加密隧道之傳輸，第（五）項使用 Windows 平台採用 L2TP/IPSec 加密測試。

（一）、 通過防火牆直接連線。

（二）、 採用 Blowfish 加密模式，以 BF-CBC 128bit 加密連線。

（三）、 採用AES加密模式，以AES-128-CBC 128bit加密連線。

（四）、 採用 Triple-DES 加密模式，以 DES-EDE3-CBC 128 bit 加密連線。

（五）、 採用 L2TP/IPSec 加密模式，在 Windows 平台上進行測試。

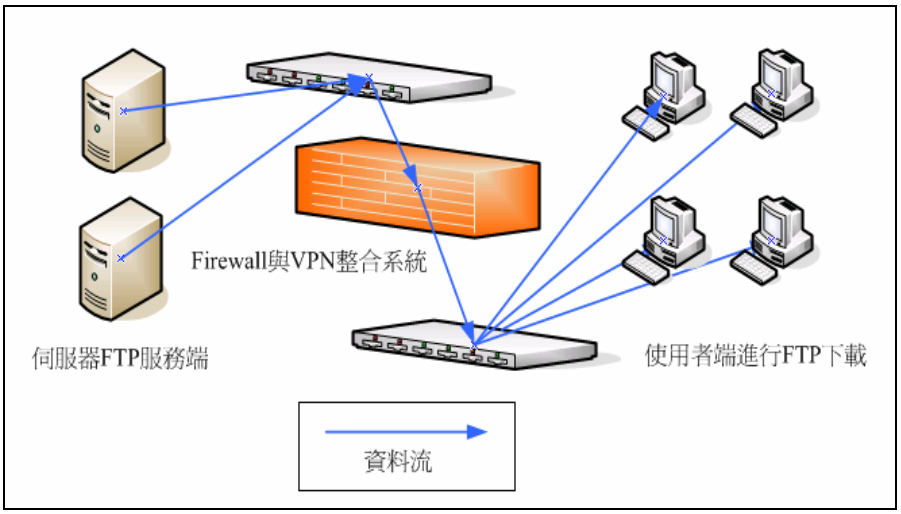

圖 26. 企業區域網路加密通道架構

貳、實際測試

一、頻寬壓力測試結果：

（一）、 未透過虛擬私有網路的架構，最大下載速率 Linux 為 441.9 Mbps，FreeBSD 為 450.2 Mbps，Windows 為 404.5 Mbps，Pfsense 為 440.8 Mbps。

（二）、 採用 BF-CBC 128 bit 加密，最大下載速率 Linux 為 149.3 Mbps，FreeBSD 為 150.9 Mbps，Windows 為 145.7 Mbps，Pfsense 為 130.0 Mbps。

（三）、 採用 AES-128-CBC 128 bit 加密，最大下載速率 Linux 為 139.8Mbps，FreeBSD 為 164.6Mbps，Windows 為 131.9 Mbps，Pfsense 為 117.2 Mbps。

（四）、 採用 DES-EDE3-CBC 128 bit 加密，最大下載速率

Linux 為 90.3 Mbps，FreeBSD 為 92.6 Mbps，Windows 為 83.2 Mbps，Pfsense 為 82.6 Mbps。

（五）、 在 Windows 平台採用 L2TP/IPSec 加密，最大下載速率為 157.9 Mbps。

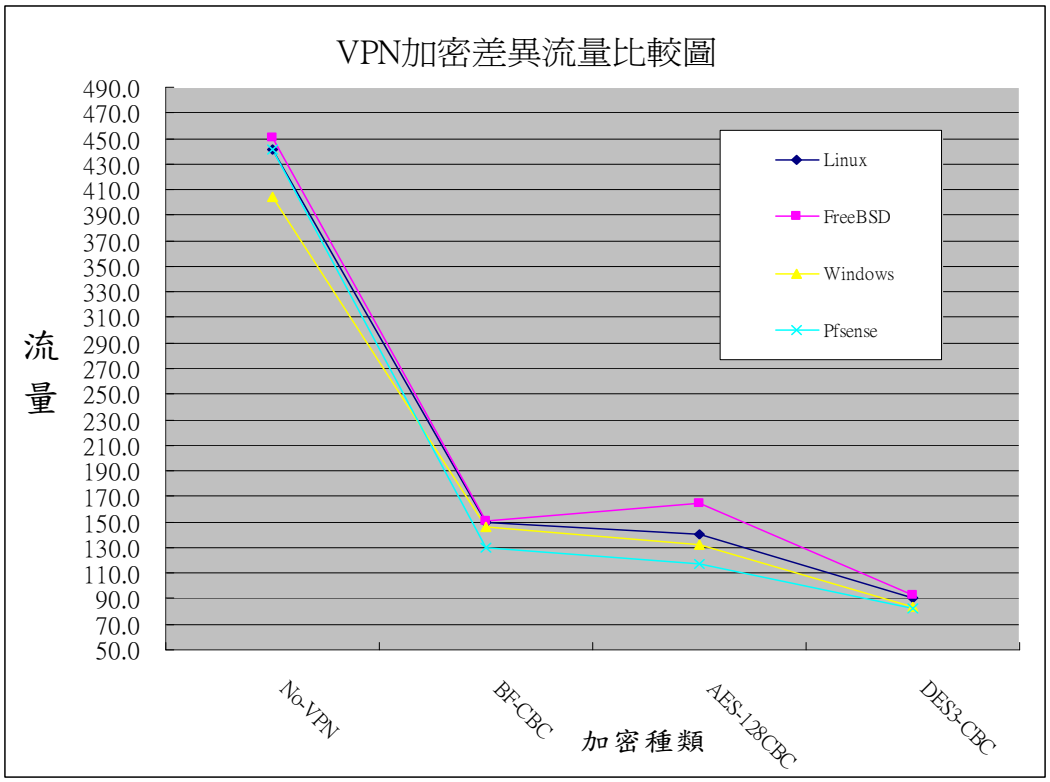

圖 27. 四種系統平台在加密差異之傳輸速率比較圖

二、加密差異頻寬結果：

Linux 所得數據中直接連線為 27.75Mbps，Blowfish 加密為 11.40 Mbps，AES 加密為 11.12 Mbps，Triple-DES 加密為 7.99 Mbps，整體數據如表 3。

表 3. Linux 系統各種加密下載頻寬

次數	直接連線	Blowfish	AES	Triple-DES
1	27.79	11.40	11.20	8.14
2	27.78	11.34	11.15	7.21
3	28.30	11.53	11.13	8.15

表 3. Linux 系統各種加密下載頻寬（續）

次數	直接連線	Blowfish	AES	Triple-DES
4	28.15	11.51	11.27	8.15
5	27.50	11.59	11.01	8.02
6	27.11	11.49	11.00	8.01
7	28.00	11.16	11.26	8.06
8	27.49	11.38	10.95	8.05
9	27.74	11.28	11.12	8.01
10	27.59	11.29	11.08	8.13
平均	27.75	11.40	11.12	7.99

FreeBSD 所得數據裡直接連線為 27.83Mbps，Blowfish 加密為 11.47 Mbps，AES 加密為 11.98 Mbps，Triple-DES 加密為 8.41 Mbps，整體數據如表 4。

表 4. FreeBSD 系統各種加密下載頻寬

次數	直接連線	Blowfish	AES	Triple-DES
1	28.17	11.40	12.09	8.36
2	28.26	11.40	11.88	8.39
3	28.00	11.44	12.07	8.40
4	27.46	11.46	11.84	8.40
5	28.09	11.46	11.85	8.40
6	27.74	11.46	11.92	8.41
7	27.56	11.46	11.98	8.41
8	27.81	11.46	12.16	8.42
9	27.67	11.58	11.75	8.43
10	27.49	11.59	12.27	8.43
平均	27.83	11.47	11.98	8.41

Windows 所得數據中直接連線為 26.54Mbps，Blowfish 加密為 10.09 Mbps，AES 加密為 10.68 Mbps，Triple-DES 加密為 7.78 Mbps，整體數據如表 5。

表 5. Windows 系統各種加密下載頻寬

次數	直接連線	Blowfish	AES	Triple-DES	L2TP/IPSec
1	26.61	10.00	10.89	7.74	8.76
2	26.38	10.53	10.95	7.90	8.83
3	26.11	10.25	10.55	7.91	8.93
4	26.12	9.59	10.63	8.08	8.84
5	27.03	9.78	10.84	7.70	8.60
6	26.75	10.17	10.42	7.70	8.58
7	26.70	10.36	10.31	7.70	8.88
8	26.71	10.15	10.78	7.65	8.89
9	26.59	10.13	10.73	7.71	8.91
10	26.42	9.90	10.70	7.74	8.85
平均	26.54	10.09	10.68	7.78	8.81

Pfsense 所得數據裡直接連線為 26.29Mbps，Blowfish 加密為 10.76 Mbps，AES 加密為 10.16 Mbps，Triple-DES 加密為 7.77 Mbps，整體數據如表 6。

表 6. Pfsense 系統各種加密下載頻寬

次數	直接連線	Blowfish	AES	Triple-DES
1	26.18	10.86	10.23	7.78
2	26.79	10.72	10.13	7.78
3	26.92	10.74	10.12	7.76
4	26.79	10.81	10.08	7.84
5	26.81	10.80	10.15	7.79
6	25.99	10.65	10.17	7.75
7	26.87	10.89	10.24	7.76
8	25.56	10.78	10.06	7.77
9	25.69	10.59	10.11	7.76
10	25.27	10.78	10.27	7.66
平均	26.29	10.76	10.16	7.77

綜合以上數據發現，無論是頻寬壓力測試結果及各種加密後的傳輸速度，均以 FreeBSD 系統效能表現卓越，因此本研究採用 FreeBSD 系統作為嵌入式系統之核心，並進行系統功能精簡化步驟，使該嵌入式系統以防火牆與虛擬私有網路運作功能為主，以達系統高效能與穩定性的表現，最後針對建置後嵌入式系統與原本的 FreeBSD 系統再次進行效能比較，以評估該嵌入式系統的效能優劣。

建置嵌入式系統時，將原本安裝作業系統硬碟設備，置換成耐高溫運作的 IDE Flash Memory，以確保系統運作穩定性，避免系統長時間運作下發生硬碟故障等狀況，安裝 FreeBSD 系統時採用最小安裝模式並修改其核心，剔除無須使用之硬體支援，本系統採用的防火牆與虛擬私有網路技術均著重於 CPU 的能力，因此在挑選類型與等級時，應精確的選擇並刪除非必要的 CPU 支援（如表 7 所示），透過該步驟可以使 CPU 硬體效能完整展現，隨後安裝 OpenVPN 所需相關軟體，進行作業系統精簡化步驟，刪除防火牆與虛擬私有網路運作非必要之系統指令、程式、服務，使得該系統以最小化呈現，並對該系統進行頻寬壓力測試與加密頻寬差異，將該系統命名為 OVPNBSD。

表 7. OVPNBSD 核心參數表

設定參數		備註
machine	i386	系統平台
cpu	I686_CPU	中央處理器等級
ident options options options	OVPNBSD SCHED_ULE PREEMPTION INET	核心名稱

表 7. OVPNBSD 核心參數表（續）

設定參數		備註
device	pci	介面卡支援
options	FFS	基礎檔案系統支援
options	UFS_ACL	
options	MD_ROOT	
options	PROCFS	
options	PSEUDOFS	
options	GEOM_GPT	
options	KBD_INSTALL_CDEV	
options	ADAPTIVE_GIANT	
device	apic	多中央處理器支援
options	SMP	
options	MPTABLE_FORCE_HTT	
options	IPI_PREEMPTION	
device	ata	硬碟機介面
device	atadisk	
options	ATA_STATIC_ID	
device	atkbdc	鍵盤滑鼠支援
device	atkbd	
device	kbdmux	
device	vga	顯示介面支援
device	sc	
device	em	網路卡支援
device	miibus	
device	bge	
device	fxp	
device	rl	
device	agp	顯示卡介面支援
device	loop	虛擬介面支援
device	random	
device	ether	

表 7. OVPNBSD 核心參數表（續）

設定參數		備註
device	apm	進階的電源管理支援
device	sio	序列埠支援
device device device device device device device	ppp tun pty md bpf firewire few	網路連線模式支援
device device device	pf pflog pfsync	防火牆支援

參、OVPNBSD 實際測試：

一、頻寬壓力測試結果：

未透過虛擬私有網路的架構下載速率為 452.3 Mbps，BF-CBC 128 bit 加密下載速率為 156.5 Mbps，AES-128-CBC 128 bit 加密下載速率為 166.2 Mbps，DES-EDE3-CBC 128 bit 加密下載速率為 95.2 Mbps。

二、加密差異頻寬結果：

OVPNBSD 所得數據為：直接連線 29.31Mbps，Blowfish 加密為 11.62 Mbps，AES 加密為 12.34 Mbps，Triple-DES 加密為 8.55 Mbps，整體數據如表 8。

表 8. OVPNBSD 系統各種加密下載頻寬

次數	直接連線	Blowfish	AES	Triple-DES
1	29.63	11.93	12.29	8.38
2	29.50	11.77	12.30	8.42
3	29.39	11.57	12.32	8.46
4	29.32	11.88	12.33	9.46
5	29.27	11.58	12.35	8.44
6	29.18	11.48	12.37	8.42
7	29.15	11.52	12.40	8.49
8	29.01	11.52	12.47	8.47
9	28.90	11.48	12.48	8.42
10	29.72	11.48	12.09	8.50
平均	29.31	11.62	12.34	8.55

綜合所有數據我們可以得知，經修改過後的嵌入式系統在各種加密傳輸效能均有改善，在直接連線方式傳輸改善了 5.05%，BF-CBC 128 bit 加密傳輸改善了 1.29%，AES 加密傳輸改善了 2.92%，Triple-DES 加密傳輸改善了 1.64%，數據及比較圖如表 9 與圖 28 所示。

表 9. 作業系統加密下載頻寬比較表

次數	直接連線	Blowfish	AES	Triple-DES
Linux	27.75	11.40	11.12	7.99
FreeBSD	27.83	11.47	11.98	8.41
Windows	26.54	10.09	10.68	7.78
Pfsense	26.29	10.76	10.16	7.77
OVPNBSD	29.31	11.62	12.34	8.55

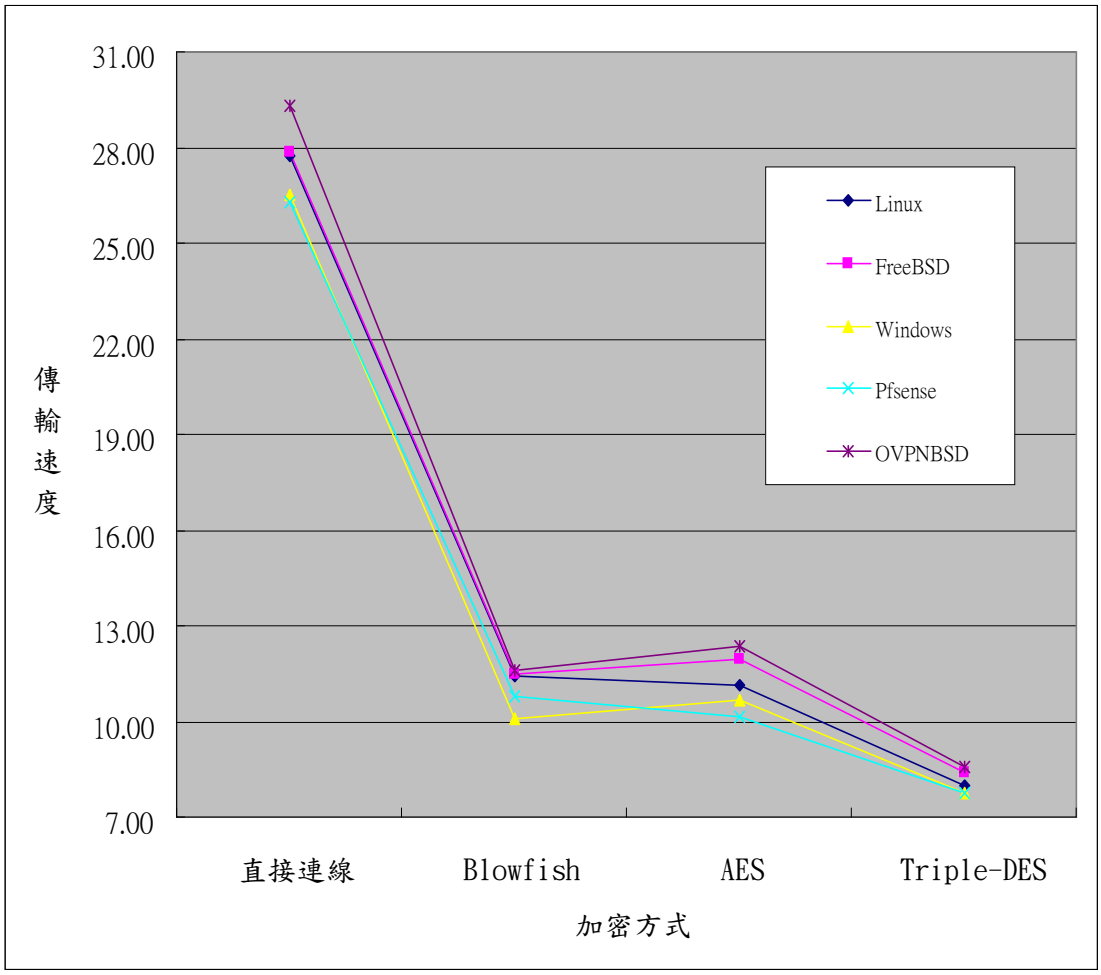

圖 28.作業系統加密下載頻寬比較圖

三、穩定度測試：

由網頁記錄的數值得知（如圖 29、30、31），該系統具有高度的穩定性，以每分鐘進行連線測試，如所繪製出的紀錄圖得知，在每天及每週的記錄圖裡，防火牆的連通率與虛擬私有網路的連通率均為 100%，以高穩定的狀態呈現，並無發生任何封包遺失的狀況。

OVPNBSD連通狀況　更新時間：2007年05月03日02時34分

連通記錄	單位	防火牆IP	連通率(%)	VPN連通測試	連通率(%)
1	OVPNBSD系統	192.168.1.254	100	192.168.0.2	100

圖 29. OVPNBSD 連通測試紀錄

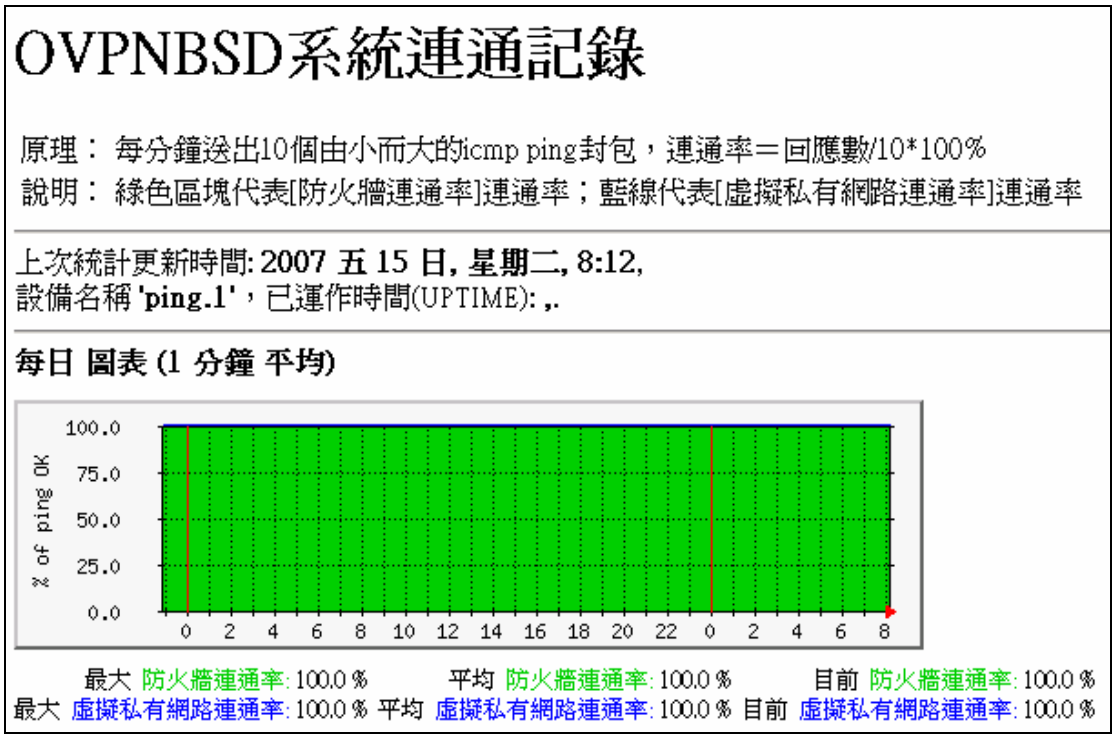

圖 30. OVPNBSD 每日封包遺失測試圖

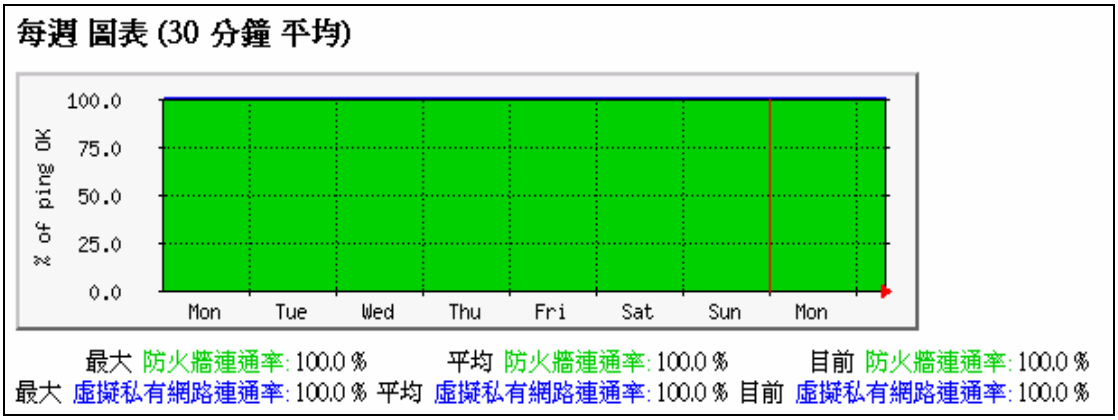

圖 31.OVPNBSD 每週封包遺失測試圖

縱合以上各方面資料，我們可以歸納以下幾點：

一、在頻寬的壓力測試效能表現

OVPNBSD（452.3Mbps） > FreeBSD（450.2 Mbps） > Linux（441.9Mbps） >Pfsense （440.8Mbps） >Windows （404.5 Mbps），各種平台傳輸速度均超過 400Mbps，以目前企業內部網路大都使用 100Mbps 的網路架構，相較之下該頻寬應可滿足企業需求。

二、採用 Blowfish 加密方式時傳輸的速度

OVPNBSD（156.5 Mbps） > FreeBSD（150.9 Mbps） > Linux（149.3 Mbps） > Windows（145.7 Mbps） > Pfsense（130.0 Mbps）排列，傳輸速度分別耗損 OVPNBSD 65%，FreeBSD 66%，Linux 66%，Windows 64%，Pfsense 71%。

三、採用 AES 加密方式時傳輸的速度

OVPNBSD（166.2Mbps） > FreeBSD（164.6 Mbps） > Linux（139.8Mbps） > Windows（131.9Mbps） > Pfsense（117.2 Mbps）排列，傳輸速度分別耗損 OVPNBSD 63%，FreeBSD 63%，Linux 68%，Windows 67%，Pfsense 73%。

四、採用 Triple-DES 加密方式時傳輸的速度

OVPNBSD（95.2 Mbps） > FreeBSD（92.6Mbps） > Linux（90.3Mbps） > Windows（83.2Mbps） > Pfsense（82.6Mbps）排列傳輸速度分別耗損 OVPNBSD 79%，FreeBSD 79%，Linux 80%，Windows 79%，Pfsense 81%。

五、Wndows 採用 L2TP/IPSec

傳輸速度雖比使用 OpenVPN 架構採用 AES 加密方式快 16.47%，但 CPU 使用負載卻呈現 100%狀態，且當下防火牆規則皆無法進行設定控制作業。

第五章 研究結論與未來發展方向

第一節 結論

本研究以防火牆結合虛擬私有網路技術應用於企業區域網路中之通訊安全，主要考量為資訊傳遞安全性，現有網路環境下所使用通訊協定，並非皆支援 SSL 通訊協定技術，在企業實際應用狀況中，存有許多無法以 SSL 通訊協定技術克服之狀況，而採用本研究所提出之方法，除了可以免去購買硬體式防火牆及虛擬私有網路設備高經濟負擔外，本研究所採用 OpenVPN 軟體除跨平台性極具便利，作業系統平台支援度也十分良好，亦可滿足企業裡多種作業平台的需求，在備援線路的建置上也極為容易，是一套非常適合企業使用的虛擬私有網路軟體。

壹、建置便利性

分析現有 Linux、FreeBSD、Windows、Pfsense 及 OVPNBSD 作業系統平台建置防火牆結合虛擬私有網路系統技術之間差異，其中 Windows Server 建置程序最為方便，透過簡易視窗管理畫面，對於管理者之學習跨入障礙亦最低；Pfsense 系統，保有嵌入式系統易於安裝建製特色，系統裝設過程最為迅速；在不微調系統設定值狀況下，以 FreeBSD 效能表現最為優異，但硬體支援較為嚴苛，並不適合所有設備安裝；Linux 效能呈現雖非突出，但在廣泛驅動程式支援優勢下，適合一般企業建置系統時採用；自製 OVPNBSD 系統，除有嵌入式系統易於部署安裝之特性外，經過修改核心與系統最佳化調整，效能更優於原本 FreeBSD 系統，並具有可快速重新建置與跨硬體設備平台之優點。IPSec 虛擬私有網路建置步驟過於複雜，導致佈署時容易出錯，比

較下 OpenVPN 軟體建置便利性較高。

貳、安全性探討

在加密速度考量下，當 Windows 採用 L2TP/IPSec 架構時，雖然傳輸速度高於OpenVPN架構採用 AES-128-CBC 128 bit加密速度，但CPU負載表現差異大，穩定性表現較差，因此 OpenVPN 優異的表現將會是未來企業建置虛擬私有網路可行的新方案。此外以預設的 Blowfish 傳輸速度較快速，但在安全性與傳輸速度的全面考量下，建議使用加密性較安全的 AES 方式建立連線。

參、系統效能探討

採用 Pfsense 嵌入式系統建置雖為便利，但效率表現不及其它平台，原因為該系統硬體支援廣泛，以致核心負載高、效能表現差；相對之下 OVPNBSD 經過硬體支援校正與系統程式簡化，故效能表現較為優異；其餘平台效能比較排列為 FreeBSD > Linux > Windows。此外 OpenVPN 虛擬私有網路軟體支援負載平衡機制，故在效能擴充上遠比 IPSec 架構具有彈性。

肆、穩定度探討

除便利性外，穩定性仍是企業採用新系統時一個重要指標，在本研究實際測試下，OpenVPN 虛擬私有網路系統具有高度的穩定性，連線測試紀錄顯示，在每分鐘透過 ICMP 通訊協定進行連線測試品質，每日、每週之封包連通率均為 100%，且該軟體具有負載平衡、動態 IP 連線機制，極適合企業建置虛擬私有網路使用。

第二節 未來研究的建議與方向

虛擬私有網路加密通道連線下，雖然可以避免資料遭受竊取判讀，但在合法使用者連線後，並無法檢視封包內容是否具有異樣之行為，當合法使用者端遭受入侵，仍有可能透過虛擬私有網路入侵伺服

器與其它電腦設備。本研究所採用 OVPNBSD 系統，雖具有高效率傳輸，及便於安裝等優點，但在系統操作方面尚欠缺便利性，建議未來研究時可透過網頁控制方法降低設定變更之複雜度；傳輸速度乃取決於採用的加密種類，因此如何採用一個安全性足夠且傳輸資料迅速的加密方法亦是一個重要課題。此外當使用者系統中毒時所衍生大量之網路攻擊行為，勢必將對防火牆與虛擬私有網路系統造成極大的負擔等問題，另外雖然使用嵌入式系統可大幅提升系統效能，但仍不足硬體設備效能表現，如何把 OpenVPN 建置為硬體設備並與防火牆結合，這些都是將來研究的重點。

參　考　文　獻

一、中文部份

[1] 王金龍，嵌入式系統硬體架構與設計，初版，台北市，碁峰資訊股份有限公司，民國九十五年。

[2] 吳松霖，「虛擬私有網路之雙層式動態頻寬配置」，國立中央大學碩士論文，87年6月。

[3] 李昆育，「慎選合適的企業防火牆」，資訊與電腦雜誌，208期，95~96頁，86年11月。

[4] 李俊德，「應用Embedded Linux系統開發產品關鍵因素之研究─以台灣工業電腦產業例」，世新大學管理學院碩士論文，94年6月。

[5] 李英瑞，「嵌入式系統與網際網路之整合與應用」，國立中山大學碩士論文，93年6月。

[6] 李國熙、陳永旺，電子商務與網路安全，初版，台北市，歐萊禮，民國八十八年。

[7] 周樹林，「2003-2004我國自由軟體之硬體應用趨勢分析」，軟體產業通訊，第56期，7~10頁，93年6月。

[8] 夏雲浩，防火牆與網路安全，初版，台北市，台灣培生教育出版股份有限公司，民國九十二年。

[9] 翁木龍，「Linux環境下以AES及SHA-256強化VPN的設計與實現」，高雄第一科技大學碩士論文，91年7月。

[10] 黃文穗、林守仁、及蔡瑜珍，「連線狀況及連通記錄系統之建置與應用」，2002 年台灣網際網路研討會，國立清華大學，台灣，91 年 10 月，1134~1137 頁。

[11] 黃建中，「虛擬私有網路技術於無線網路上之通訊安全應用」，義守大學碩士論文，95 年 7 月。

[12] 葉輝煌，「動態 IP 網路中實行 IPSec VPN Implementing the IPSec VPN in a dynamic IP network」，國立台灣科技大學碩士論文，94 年 7 月。

[13] 劉修仁，「在交換式乙太區域網路中防範封包監聽之研究」，義守大學碩士論文，93 年 6 月。

[14] 劉惠鳳，探索IT新契機-未來3年不可不知的30種新產品&新技術，初版，台北市，大椽股份有限公司，民國91年。

[15] 蔡國棟，「網際網路的守門神：防火牆」，網路生活雜誌，27期，64~66頁，87年4月。

二、西文部份

[16] Charlie Hosner , “OpenVPN and the SSL VPN Revolution”, Information Security Reading Room, SANS Institute, August 2004.

[17] Charlie Scott, Paul Wolfe, and Mike Erwin, Virtual Private Network, Second Edition, O'Reilly, December 1998.

[18] D. Brent Chapman, Elizabeth D. Zwicky, Building Internet Firewalls, First Edition, O'Reilly, November 1995.

[19] Markus Feilner, OPENVPN, First Edition, Packt, April 2006.

[20] Naganand Doraswamy, Dan Harkins, IPSec: the new security standard for the Internet, intranets, ad virtual private networks, Sceond Edition, Prentice Hall, March 2003.

[21] Raul Siles, “Real World ARP Spoofing”, GIAC Certified Incident Handler （GCIH） Practical, SANS Institute, August 2003.

[22] Robert Zalenski, “Firewall Technologies”, IEEE Potencials, Vol. 21, pp. 24~29, 2002.

[23] Scott M. Ballew, Managing Ip Networks with Cisco Routers, First Edition, O'Reilly, October 1997.

[24] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, Internet proposed standard RFC 2401, November 1998.

[25] T. Dierks, C. Allen, The TLS Protocol Versions 1.0, Internet proposed standard RFC 2246, January 1999.

三、網站部份

[26] CENTOS, http://www.centos.org, 2007.

[27] CERT/CC, http://www.cert.org/stats/cert_stats.html, 2006.

[28] Computer Security Institute, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf, 2006.

[29] Eric Cole,「確保傳輸安全」, http://www.isecutech.com.tw/feature/view.asp?fid=684, 2006.

[30] FreeBSD, http://www.FreeBSD.org, 2007.

[31] Micorsoft,「虛擬私人網路」, http://www.microsoft.com/taiwan/technet/prodtechnol/windows2000serv/maintain/reskit/intch09.aspx, 2000.

[32] OpenVPN, http://openvpn.net, 2007.

[33] Pfsense, http://www.pfsense.com, 2007.

[34] 朱澔偉,「VPN 全球市場現況預測」, http://www.itri.org.tw/chi/services/ieknews/2004111709232400000006-0126-0.doc, 2004.

[35] 陳漢儀,「嵌入式系統導覽」, http://www.study-area.org, 2001.

[36] 黃淑琴,「全球嵌入式作業系統發展現況與趨勢」, http://203.66.161.5/document/mic_digi/MIC/Reports/eBusinessSoftware&Services/200310/CDOC20031028001.pdf, 2003.

附　　錄　　一

OpenVPN 伺服器參數設定：

```
#伺服器位置設定
local 192.168.1.254
#提供服務埠
port 1194
#採用 tcp 通訊協定
proto tcp
#使用路由模式
dev tun
#使用憑證方式驗證
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
#連線後配發之虛擬位置網段
server 192.168.100.0 255.255.255.0
#設定使用者端連線紀錄檔
ifconfig-pool-persist ipp.txt
#設定伺服器靜態路由
push "route 192.168.0.0 255.255.255.0"
#設定測試存活連線頻率
keepalive 10 120
#採用 AES 加密模式
cipher AES-128-CBC
#設定連線上限數量
max-clients 100
#設定啟動虛擬私有網路之使用者及群組
```

```
user nobody
group nobody
#重新連線時避免重複執行相同存取設定
persist-key
persist-tun
#設定虛擬私有網路狀態紀錄位置
status openvpn-status.log
#設定記錄檔紀錄事件範圍
verb 0
```

附　　錄　　二

OpenVPN 使用者參數設定：

```
float
#VPN 系統採用通訊 Port
port 1194
#使用路由模式
dev tun
#指定虛擬網路卡介面
dev-node openvpn
#採用 TCP 模式傳輸
proto tcp-client
#虛擬私有網路伺服器位置與通訊埠
remote 192.168.1.254 1194
#設定測試存活連線頻率
ping 10
#重新連線時避免重複執行相同存取設定
persist-tun
persist-key
#採用 TLS 協定通訊
tls-client
#採用憑證方式驗證
ca ca.crt
cert client.crt
key client.key
ns-cert-type server
pull
#採用 AES 加密模式
cipher AES-128-CBC
#設定記錄檔紀錄事件範圍
verb 0
```