行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※

※ 下一代虛擬私有網路核心技術之研究---子計畫三 ※

※ 以無線網路提供下一代 VPN 服務關鍵技術之研究 ※

※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：□個別型計畫　■整合型計畫

計畫編號：NSC　91－2219－E－002－034

執行期間：91 年 8 月 1 日至 92 年 7 月 31 日

計畫主持人：國立台灣大學電信工程研究所　蔡志宏教授

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：國立台灣大學電信工程研究所

中　華　民　國　92　年　12　月　30　日

摘要

本計畫提出一套以私有虛擬網路VPN (Virtual Private Network)爲基礎的解決方案，同時考慮公司內部使用與公司外來訪客的上網需求，且同時滿足兩者網路安全上的不同考量考量。對公司外來訪客，本計畫提供公司內部網路的 VPN 通道使其經認證機制及政策性路由之護送下供其連上 Internet 上網。經由適當的系統設定與網路規劃，我們的 VPN (Virtual Private Network)技術可解決外來的訪客上網需求，並且也能同時保護公司內部網路的安全與服務品質。

Abstract

In this project, we propose an VPN-based solution to satisfy the network service demands and security requirements from both internal users and external visitors, within a corporate environment. For external visitors, we first establish an authentication mechanism. Then through a VPN tunnel and related policy based routing mechanism, we escort the visitors' traffic to the external gateway of the Internet. Via proper network configuration, our VPN solution can provide for the external user network access, while protecting the security and quality of service of the internal users.

一． 前言

近年來由於對於網路安全的重視以及成本上之考慮，使 VPN 的應用愈來愈普遍。VPN 在一般企業上是應用在 Internet 的兩端，如兩家不同的分公司需要作資料傳輸時，先由 VPN gateway 將資料加密後，再經由 ISP 所提供的網路服務透過 Internet，傳到另一家分公司，由於資料經過加密，所以 Internet 上的其他人並無法取得該資料，換言之，就是在 Internet 上以特殊的形式建立一條類似專屬的通道(tunnel)，就像是私人網路一樣；但是在本計畫中將在 VPN IPSec 的 tunnel 技術做另一方面的應用的運用。

對於經常外出到客戶公司做商務洽談的業務或工程師，在客戶的公司裡連上 Internet 是常見的需求。但是常常因爲安全上的要求，而被迫只能透過自已手機來上網或者要到有網路連線的地方上網，一方面不方便而且速度慢也不經濟。對這樣的情形，我們希望能利用 VPN 的 IPSec [1] tunnel 技術，將外來訪問的資料封包以 AH [2]或 ESP [3]作封裝，並 tunnel 到公司的 Firewall 外，以分開外來使用者以及公司內部網路的資料，達到同時保護公司網路的安全以及使外來使用者上網之目的。

接下來在第二節的部份，會簡介我們將如何利用 VPN 之 IPSec 技術來實現整個系統以達成我們的目標，在第三節裡，會列出實驗的系統所使之設備以及實驗架構圖，然後，在第四節中，將列出實作步驟及結果，最後的部份則是結論及未來需要再改進的地方。

二． 實作系統簡介

首先，先定義實作之系統主要目的：希望能利用 VPN，將外來的訪客上網的封包作加密並加以包裝，然後直接送到公司的防火牆外之 Internet，以保護內部網路，同時也保護外來的訪客。

接著，我們將外來使用者規劃爲使用 Wireless LAN (IEEE 802.11b/a/g)上網，並希望使用者能經由以下之流程上網：首先，使用者先設定好 Wireless LAN 之設定，並將網路設定爲自動取得 IP 位址及自動取得 DNS 伺服器位址，並且不須額外再安裝其他軟體或程式等。

然後，建置之 DHCP Server 會先給予一個暫時性的 IP 位址給使用者，由此暫時性的 IP 位址，使用者可以開啓網頁瀏覽器(IE 或 Netscape 等)。接下來進入認證之網頁做登入的動作：輸入使用者名稱及密碼，在確認過身份

後，DHCP Server 將會收回之前所分配之暫時的 IP 位址，並根據使用者的身份給予新的 IP 位址，而使用者便可使用此新的 IP 位址上網了。

在完成認證之後，因爲外來的使用者的封包必被加密包裝，所以 Layer 3 Switch 必須依所給予之新的 IP 位址將封包做分類以及 policy route，如果是外來之使用者，則將之繞送到 VPN Gateway 做封裝並 tunnel 到 Firewall 外，反之，若是本地的使用者則不需要做封裝，並且可以任意存取內部之網路。

三． 使用設備及實驗架構圖

爲了實現此系統，我們將系統分爲：VLAN 分割、分流、VPN 封裝以及認證（區分內部使用者或是外來訪客）等部份來完成，其架構如圖 1 所示。

在 VLAN 分割和 traffic 分流方面，主要由 River Stone 的 RS8000 L3 Switch [4] 來完成，使用這台 L3 Switch 我們可以切割 IP based 之 VLAN，並 source IP address 之 policy routing。

在 VPN 封裝方面，分別由兩台 Intel Xeon 雙 CPU Desktop PC，搭配 Linux RedHat8.0 之作業系統及 FreeS/WAN 1.99 [5] 之 VPN 軟體來完成。

在認證方面，我們使用了一台華碩的雙CPU Server搭配Linux RedHat8.0來作爲認證之 Server，並在上面啓動 Apache Web Server [6]、MySQL [7]、PHP[8]、DHCP Server [9]、BIND DNS Server [10]、iptables (NAT)[11] 以及 Linux Routing policy [12]，至於爲何使用這些軟體，將在第四節做說明。表 1 和圖 1 分別爲本系統所使用之設備及實驗架構圖。

表一 使用設備一覽表

網路端設備	
Layer 3 Switch	◆ RiverStone RS8000
802.11b AP	
VPN Gateway	◆ CPU：Intel Xeon 2GHz *2 ◆ 記憶體：512MB ◆ OS：Linux RedHat 8.0 kernel 2.4.20 ◆ VPN Software：FreeS/WAN IPSec1.99
NAT/DNS/ DHCP/ Web Server	◆ CPU：Intel Xeon 1.8GHz*2 ◆ 記憶體：512MB ◆ NIC：Intel 82554EI Gigabit Ethernet, Intel 82544GC Gigabit Ethernet ◆ OS：Linux RedHat 8.0 kernel 2.4.18 ◆ 其它：Httpd-2.0.45, MySQL-3.23.55, PHP-4.3.1, DHCP-3.0.1rc11, Bind-9.2.2, iptables-1.2.6a
用戶端設備	
Client 端 Notebook	◆ IBM ThinkPad A22e ◆ CPU：Pentium III 850MHz ◆ 記憶體：128MB ◆ NIC：Intel Pro/100 ◆ OS：Windows 2000 Professional

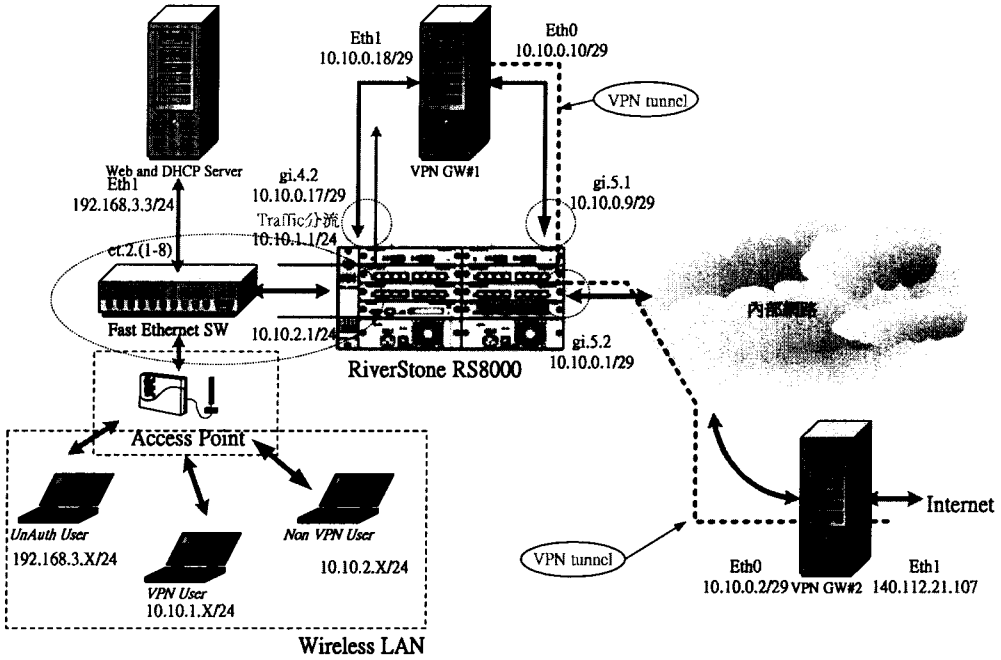

圖 1 實驗架構圖

四、 實作步驟與結果

1. VLAN 分割及 Traffic 政策性分流)

首先，我們先把 Wireless LAN 上的使用者及其 IP Address 分爲 3 類：未認證過之使用者如(192.168.3.X/24)、已認證過之內部使用者如(10.10.1.X/24)和已認證過之外來使用者如(10.10.2.X/24)。其中 10.10.1.X/24 之使用者以 10.10.1.1 作爲 Gateway 上網。同理，10.10.2.X/24 之使用者以 10.10.2.1 作爲 Gateway 上網。

所以，在 RS8000 上我們切割出四個 IP based VLAN (LAN、WAN、VPNLAN 及 VPNWAN)，並設定其對應之 IP address interface (見 RS8000 設定.txt 1~14 行)。

接著設定 Routing policy rules，將所有的 10.10.1.X/24 封包送往 10.10.1.18；所有的 10.10.2.X/24 封包送往 10.10.0.2。我們先定義兩個 Access Control List (acl)，封包來自 10.10.1.X (user-vpn)和 10.10.2.X (user-nonvpn)。然後產生兩個 policy VPNpolicy 和 nonVPNpolicy 並將這兩個 policy apply 到 LANipinterface。

2. VPN 封裝

本研究所使用的 VPN 協定爲 IPSec (Internet Security Protocol)，它是一個由 IETF 所提出並維護的通用架構，提供了身分驗證(authentication)、資料完整性(integrity)、存取控制(access control)，以及通訊保密(confidentiality)等保護措施。

IPSec 提供了兩種加密的模式：傳輸模式(transport mode)及通道模式(tunnel mode)。傳輸模式只對上層的封包做加密，並不對 IP Header 作處理，而通道模式則加密同時包含了資料與 Header。而在計劃中，我們將使用通道模式來建立通道將外來使用者的資料包裝並護送到公司防火牆外。

我們將使用 FreeS/WAN 在 Linux 平台上作爲 VPN 之實作。我們將在 VPN GW#1 和 VPN GW#2 之間建立一條 security tunnel。將內部使用者與外來使用區隔開來。

3. 認証服務

爲了要區分公司內部使用者及外來訪客，並且 VPN gateway 能針對外來訪客進行加密的動作，因此必須要針對不同類型的使用者給予不同 IP 位址的範圍，Layer 3 switch 再根據 IP 位址做分流，決定是否要經由 VPN 加密，以確保公司內部網路的安全，所以在做認證之前，要先在 DHCP server 中宣告 3 個 address pools：

192.168.3.1~192.168.3.100 (認證用的暫時 IP 位址)、10.10.1.2~10.10.1.100 (需要 VPN 加密的外來訪客)、10.10.2.2~10.10.2.100 (公司內部使用者)。

除了以使用者的不同分成 3 個 pools 之外，這 3 個 pools 個別也有一些不同的需求，像認證用的暫時 IP 位址必須要能強制使他連到認證的網頁，而不能直接連上 Internet，爲了實現這個功能，可以在 WLAN AP 後面接一個 DNS server，此 DNS server 會將使用者所輸入的網址全部轉成公司的認證網頁。

另一方面，在分配給使用者可上網的 IP 位址之後，還必須根據 IP 的網域設定不同的 router，這個部分可透過 omapi (Object Management Application Programming Interface) [9]，利用設定 DHCP option 敘述中的 router 參數來完成。除了 DHCP 的設定之外，還必須要將登入的使用者名稱，將所分配到的 IP 位址紀錄下來，這麼做有兩個目的：

1. 知道哪些 IP 位址已經被使用，哪些還沒被使用，就可以用一個 omapi 的程式去分配、回收 IP 位址。
2. 避免有人以同樣的使用者帳號取得多個 IP 位址。

解決的方法就是使用資料庫儲存這些紀錄，並且讓 Web server 可以有權限去編輯、修改和查詢其中的資料，在我們的這個環境中，要在資料庫中有建立 4 個 table：USER_ID、VPN_IP_ADDR、REG_IP_ADDR 和 USER-LOG。

認證的網頁將依序執行以下的動作：

1. 與資料庫連結
2. 比對存放在 USER_ID 的使用者帳號與密碼，不符合則登出
3. 認證成功後取得使用者的使用權限
4. 根據使用者權限，從 VPN_IP_ADDR 或 REG_IP_ADDR 取得一個沒有使用的 IP 位址
5. 執行 omapi 的程式，將使用者的帳號、MAC 位址，從 4.取得的 IP 位址加到 DHCP server 所需要處理的物件中
6. 以 at (Linux 排程指令)讓 DHCP server 在 IP 位址的租約到期後執行登出的動作
7. 更新 VPN_IP_ADDR 或 REG_IP_ADDR 中這個 IP 位址的使用狀態
8. 將使用者的資料寫入 USER_LOG 中

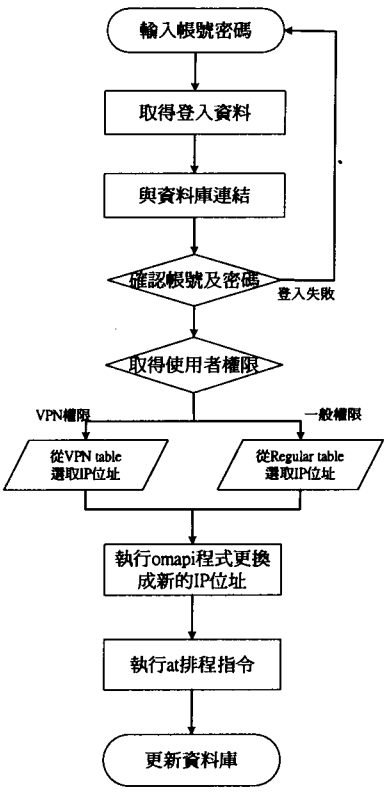

圖 2 登入流程圖

登出同樣需要跟資料庫做連結，與登入不同的是不需要用網頁的模組去控制資料庫，而

是以 C API 與資料庫連結，流程如下：

1. 執行 omapi 程式，將使用者在 DHCP server 處理的物件中刪除
2. 與資料庫連結
3. 更新 VPN_IP_ADDR 或 REG_IP_ADDR 中這個 IP 位址的使用狀態
4. 將使用者的資料從 USER_LOG 中刪除

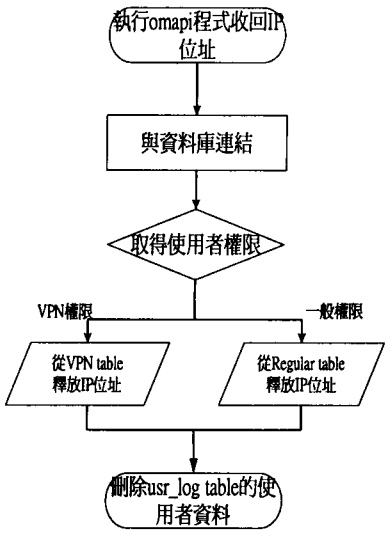

圖 3 登出流程圖

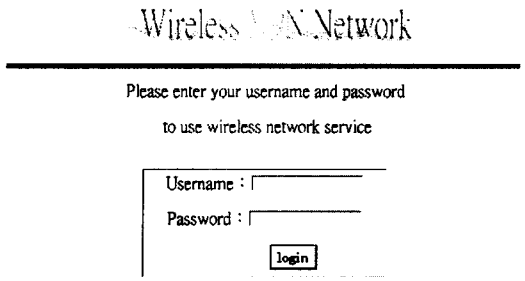

圖 4 網頁認證畫面

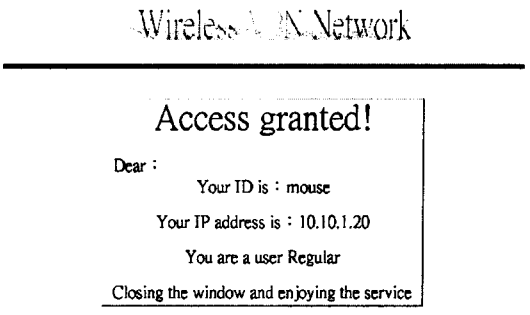

圖 5 登入成功畫面

伍． 結論與未來展望

在這個環境中，我們運用網頁認證的方式，將無線網路使用者分成公司內部使用者和外來訪客兩大類，且分別擁有不同的權限，內部使用者可以任意的存取公司內部網路的資料；外部訪客只能經由 VPN gateway 包裝後以特定的通道連上 Internet，爲了達成這樣的目的，還需要 DHCP Server 根據使用者的權限，分配不同的 IP 位址，再經由 switch 的 routing policy rules 將封包導入 VPN gateway 或公司內部網路，根據此篇的實作步驟，的確可以讓整個架構正常運作，且達成我們要的需求。

在網頁認證方面，這裡所用的帳號密碼是經由網路管理者所建立的，但是以網路使用者而言，並不希望擁有大多不同的帳號密碼，以避免發生忘記密碼的情形，爲了精簡使用者所擁有的帳號密碼，使用者的資料庫可以與其他伺服器的資料庫共用，但是爲了確保在確認身分的過程中，資料不會被第 3 者竊取，必須要有一些安全方面的機制，像是用 hash function 來保護資料，另一方面，由於防火牆已經普遍使用在企業網路中，在防火牆的環境下架設 VPN 也一直都存在一些問題[10]，VPN 和防火牆該如何架設，才能使兩者均正常運作，讓網路環境更加安全，這也是將來需要解決的議題。

五． 參考文獻

[1] http://www.ietf.org/rfc/rfc2401.txt?number=2401 RFC2401 Security Architecture for the Internet Protocol

[2] http://www.ietf.org/rfc/rfc2402.txt?number=2402 RFC2402 IP Authentication Header (AH)

[3] http://www.ietf.org/rfc/rfc2406.txt?number=2406 RFC2406 IP Encapsulating Security Payload (ESP)

[4] http://www.riverstonenet.com/products/router_rs8000.shtml River Stone RS8000 產生

訊息

[5] http://www.freeswan.org/index.html Linux FreeS/WAN

[6] http://httpd.apache.org/ Apache HTTP Server Project

[7] http://linux.tnc.edu.tw/techdoc/banic/down.html PHP4 手冊

[8] http://www.isc.org/products/DHCP/ ISC Dynamic Host Configuration Protocol (DHCP)

[9] http://menter.rightstuff.co.jp/~yasu/DHCP/ ISC-DHCP

[10] System and Computers in Japan , Vol. 31, No. 14, 2000 . Translated from Denshi Joho Tsushin Gakkai Ronbunshi , Vol. J82-D-I, No.6 June 1999, pp. 772-778 , Makoto Kayashima, Masato Terada, Tatsuya Fujiyama, and Minoru Koizumi, VPN Construction Method for Multiple Firewall Environment

[11] http://www.linux.org.tw/ Taiwan Linux User Group

[12] http://www.linux.org.tw/ Mysql Refernce M