# 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(II)—技術面、管理面、與應用面上之研究

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

**計畫編號：**NSC 89-2416-H-009-040
**執行期限：**89 年 8 月 1 日至 90 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。本研究計劃根據上年度所規劃的虛擬私有網路架構為基礎，首先以安全政策管理為出發點，進而提出相關的控管架構，做為系統管理者利用虛擬私有網路的參考。**

**關鍵詞：虛擬私有網路、政策管理**

### 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 the suggested VPN architecture, we will relate VPN management schemes based on security policy management for business to use.

**Keywords**: virtual private network, security policy management

### 二、計畫緣由與目的

**目前在虛擬私有網路、網路安全等相關研究，多半著重於技術面的探討。在上年度的計劃中(89-2416-H-009-013)，我們針對企業組織對資訊安全的需求，探討企業建構虛擬私有網路上技術面的相關課題，然而當企業組織進行電子商務時，除了技術層面的考量外，資訊安全管理上的考量與配合，也是企業組織進行電子商務是否能夠成功的重要因素。**

**本研究計劃的目的，在於提供企業運用虛擬私有網路時，在管理面的參考與建議。首先我們以安全政策管理為出發點，提出以安全政策管理為基礎的虛擬私有網路管理模式，並規劃安全政策管理系統架構；為了滿足企業組織在傳輸品質服務的需求，我們亦提出虛擬私有網路與傳輸品質服務的整合模式；最後我們進一步探討虛擬私有網路在多領域的網路環境下所延伸的系統控管課題，並提出適當的系統控管架構作為解決方案。**

### 三、結果與討論

**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，管理面與應用面相關的議題研究，並**

已獲得顯著的研究成果。針對 Internet 應用日益複雜與安全性考量的條件下，我們深入探討以政策為基礎的管理模式，並將傳輸品質服務的技術與虛擬私有網路技術整合。針對在此種技術整合下所引發的管理課題，我們最後提出一套虛擬私有網路系統的管理架構，作為企業組織與網路系統商在建構虛擬私有網路時的參考。

(一)政策管理與虛擬私有網路的整合

在 Internet Engineering Task Force (IETF)組織所公佈的 RFC2401 文件中清楚地提出了 Security Policy Database (SPD)與 Security Association Database (SAD)之間的運作關係，SPD 的內容是規範 SA 產生之依據，在金匙管理機制建立傳輸所需要的 SA 之前，會先參考到 SPD 中的規範，然後才協商產生出適當的 SA 資料項;不同的 SA 可儲存不同安全機制所要使用的資料，因此當虛擬私有網路系統在管理上有針對不同資料進行不同安全保護的需求時，金匙管理、SPD、SAD 與企業組織營運之間的相互配合，將顯得相當重要。

為了將以政策為基礎的管理模式與虛擬私有網路系統結合，以及加強對 SPD 內部資料的控管，我們需要一個安全政策管理系統，做為管理者與虛擬私有網路系統間溝通的角色，相關系統模組間的相互關係可由圖 1 所示。

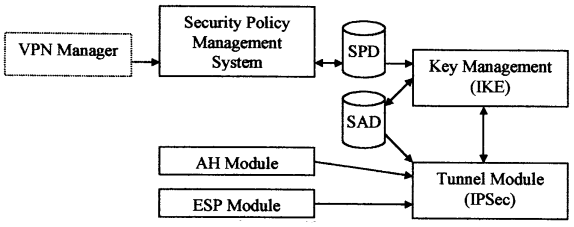



圖 1 結合政策管理之虛擬私有網路系統示意圖

良好的安全政策管理系統，不但要能夠讓管理者建立與儲存安全政策外，還必須解決相關的管理課題，才能讓政策管理發揮良好的功效。茲將相關課題探討於下：

1. 政策的一致性(consistency)：為避免新引入安全政策與系統已存在的政策相互衝突，因此在建立新政策的同時，必須進行對政策一致性的確認工作。
2. 分散式的政策管理：除了使用中央式的政策管理系統外，當網路系統或政策管理系統為分散，政策管理系統必須藉由適當的傳輸協定來溝通系統間的資訊。
3. 與企業內部資訊系統的整合：網路安全需求與企業內部的資訊系統相關，因此政策管理系統應與企業內部相關資訊系統整合，並從中建立對應關係。

根據以上針對虛擬私有網路中的安全政策管理系統之相關探討，安全政策管理系統除了提供政策儲存之用外，還必須確認新政策的一致性；而新政策的發生可能是由網路管理者產生，也可能經由其它政策伺服器取得，或是對應公司相關權限控管系統的設定。我們可依需求歸納出此管理系統內所應包含的元件，以及其相互間的關係，分別探討於下：

1. Policy Engine：用以管理系統中已存在的政策並將新的政策引入系統。其功能包括驗證(verification)新政策的一致性、簡化政策的相關性(decorrelation)、與政策的引入(resolution)。
2. SPD：用以存放政策管理系統的安全政策，以供金匙管理機制參考使用。
3. Inter-server Communication：提供標準的資訊傳輸協定的程序，以進行不同政策管理系統間的訊息溝通。
4. Policy Template：儲存政策規範的樣本，供新政策產生時的參考。
5. Policy Mapper：提供自動的程序將已存在的企業內資訊系統的安全規範，轉換成虛擬私有網路系統的安全政策。
6. User Interface：提供網路管理者建立新政策或對政策系統進行管理的介面。

茲以圖 2 表示出安全政策管理系統內外元件的相互關係，以及其間資料流動的方向：

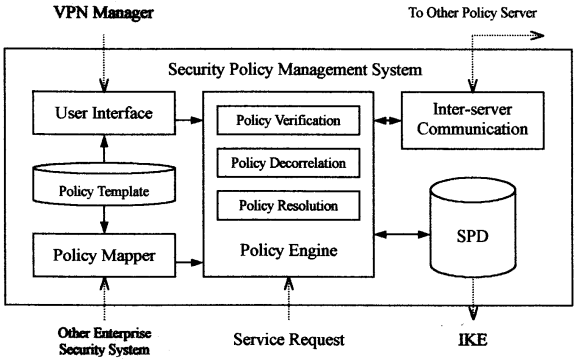



圖 2 安全政策管理系統相關模組示意圖

## (二)虛擬私有網路與傳輸品質服務的整合

傳輸品質服務的技術近年來也引入網際網路的應用，根據相關的研究與考量，我們將 Diff-Serv(differentiated services)機制作為與虛擬私有網路整合的基礎。由於在 Diff-Serv 架構下路由選擇的機制與流量控制機制相互隔離，使得在現行體系下建構此種路由器較為方便，以避免其它機制如 MPLS(multiprotocol level switch)對整個路由方式變更所造成實行上的難題。

Diff-Serv 機制與 IPSec 協定具有多處適於相互搭配運行的特點，下面針對這些相關性的進行討論：

1. 在 IP 層進行 QoS 保證：Diff-Serv 機制與 IPSec 協定同樣於是針對 IP 層進行相關機制的運作，在技術的整合上將較為方便。
2. 以資料傳輸集合為控管單元：IPSec 協定與 Diff-Serv 機制同樣以資料傳輸集合(traffic aggregation)為控管單元，因此我們可對不同集合的封包進行不同安全等級與傳輸品質的服務。
3. 僅需加強邊端節點的功能：在 Diff-Serv 機制與 IPSec 協定中，僅需要加強邊端節點的功能，而中介節點在這兩種協定中，多半保持原來運作機制即可。

除了上面提及的相關性，表 1 針對 IPSec 協定與 Diff-Serv 機制的相關特性進行整理。

表 1：IPSec 與 Diff-Serv 相關特性表

| 網路協定與機制 | IPSec | Diff-Serv |
|---|---|---|
| 核心技術 | Tunneling | PHB |
| 系統控管單元 | SA | DSCP |
| 機制運作層級 | IP 層 | IP 層 |
| 邊端節點功能加強 | 需要 | 需要 |
| 中介節點功能加強 | 不需要 | 僅增加 PHB |
| 不同等級傳輸機制 | 支援 | 支援 |
| 輔助的管理機制 | 金匙管理 | 服務仲介 |

使用 IPSec 協定搭配 Diff-Serv 機制的整合模式，將是在虛擬私有網路進行傳輸品質服務的解決方案；針對在 IPSec 安全通道中的封包，可依需求指派這些封包的 DS 欄位值，以提供傳輸品質服務，藉由不同的通道與 DS 值配對，滿足在安全性與傳輸品質具有不同等級的傳輸需求。

管理不同等級的資料傳輸集合，是虛擬私有網路中重要的系統控管工作。IPSec 協定利用對 SA 的管理，規範並儲存在不同安全等級的通道中所使用的系統參數；而在 Diff-Serv 機制則對 DSCP(DS codepoint)的控管來達成不同的傳輸品質服務。隨著相關技術的發展與多元化的應用需求，SA 與 DSCP 逐漸利用相關政策控管機制進行動態建立與管理，而這些系統參數的規範過程，均須在邊端節點完成，其系統架構可規畫如圖 3 所示：

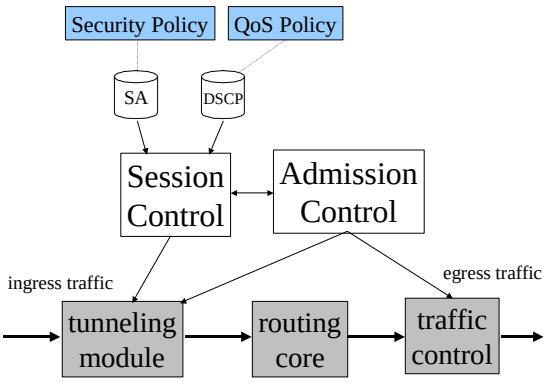
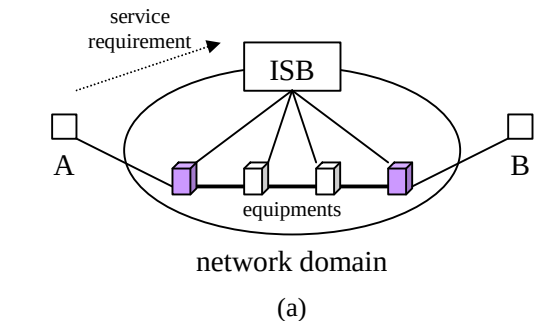



圖 3 IPSec 與 Diff-Serv 整合之邊端節點系統架構

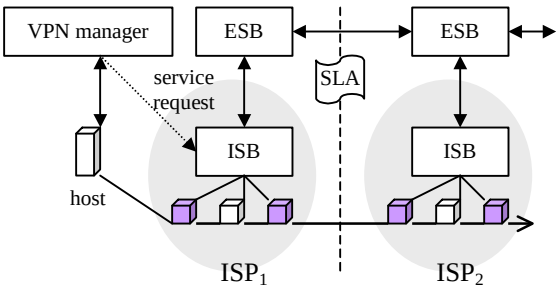
(三)虛擬私有網路的系統管理架構

為了針對不同的資料流進行不同等級的服務，我們可藉由控管 SA、DSCP 與 SLA (service level agreement)來達成，而動態的控管工作，需要倚靠相關政策的制定與良好的系統控管機制，能依照政策規範提供正確的服務並進行系統內的設備控管。

我們使用服務仲介者(service broker)做為系統控管的重心；服務仲介者接受傳輸服務需求，驗證系統是否有足夠的資源提供此服務，必要時進行對系統設備的控管。服務仲介者可分為兩級：1)內部服務仲介者(internal service broker, ISB)負責控管在單一領域內所提供的服務，並能夠依服務需求對設備進行控管；2)外部服務仲介者(external service broker, ESB)在遇到跨領域的服務需求時，進行與其他領域的協商工作。如圖 4(a)所示使用 ISB 進行服務與系統控管；當傳輸需求發生時，ISB 根據領域內的系統狀態提供傳輸服務，並對領域內的設備進行控管，像是依照政策指派適當的 SA 與 DSCP 供邊端節點使用，或對中介節點進行 PHB 的參數設定等。




(a)




(b)

圖 4 虛擬私有網路的服務控管機制

對於進行多領域環境下的服務，使用者的服務需求在送至本地端的 ISB 之後，必須再送往該領域 ESB 做為與其他領域 ESB 的協商基礎，分屬不同領域的 ESB 參照服務需求與跨領域的服務政策，取得不同領域間的 SLA 協議。ESB 並不具備對設備的控管能力，相關的設備控管工作只要指示相對應的 ISB 去達成即可。

企業組織使用虛擬私有網路時，通道建置的服務需求可透過服務管理中心來提出，此管理中心可依照企業組織對電腦設備位置、使用者或應用程式的資訊安全與傳輸品質政策，在通道建置時對網路服務提供者提出適當的服務需求。利用這些動態的管理機制相互配合，企業組織在使用虛擬私有網路時將更便利，而且無論在資訊安全或傳輸品質的控管，都將更具保障，其系統運作架構如圖 4(b)所示。

## 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，本研究針對虛擬私有網路的管理面與應用面提出具建設性的課題與解決方案；如同本計畫初期的規劃，我們以安全政策管理為基礎，歸納出適當的政策管理系統與運作模式，並依據企業的應用需求，將傳輸品質服務機制與虛擬私有網路技術整合，提出整體性的系統控管架構。本研究的成果對於虛擬私有網路技術或管理運作模式的發展上，提供可行的方針與參考。

## 五、參考文獻

[1] 羅濟群, 莊秉文, "針對虛擬私有網路進行傳輸品質服務之整合模式與系統管理架構", *第六屆資訊管理研究暨實務研討會*, 2000

[2] 羅濟群, 莊秉文, "以政策管理為基礎之虛擬私有網路系統架構", *第七屆海峽兩岸資訊管理發展策略研討會*, 2001