結合政策管理與職務角色控管機制之虛擬私有網路系統架構

羅濟群、莊秉文、邱士哲
交通大學資訊管理研究所

摘要

虛擬私有網路（virtual private network, VPN）的技術核心在於建立資料傳輸通道並利用資料驗證及加密技術在公眾網路做私密性的資料傳輸。藉著虛擬私有網路的應用，企業組織位於不同地理位置的分公司間或與企業夥伴之間，可透過公眾網路進行資料通訊，其有效性與私密性的保障就如同使用數據專線之企業內部網路（intranet）一般。

過去虛擬私有網路技術的發展，多半專注在封包傳送、資料驗證及加密等機制；然而近年來，虛擬私有網路的管理課題也逐漸受到重視。基於企業組織對於虛擬私有網路的安全需求，本研究以虛擬私有網路技術面為出發點，探討在 Internet Protocol Security（IPSec）協定為基礎的虛擬私有網路架構下，安全政策在虛擬私有網路系統中的運作與管理模式，並提出以政策管理為基礎的虛擬私有網路整合架構，提供企業組織兼具彈性，又簡化管理複雜性的網路安全管理系統。

為了結合虛擬私有網路系統與企業組織內部的安全控管機制，我們進一步探討企業組織職務角色與虛擬私有網路安全政策之整合控管模式，將原本互相獨立的管理工作，以分散管理但整合應用的精神，使職務角色、政策管理與虛擬私有網路技術相互整合，成為一自動化之安全政策產生機制，進而簡化繁複的控管工作。最後，我們根據本研究所提出的系統架構進行案例與系統可行性分析，以驗證其有效性。

關鍵字：虛擬私有網路、網路安全、政策管理

A Policy-based Virtual Private Network Using the Role-based Security Mechanism

Chi-Chun Lo, Bin-Wen Chuang, Shih-Che Chiu
Institute of Information Management, National Chiao-Tung University

Abstract

The virtual private network (VPN) provides confidentiality and privacy of data transmission by tunneling, data encryption, and data authentication. By using the VPN, an enterprise is able to share information or transmit data securely between its affiliates and business partners. The effectiveness and privacy of VPN are the same as those of the intranet in an enterprise.

In the past, the development of VPN is more emphasized on the packet forwarding, data encryption, as well as the data verification. However, the need of management on the virtual private network obtains more attention in recent years. Based on the Internet Protocol Security (IPSec) which is announced by Internet Engineering Task Force (IETF), when the VPN needs to manage multiple levels of transmission security, key management, security policy database, and security association database are very important.

This paper discusses the operation and management models of the IPSec-based VPN. The proposed model provides organizations a flexible and effective network security system on the foundation of policy management. We further integrate the VPN management model with the role-based security mechanism, which may be employed in the enterprise. The entire architecture not only satisfies the requirements of VPN, but also improves the efficiency of virtual private network by automating the management of security policy.

Keywords: virtual private network (VPN), network security, policy management

壹、緒論

網路安全隨著網路應用的普及而漸受重視，虛擬私有網路（virtual private network, VPN）的技術在於利用公眾網路進行私密資料的傳輸，其所要達成的功能，便是讓公眾網路上具有存取企業內部網路權限的主機或使用者，能夠在不同的地理位置進入內部私有網路存取資訊，並排除其他不具權限的使用者盜取或竄改內部網路所流通的資訊[2]。大體上來說，企業組織可在不同位置的內部網路自行架設安全閘道器（security gateway）來建構虛擬私有網路，或利用網路提供者（internet service provider, ISP）所提供的虛擬私有網路服務來達成；基於網路安全的考量，利用企業自行架設的虛擬私有網路建構模式是有效保障資料安全的解決方案[3]，本研究根據該建構模式，提出以網際網路安全協定（IP security, IPSec）為基礎的虛擬私有網路整體架構與運作模式，以滿足企業組織對於虛擬私有網路的安全與管理需求。

過去在虛擬私有網路的發展上，多半專注在通道建置、資料驗證及加密機制等技術性的探討；然而近年來，虛擬私有網路的管理課題也逐漸受到重視。在以 IPSec 協定為基礎的虛擬私有網路技術中，與管理相關的課題包括安全政策的建立、密鑰管理、以及安全關聯（security association, SA）等相關技術的運作模式。在 Internet Engineering Task Force（IETF）組織所公佈的 RFC2401[6]標準文件中，提出了安全政策資料庫（security policy database, SPD）與安全性關聯資料庫（security association database, SAD）之間的運作關係，尤其當虛擬私有網路系統在運作上需要滿足不同的傳輸安全需求時，密鑰管理、SPD、SAD與企業組織間的相互配合，就顯的非常重要。隨著虛擬私有網路應用日益複雜，使用以政策為基礎的管理模式，將是虛擬私有網路技術發展的必然方向。

為了貼近企業組織對於虛擬私有網路的應用需求，並滿足在管理上的需要，本研究深入探討以政策管理為基礎的虛擬私有網路運作模式，並提出建立與管理安全政策的解決方案，同時整合企業內部的職務角色控管機制，將原本互相獨立的管理工作，以分散管理但整合應用的精神，使職務角色、政策管理與虛擬私有網路技術相互整合，成為一自動化之虛擬私有網路系統架構。

本文首先於第貳章探討以 IPSec 協定為基礎的虛擬私有網路相關技術，以及網路的政策管理和職務角色控管機制等；第參章將提出以政策管理為基礎的虛擬私有網路系統架構。第肆章乃是針對此架構中安全政策管理系統與職務角色控管機制的整合模式進行深入探討，並於第伍章進行案例分析以驗證本系統架構與運作模式的有效性。最後於第陸章總結。

貳、文獻探討

本章針對本研究之基本技術做簡略探討，包括 IPSec 協定與虛擬私有網路相關技術、網路的政策管理、以及職務角色控管機制等。

一、虛擬私有網路技術與 IPSec 協定

虛擬私有網路運用並整合了許多資訊安全與網路傳輸的技術與機制，其中最重要的核心技術便是通道建置技術（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，在私有網路內的封包，先依照通道建置協定封裝成新的封包，再送到公眾網路上傳輸。常見的通道建置協定包括 IPSec、PPTP、L2TP 等三種[9]。這些通道建置協定最大的不同在於，IPSec 的技術可提供較為安全的資料傳輸，並讓使用者可以同時連接網際網路與虛擬私有網路；而 PPTP 與 L2TP 僅提供點對點的傳輸，所以只能在網際網路或虛擬私有網路的兩種功能中擇一使用。

由於 IPSec 本身已整合封包驗證、資料加密、與相關的密鑰管理機制，這使得以 IPSec 協定為基礎來建構虛擬私有網路，有更具多元化的應用。茲將其相關的虛擬私有網路技術簡述於下：

1. **加密技術**（encryption）：在 IPSec 通道建置技術中的 Encapsulation Security Payload（ESP）機制[8]可透過傳輸雙方的 Security Association（SA）協議，利用系統支援的資料加密技術將訊息封裝加密，以達到訊息的私密性保證。
2. **驗證技術**（authentication）：在 IPSec 通道建置技術中的 Authentication Header（AH）機制[7]已將訊息驗證技術整合，而在相關的密鑰管理協定中，亦納入了設備驗證的機制；企業組織可以依照安全需求與公司的資訊系統配合，將虛擬私有網路技術擴充，以滿足對身份驗證的需求。
3. **密鑰管理機制**（key management）：在 IPSec 協定中，Internet Key Exchange（IKE）協定[4]能藉由安全政策（security policy）的制定，並與 IPSec 協定配合達成協議與交換 SA 的工作，是故成為以 IPSec 為基礎的虛擬私有網路中，密鑰管理的最佳解決方案。

IPSec 通道的建置可能是由通訊的兩端自行將資料加密驗證來達成（transport mode），或在封包進入網際網路前透過安全閘門器將原始封包內容用 IPSec 的封包方式送出（tunnel mode），其運作模式如下圖 1 所示：

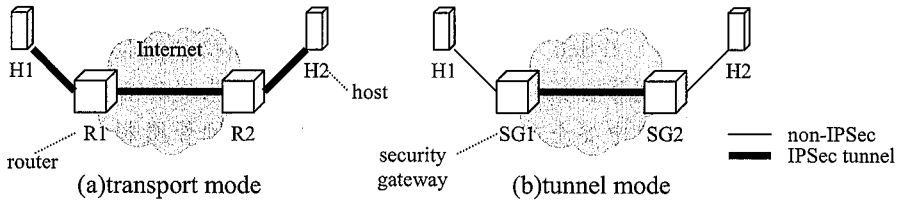

圖 1：虛擬私有網路通道建置示意圖

由以上的探討我們不難歸納出，以 IPSec 協定為基礎來建構虛擬私有網路是較佳的解決方案；IPSec 協定與網際網路有最佳的相容性，其中的 AH 與 ESP 機制提供了最基本的安全需求，藉由與 IKE 等金匙管理協定的配合控管傳輸雙方的 SA 協議，理論上能適用於大多數的虛擬私有網路需求。

二、以政策為基礎的網路管理

現今的網路應用逐漸從對所有服務需求提供最優（best-effort）品質的服務模式，轉換到可預測並提供與各種不同的服務品質之網路服務模式，面對新服務模式所引發的技術與管理課題，以政策性為基礎的網路管理（policy-based network management, PBNM）已成為最新之網路管理概念[14]。新一代網路產品已經逐步利用這種以政策性為基礎的網路管理觀念來設計管理機制，使越趨複雜的網路系統能更容易地進行管理。政策性網路管理可應用的範圍包括服務品質、網路安全、組態設定等，網路管理者建立網路資源與服務使用權限的政策或規則，政策管理系統將對照使用者或應用程式的相關資訊，根據系統中的網路政策，自動對網路設備進行控管，因此網路管理者不需要對個別的設備進行控管，僅需對欲管理的網路系統整體制定出適當的管理政策即可，因此無論對管理工作複雜度的降低或管理的一致性，政策管理模式提供了良好的解決方案。

常見的政策管理系統架構可分為二階與三階兩種模型。所謂的三階模型，乃是由政策執行點（policy enforcement point, PEP），政策決策點（policy decision point, PDP），政策儲存點（policy repository, PR）所構成；而二階模型多半是整合了 PEP 與 PDP，而與 PR 分散的模式。茲將相關的政策管理元件分述於下：

1. **政策控制台**：多半以一個使用者介面為主，用以建構政策、部署政策與監控狀況的政策管理環境。
2. **政策決策點**：依據政策作出設備的管理決策。
3. **政策執行點**：根據 PDP 的決策，執行對設備進行設定或控制的單元。
4. **政策儲存點**：提供儲存政策及其相關資訊的設備或機制。
5. **政策傳輸協定**：負責從政策儲存點讀寫資料及 PDP 與 PEP 間的資料傳輸。

為了方便進行政策管理，我們可將網路設備視為受政策控管的狀態機（state machine）；政策的內容多半是若干評判規則的組合，規則中定義了適用於該規則的條件（condition）與因應的控管行為（action），用以規範若干群體在網路管理需求發生時所對應的管理工作，若是輔以適當的政策管理系統，將使得網路管理的工作更為方便，亦具備較高的有效性與彈性。

三、以角色為基礎的控管機制

以角色為基礎的安全管理正逐漸受到重視，原因在於角色的概念更貼近組織管理的架構，其可依照組織架構與職權延伸，並且具有職務承繼的功能與權限調整的彈性。在以角色為基礎的執行權管制（role-based access control, RBAC）[13]上，透過角色之定義以及權限之賦予，管理者只須專注於組織人員角色之指派，以簡化原本繁複的管理工作。在企業組織中，人員的變動是常態，職務則是制度的一部分，更改的頻率相對而言就要少得多；以角色為基礎的執行權管制機制，有助於落實企業組織制度化的安全控管環境的建立，同時減少因人為疏失或舞弊所造成的資訊安全問題。一般而言，使用職務角色控管機制具有下列幾項優點：

1. **授權管理**：職務角色控管機制將權限授與給角色，而使用者必須取得該角色才具有所賦予的權限，這種作法可簡化安全管理工作。
2. **階層式角色**：基於一般化和特殊化的原則，職務角色多半具備的階層性，並依需要進行權限的繼承；階層式角色更進一步簡化了授權管理。
3. **最小特權**：職務角色控管機制讓使用者得以參與某特定工作所需要的最小特權去簽入系統；如此可減少損壞發生的機會。
4. **授權分工**：職務角色控管機制可透過衝突角色的定義或強化控制，進行權限的分工，以避免使用者取得不當的特權。
5. **使用者分類**：職務角色控管機制依據使用者在組織中所扮演的角色，自動對眾多使用者進行角色分類。

職務角色控管機制是以使用者在系統中所執行的活動做基礎，去調整該使用者的一切行為。以 Sandhu 所提出的 RBAC 為例，對系統資源的存取授權是被指定給角色，使用者則被指定去扮演某一個角色[13]。一般而言，使用者能夠在不同場合裡，扮演不同的角色，相同的角色可能被許多人同時扮演，有些機制甚至允許使用者在相同的時間同時扮演多重角色。

參、以政策管理為基礎之虛擬私有網路架構

根據 RFC2401 標準文件的規範，虛擬私有網路的政策管理可透過 SPD 與 SAD 之間的相互運作來達成[6]。SPD 用於儲存安全政策以規範所有進出資料的傳輸行為，及所要使用的安全機制或演算法；此外，SPD 的內容可供密鑰管理機制參考使用，以作為 SA 協商之依據。不同的 SA 資料項可儲存不同安全機制所要使用的資訊與密鑰，因此密鑰管理、SPD、SAD 之間的相互配合，將顯得相當重要。圖 2 顯示使用 IPSec 協定傳輸時相關模組的示意圖，當應用程式發出傳輸需求，位於主機中的 IPSec 模組參考對應的安全政策決定其傳輸行為，並透過 IKE 模組動態協商出傳輸所需要的 SA，同時儲存於 SAD 中；此處的安全政策乃是透過政策代理程序取得，而政策的儲存可能使用目錄服務或分散式資料庫。

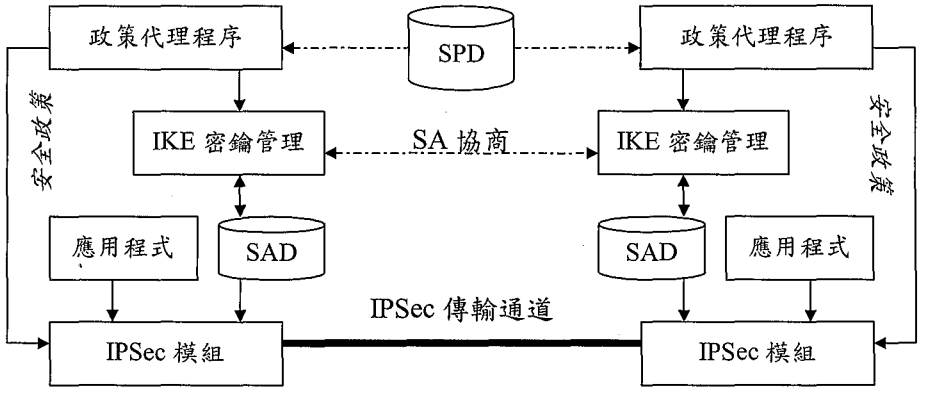

圖 2：結合政策管理之 IPSec 協定傳輸示意圖

為了有效管理虛擬私有網路系統中的安全政策，本研究提出適當的安全管理架構，以集中式管理而分散儲存的設計理念，形成一分工負責的分散式安全管理機制。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，作為管理者與虛擬私有網路系統間溝通的橋樑。安全政策管理系統（security policy management system, SPMS）是架構中的安全管理中心，所有安全政策都可經由 SPMS 作正確的管理，管理者根據安全規則設定正確的安全政策，再由 SPMS 經由公眾網路透過安全政策協定（security policy protocol, SPP）[11]，將安全政策傳送到所屬的虛擬私有網路區域系統（VPN local system）儲存以供執行。

一般而言，安全政策的設定方式基本上有兩種方式，第一種是由 SPMS 集中設定再分發到區域性的系統中；第二種是由區域性的系統中設定，再經 SPMS 驗證後，更新區域性的系統。虛擬私有網路系統的管理者可由 SPMS 直接透過管理介面進行安全政策建立，並驗證新政策對於舊有政策的一致性，然後進行政策簡化與合併，最後將新的政策引入儲存在 SPMS 中的 SPD；此外，各區域性的虛擬私有網路系統的管理者亦可透過區域性的政策管理伺服器（local policy management server, LPMS）進行安全政策設定，LPMS 會先將新安全政策傳送到 SPMS，執行驗證新政策對於舊有政策的一致性，再將新的政策引入。SPMS 與區域的虛擬私有網路系統間相互關係，可由圖 3 的相關系統模組架構圖清楚的表示其相互間的關聯性。系統架構主要分為安全政策管理系統與區域性的虛擬私有網路系統兩個主體，區域性的虛擬私有網路系統是執行資料傳輸的單元，當傳輸需求發生時，依據所在區域的 SPD 規範，評判該傳輸需求所適用的傳輸行為；無論新政策的設定於何處產生，均需透過 SPMS 先行驗證與管理後才得以建立，再透過安全政策協定傳送到所屬的 LPMS 儲存在區域的安全政策資料庫中；區域性的 SPD 與「非區域性」的 SPD 其差異在，非區域性的 SPD 在本研究中將其定義為集中管理的 SPD，它所儲存的資料包含了所有分散區域的 SPD 的資料，而區域性的 SPD 的資料則只儲存區域系統所需要的安全政策。

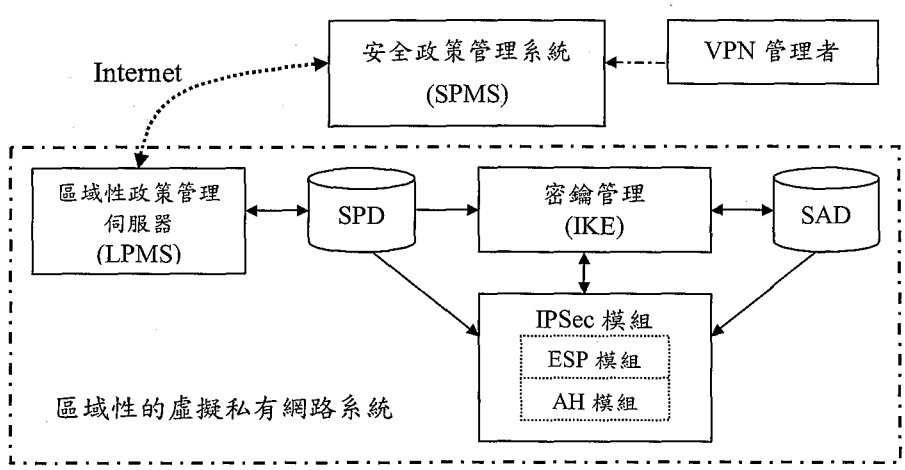

圖 3：安全政策管理系統與虛擬私有網路相關模組架構圖

本研究所提出的虛擬私有網路系統架構，乃是以安全政策管理系統為核心，以加強對安全政策的控管並滿足虛擬私有網路應用上的需求。下面就針對本研究之系統中 LPMS 與 SPMS 相關元件作詳細說明。

一、區域性的政策管理伺服器

根據以政策為基礎的網路管理概念而言，區域的虛擬私有網路系統同時整合了政策決策點（PDP）與政策執行點（PEP）；PDP 負責管理區域性安全政策，並依據政策規則來決定傳輸行為，PEP 執行由 PDP 接收的決策。依據本研究的規劃，位於區域的虛擬私有網路系統的政策管理伺服器即屬於 PDP 的部分，而依照政策規則進行不同傳輸行為與動作的 IPSec 模組與 IKE 密鑰交換等，通常是建構在所謂的安全閘道器（security gateway, SG）之中，而屬於 PEP 的部分。茲將區域性的虛擬私有網路系統與政策管理的關係表示於圖 4。

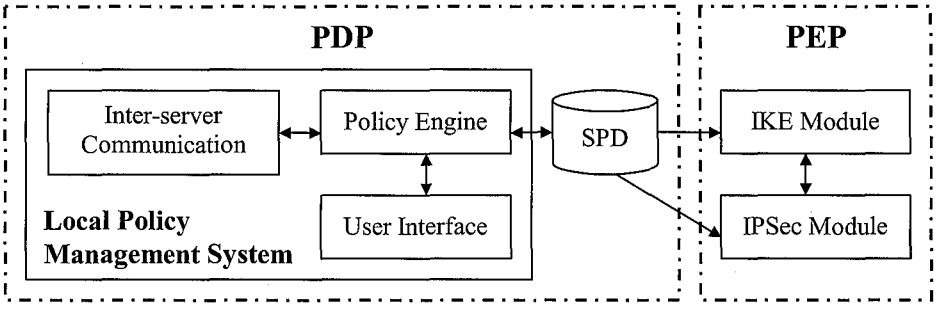

圖 4：區域性政策管理伺服器相關模組示意圖

區域的政策管理伺服器可視為虛擬私有網路中安全閘道器的政策代理程序，其主要的功能在與集中管理政策之安全政策管理系統（SPMS）溝通，以取得區域系統需要且正確的政策規則。相關的模組功能說明於下：

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。新的安全政策可以由區域的管理者透過人機介面進行設定，或透過 Inter-server Communication 模組，接受來自中央控管的 SPMS 之中的安全政策設定。在將新的政策引入系統之前，必須先行驗證新政策對於舊有政策的一致性；在本研究的規劃下，無論政策新增的方式為何，其政策一致性的驗證均交由 SPMS 負責。
2. **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人機介面，提供區域安全管理者進行安全政策的設定。
3. **Inter-server Communication**：提供標準的資訊傳輸程序，以進行不同政策管理系統間的訊息溝通，其主要功能可用在與 SPMS 進行安全政策的交換。在本研究的規劃，乃使用安全政策協定（SPP）作為政策管理系統間之標準的訊息傳輸協定，為了加強傳輸內容的安全保障，在政策的交換可以同時使用適當的安全機制（如 IPSec 協定）來保護 SPP 的資料傳輸。

二、安全政策管理系統

利用政策管理模式可協助虛擬私有網路系統進行系統管理，包括協助密鑰管理系統溝通傳輸所需的 SA，以及針對不同傳輸位址、應用程式、或使用者等進行不同安全等級的傳輸保障。良好的政策管理系統，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**：在建立新的安全政策時，新的政策有可能與系統已存在的政策相互衝突，因此政策管理系統必須在建立新政策的同時，進行對政策一致性(consistency)的確認工作，以提醒管理者訂定出適當的政策規則。
2. **分散式的政策管理**：企業組織運用虛擬私有網路時，其網路系統或政策管理系統均可能分散在各處，並由不同的網路管理者加以控管，因此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。除了設計適當的溝通方式使分散的系統間互通訊息外，使用中央式的政策管理系統用以管理整體網路的安全政策亦是可行的解決方案。
3. **與企業內部資訊系統的整合**：虛擬私有網路的傳輸安全需求多半與企業內部的資訊系統相關，這些系統包括防火牆、身份驗證系統、存取控制等，而這些系統對應用程式與使用者的控管亦可能使用政策管理的方式，因此虛擬私有網路系統的政策管理應與企業內部相關資訊系統整合，並從中建立對應關係。

根據本研究所提出的安全管理架構，安全政策管理系統（SPMS）是一個集中式的管理機制，政策的建立與管理可透過管理者手動設定，或透過與企業內部安全控管機制的對應自動產生，然後將更新的政策設定分散到所屬的區域性的虛擬私有網路系統上的 LPMS；安全政策管理系統亦可接受來自 LPMS 政策設定或需求，並產生適當的回應，以達到集中控管的目的。我們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。茲將此政策管理系統的相關模組示意如圖 5，並說明相關模組的目的。

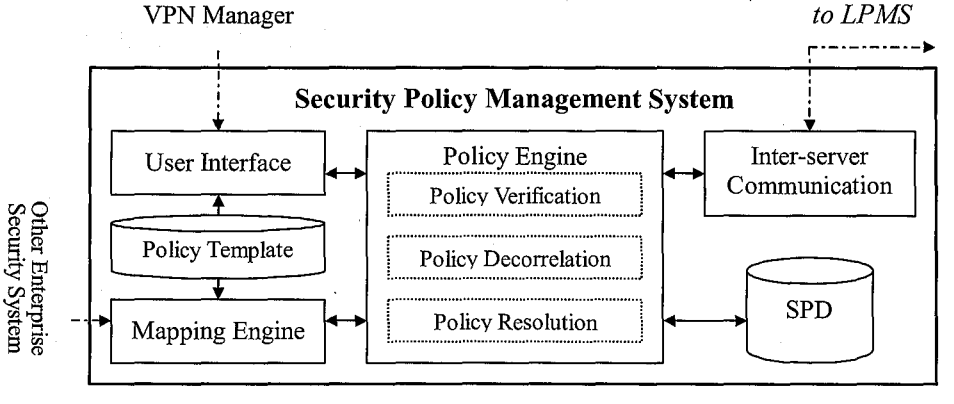

圖 5：安全政策管理系統相關模組示意圖

1. **Policy Engine**：管理系統中已存在的政策並將政策引入。在將新的政策引入系統之前，必須驗證（verification）[5]新政策對於舊有政策的一致性，簡化政策規則的相關性後（decorrelation）[12]，再將政策引入（resolution）。除了建立與管理安全政策外，當接收到來自 LPMS 發出安全政策需求時，必須能夠找尋到對應的政策，或是透過其它方式產生新的政策。
2. **SPD**：存放政策管理系統中安全政策的資料庫，SPMS 集中管理所有區域虛擬私有網路的安全政策，其內容要符合標準以供密鑰管理等機制使用。
3. **Inter-server Communication**：提供標準的傳輸協定，以進行不同政策管理系統間的訊息溝通，其主要功能可用在與 LPMS 進行安全政策的交換。
4. **Policy Template**：儲存政策規範的範本，供管理者或其他產生新政策的單元參考使用。政策範本的內容為系統管理者根據不同安全等級的特性事先設定，其的功用在於簡化政策新增時的管理課題，範本的內容包含不同安全政策中必要且共通的資訊，並可提供政策的基本分類。
5. **Mapping Engine**：提供自動建立政策的程序，其目的將已存在的企業內資訊系統的安全規範，與虛擬私有網路系統的政策範本進行對應與關聯，以加速與方便對虛擬私有網路的管理。
6. **User Interface**：提供虛擬私有網路網路管理者建立新政策或對政策系統進行管理的人機介面。

三、系統運作模式說明

根據 3.1 與 3.2 節的說明，本研究所提出的架構是以 SPMS 為系統中安全政策管理的中心，SPMS 透過安全政策協定，將各區域的虛擬私有網路系統所屬的安全政策傳送到各 LPMS；虛擬私有網路管理者可以新增、刪除或修改安全政策，而安全政策經過 SPMS 中的 policy engine 模組處理後儲存在集中管理的 SPD 中；為了與企業內部的安全控管系統結合，SPMS 可提供自動對應的機制產生適當的安全政策；當 LPMS 對 SPMS 提出安全政策的需求時，SPMS 亦可回應適當的政策供使用。

我們以點對點資料傳輸案例[10]來說明本系統架構的運作模式。假設分屬於不同區域虛擬私有網路系統的主機 H_1 與 H_2 分別透過安全閘道器 SG_1 與 SG_2 進行資料傳輸，其系統運作模式如下所述：

1. H_1 的應用程式發出與 H_2 間的資料傳輸需求。
2. SG_1 接收到 H_1 的傳輸需求後，向所屬的 LPMS 提出 H_1 到 H_2 間的政策需求，LPMS 自 SPD 查詢對應的安全政策，將安全政策回覆給 SG_1。當對應的安全政策不存在於區域的 SPD，LPMS 必須向 SPMS 提出政策需求，以取得適當的政策設定。
3. SG_1 對應的安全政策後，用以決定 H_1 與 H_2 間的傳輸行為，並透過 IKE 模組進行 SG_1 與 SG_2 間的 SA 協商，取得所要使用的加密或驗證演算法，以及進行密鑰的交換。
4. SG_2 接收到來自 SG_1 的 SA 協商需求，以類似的程序向所屬的 LPMS 取得對應的安全政策作為協商的依據。
5. 協商完成的 SA 資訊提供給 SG_1 與 SG_2，作為 IPSec 模組用來建立 SG_1 與 SG_2 間的

傳輸通道之用。

6. H_1 與 H_2 間開始透過 SG_1 與 SG_2 之間的 IPSec 通道傳輸資料。

本例中所闡述的傳輸模式可歸類為 IPSec 通道模式（tunnel mode），亦是一般虛擬私有網路系統較為常用的模式；若為了保障傳輸資訊在企業內部網路的安全，安全通道的建置必須位於傳輸主機之間（即本例的 H_1 到 H_2 之間），而在主機上必須建置 IPSec 與 IKE 相關模組，且要能夠與所屬的 LPMS 溝通。

肆、虛擬私有網路與職務角色控管機制的整合

以角色為基礎的安全管理正逐漸受到企業組織的重視，原因在於角色的概念更貼近實際組織管理的架構，其可依照組織架構與執掌延伸，並具備職務承繼與權限動態調整的彈性，而與傳統依各應用系統管理需求而產生群組（group）的模式有所不同。尤其是在資訊資源的執行權管制上，透過角色的定義以及權限之賦予，管理者只須專注於組織人員角色之指派，可以簡化原本繁複的管理工作。

根據上一章針對虛擬私有網路與政策管理系統整合之相關探討，本研究考慮實際的企業組織的安全管理的需求，將安全政策的管理與公司相關權限控管機制的結合。在企業組織中，人員的變動是常態，職務則是制度的一部分，更改的頻率相對而言就要少得多。以角色為基礎的控管機制，有助於落實企業組織制度化的安全控管環境的建立，提供更具彈性的資訊管理模式，本研究進一步將研究主題架構在政策管理的虛擬私有網路基礎上，透過安全政策管理系統與企業內專屬或已存在之角色控管機制整合，成為安全政策控管的自動機制。

企業資訊傳遞的安全性是以組織整體為主，因此安全政策的管理也應該以組織整體為基礎。職務角色控管機制實能以組織整體為考量，進而有效控管組織內的行為；對於組織內人員進行組織活動時，其扮演的角色乃是根據所從事之行為進行動態賦予，因此同一位使用者在進行不同的活動時在系統中可能扮演不同的角色。職務角色控管機制使用上述的動態角色賦予方式來解決角色權限的分級與衝突，特別適用於虛擬私有網路中安全政策的管理；當使用者利用虛擬私有網路技術進行資料傳輸時，根據使用者從事的活動所扮演的角色，可對應出該活動所需要的傳輸安全等級與安全政策等，以有效保障組織整體的資訊安全性。

由於資料傳輸的安全等級與傳輸雙方所扮演的角色相關，因此在本研究中，安全政策與角色的對應關係是以傳輸雙方的角色關係為基礎，在同一個企業組織中，可根據角色的關係使用對應的安全政策，對於企業間或與客戶間的資料互傳，除了提供特殊窗口以規範企業外部使用者的職務角色外，對於具備長期合作關係之企業，可進行企業間職務角色控管機制的整合，以取得具備完整性的職務角色關係。

根據本研究的規劃，位於安全政策管理系統的 Mapping Engine 模組是整合企業內角色控管機制與虛擬私有網路系統的橋樑，其中重要的元件如圖 6 所示，並說明於下：

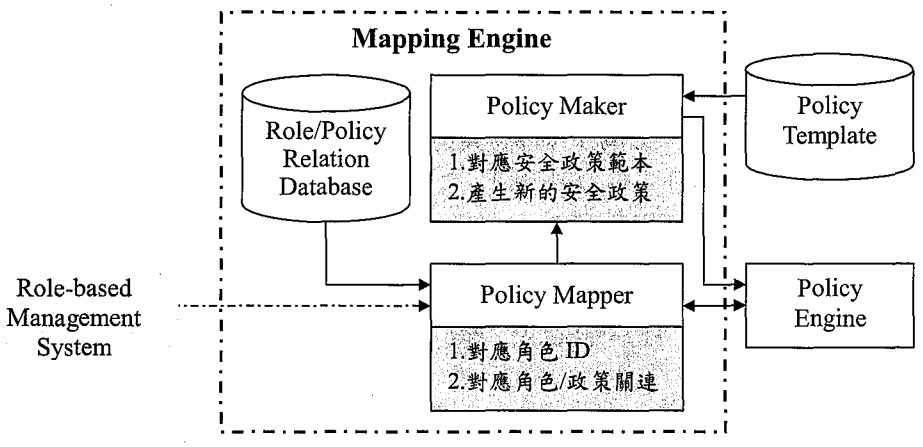

圖 6：Mapping Engine 模組相關元件示意圖

1. **角色與政策關聯資料庫（role/policy relation database）**：紀錄角色與政策範本的對應資料，以建立其間的關聯性。管理者根據職務角色的安全等級分類與安全政策範本的政策，定義企業內資訊系統的安全政策與職務角色之對應關聯。此資料庫並不是對應每一個個人的設定，而是以角色歸類的設定資料，本研究規劃其欄位包括角色 ID、IP 位址與政策範本序號等。
2. **Policy Mapper**：根據使用者資訊取得職務角色的索引資料。根據查詢所得的角色，以及角色與政策關聯資料庫的設定，對應正確的安全政策範本序號，再交由 Policy Maker 取出安全政策範本，以產生新的安全政策。
3. **Policy Maker**：根據安全政策範本序號取得安全政策範本的資訊，根據政策範本的資訊，以及相關的使用者與 IP 位址等資訊，產生新的安全政策。最後，回覆新產生完成的安全政策給 Policy Engine。

當安全政策管理系統接收到政策需求時，先確認是否有相對應的安全政策在現有的安全政策資料庫（SPD）中，若對應的安全政策不存在，就必須新增需要的安全政策，本研究透過 Policy Engine 與 Mapping Engine 相互配合，並藉由系統管理者對角色與政策關聯資料庫、政策範本資料庫、以及企業內職務角色參數之設定，形成安全政策的自動產生機制。茲將本研究所提出的安全政策自動產生機制之運作流程圖示意於圖 7：

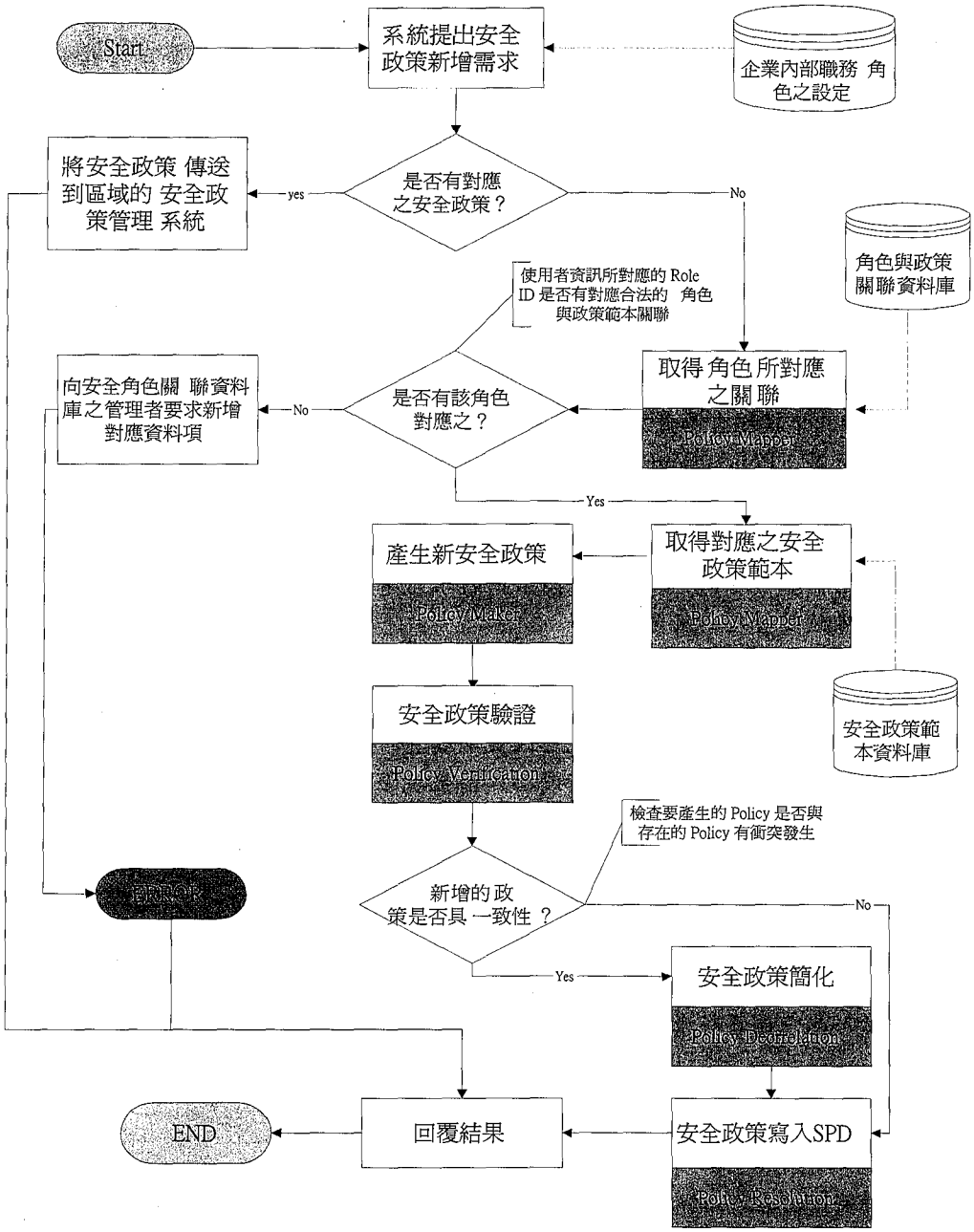

圖 7：安全政策自動產生機制之系統運作流程圖[1]

整個安全政策產生的流程大致可分類成下列數個步驟：

1. **接受政策需求**：當系統所需要的安全政策不存在，將透過 Policy Engine 模組接受該政策新增的需求，並接取需求傳入的選擇器（selector）與使用者資訊作為後續處理的依據。
2. **驗證角色**：由 Policy Mapper 模組啟動角色確認處理程序，向企業內的角色控管機制取得使用者的角色資訊。使用者的角色資訊為角色控管系統之管理者事先設定，而使用者所扮演的角色乃是根據其職務與目前從事的活動，由企業內的角色控管系統動態賦予。
3. **查詢角色與政策關聯資料庫**：根據使用者所扮演的角色與相關資訊，取得已由系統管理者事先定義之角色與政策範本關聯。
4. **產生新政策**：根據角色與政策關聯資料庫的設定，取得對應的安全政策範本，由 Policy Maker 模組自動產生新的安全政策。
5. **驗證新政策**：Policy Engine 驗證新政策與現有存在的政策之一致性，再進行簡化合併安全政策及政策引入的步驟。
6. **更新 SPD**：將驗證過的新安全政策寫入 SPD。
7. **回覆政策需求**：Policy Engine 將結果回覆給需求的系統，並將安全政策傳送到適當的區域性政策管理伺服器。

利用本研究所提出的安全政策管理系統，相關功能模組能夠依照政策需求自動進行角色與政策範本的對應，用以自動產生所需要的安全政策，其運作流程需要參考三個資料庫，分別為安全政策範本資料庫、角色與政策關聯資料庫與企業內部職務角色之設定，因其資料內容各自獨立無法自動產生，所以必須由系統管理者依據企業的組織與政策進行人工設定；然而依照本研究所提出的系統架構，管理者藉由對安全政策範本的規劃，僅需專注於不同安全等級的參數設定，而非對所有的角色或使用者之安全政策進行設定，可大幅簡化管理的複雜度，亦便於對安全政策的參數變更。結合職務角色機制同樣可以降低管理的工作量，其主要功效在於減少使用者與政策範本之間關聯性的設定，進而提升系統運作的效率，減少管理上的誤謬，並與企業組織的職務角色連結。由於考慮到企業資訊安全的管理權責分工，此三個資料庫可能分屬不同的安全系統管理者管理之。

伍、案例與可行性分析

本研究針對虛擬私有網路與政策管理系統整合之相關性加以探討，並考慮實際的企業組織的管理需求，使用集中管理且分散儲存的政策管理模式，並進一步與職務角色控管機制整合，歸納出安全政策的自動產生機制。本章就根據本研究所提出之虛擬私有網路系統架構與運作流程，制訂出適當的資料項與資料欄位，並套用到實驗性的組織架構，並驗證此理論模型的合理性與可行性。

一、資料庫說明

本研究所探討的安全政策管理系統透過 Policy Engine、Mapping Engine 等模組，構成可行的自動化處理之安全政策管理模式。安全政策管理系統中的安全政策範本資料庫與角色與政策關聯資料庫為自動產生安全政策的核心，根據此兩個資料庫的關聯對應關係，進而透過 Mapping Engine 模組建立虛擬私有網路系統所需要的安全政策。本研究中所探討的安全政策範本，乃是根據安全政策各欄位的屬性，擷取部分欄位並加入其他必要之欄位，我們定義其所需要的基本資料欄位包括：範本序號、資料安全等級（security level）、動作、IPSec 模式、及演算法等，其資料型別如表 1 所示。

表 1：安全政策範本之資料欄位與型別

Template ID	Security Level	Action	IPSec Mode	Algorithm
Order list	Integer	{IPSec, Non-IPSec,Discard}	{AH,SP}+{Tunnel, Transport}	{56/64/128 bit, DES, 3DES, RC2, RC4, RSA, DSA, SHA-1, MD5}

在本研究中所探討的角色與政策關聯資料庫中，我們定義了其所需要的基本資料欄位包括：資料序號、來源角色 ID、來源位址、目的角色 ID、目的位址、傳輸通訊埠及安全政策範本 ID，其中除了資料序號與政策範本 ID 外，其餘欄位均是提供角色與政策範本的對應索引之用，其資料型別如表 2 所示。

表 2：角色與政策關聯資料項之資料欄位與型別

Relation ID	Src. Role ID	Src. Address	Dst. Role ID	Dst. Address	Transport Port	Template ID
Order list	Integer	single value, range, or wildcard	Integer	single value, range, or wildcard	single value, range, or wildcard	Integer

安全閘道器間使用 IPSec 進行安全性傳輸資料時，安全政策提供對應的參考資訊以供密鑰管理機制在交涉 SA 時所需，以及規範 IPSec 模組用來傳輸資料的行為。SA 是存在於兩端通訊實體的一種單向關係，所以進行雙向的安全通訊時，必須個別建立不同傳輸方向的 SA，同樣地安全政策也繼承此種單向關係；因此我們設計角色與政策關聯資料項時特別考慮其方向性，故分別定義了相關的來源與目的資料欄位做為索引，以達到管理雙向安全通訊的目的。

二、案例說明

本節我們以一個公司階層式的職務組織，套用本研究所提出的理論架構與規劃，以驗證其有效性。如圖 8 所示，H_1（10.2.3.4）、H_2（128.10.2.37）、H_3（10.2.3.50）與 H_4（128.10.2.50）分別屬於兩個不同的安全網域，我們以公司內負責不同工作之職務角色，包括處長（role ID 20）、經理（role ID 18）、副理（role ID 16）與工程師（role ID 14）等在其間進行資料傳輸

時，SPMS 對相關安全政策的設定進行說明；其中傳輸雙方角色關係與安全政策範本的關聯需要事先定義於角色與政策關聯資料庫，而預設的傳輸安全等級利用安全政策範本進行規範，本案例的安全等級假以訂定為 5 種等級，愈大的安全等級值（security level）代表具有較高傳輸安全性的安全等級，並使用對應之參數來規範每個安全等級所使用的資訊安全技術。茲將預先設定的相關資料內容示列於表 3。

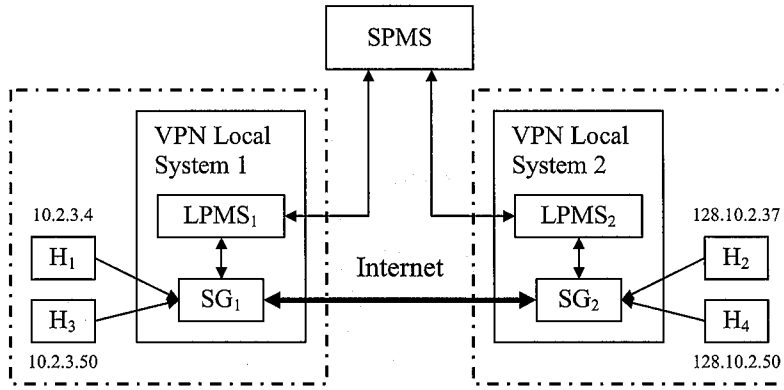

圖 8：虛擬私有網路系統資料傳輸案例

表 3：相關資料庫資料內容案例

角色與政策關聯資料項

Relation ID	Src. Role ID	Src. Address	Dst. Role ID	Dst. Address	Transport Port	Template ID
1	20	H2	18	*	*	2
2	20	*	14	H3	*	4
3	18	*	20	H2	*	3
4	16	H4	16	H1	*	3
5	14	*	20	*	*	5

註："*"表任何可能之 IP address 或 IP port

安全政策範本

Template ID	Security Level	Action	IPSec Mode	Algorithm
1	100	IPSec	AH+ESP Tunnel	128 3DES+MD5
2	70	IPSec	ESP Tunnel	128 DES, SHA-1
3	50	IPSec	AH Tunnel	MD5, SHA-1
4	30	Non-IPSec	-	-
5	20	Discard	-	-

（一）案例一

使用者 A 的角色為經理自 H_1 進行雙向資料傳輸到 H_2 給角色為處長的使用者 B，其系統運作流程如下：

1. SG_1 收到 H_1 發出連線需求後，向 $LPMS_1$ 送出安全政策查詢的需求訊息。
2. 當 $LPMS_1$ 找不到對應的安全政策時，$LPMS_1$ 會向 SPMS 發出安全政策查詢的需求，查詢 H_1 到 H_2 適用的安全政策。
3. SPMS 根據傳入的政策需求，先向職務角色控管機制查詢取得其角色為經理與處長，所對應出的 role ID 分別為 18 與 20。
4. SPMS 在根據角色與政策關聯資料庫的設定，取得角色與政策關聯的資料項序號分別為 1 和 3，以及對應的安全政策範本序號分別為 2 和 3。
5. 根據安全政策範本、目的端 IP 位址、來源端 IP 位址與服務通訊埠等，產生出新的安全政策如下。

Policy ID	Src. Address	Dest. Address	Src. Port	Dest. Port	User ID	Action	IPSec Mode	Algorithm
1	*	128.10.2.37	*	*	A	IPSec	AH Tunnel	MD5, SHA-1
2	128.10.2.37	*	*	*	B	IPSec	ESP Tunnel	128 3DES

註：”*”表任何可能之 IP address 或 IP port

1. 將新產生的安全政策進行一致性檢查後，再寫入 SPD。
2. SPMS 將正確的安全政策傳送至 H_1 與 H_2 所屬的 LPMS，LPMS 依據 SPMS 告知的安全政策更新區域的 SPD，並回覆訊息給 SG_1 與 SG_2。
3. SG_1 與 SG_2 依據安全政策的設定進行密鑰交換以及建置 IPSec 傳輸通道。

（二）案例二

延續案例一，角色為工程師的使用者 C 自 H_3 進行雙向資料傳輸到 H_2 給使用者 B。同樣地，SPMS 根據相關的資訊取得對應的角色與政策關聯 2 和 5，以及安全政策範本 4 和 5，並歸納出新的安全政策如下所示：

Policy ID	Src. Address	Dest. Address	Src. Port	Dest. Port	User ID	Action	IPSec Mode	Algorithm
3	*	*	*	*	C	Discard	null	null
4	*	10.2.3.50	*	*	B	non-IPSec	null	null

註：”*”表任何可能之 IP address 或 IP port；”null”表欄位不含任何資料

由於新產生的安全政策 4 與已現存的安全政策 2 有相關性，所以必須進行政策的簡化。經過去除相關性的演算後，最後 SPD 資料更新如下所示：

Policy ID	Src. Address	Dest. Address	Src. Port	Dest. Port	User ID	Action	IPSec Mode	Algorithm
1	*	128.10.2.37	*	*	A	IPSec	AH Tunnel	MD5, SHA-1
2	128.10.2.37	10.2.3.50	*	*	B	non-IPSec		
3	128.10.2.37	*-10.2.3.50	*	*	B	IPSec	ESP Tunnel	128 3DES
4	*-128.10.2.37	*	*	*	B	non-IPSec		
5	*	*	*	*	C	Discard		

註：”*”表任何可能之 IP address 或 IP port；”-”為差集合運算符號

SPMS 產生新政策後，H_2 與 H_3 根據 SPD 資料開始進行適當的資料傳輸行為，由於 SPD 中的政策 5 指定使用者 C 對任何主機的傳輸都被拋棄，故此案例為禁止傳輸的案例。由此案例得知，同一個使用者 B 對於不同的使用者可進行不同的資料傳輸行為（即使安全通道同樣建置在 SG_1 與 SG_2 之間），增加虛擬私有網路應用上的彈性，並達成結合角色控管機制的目的。

三、系統複雜度分析

為了進一步驗證本文提出之系統架構的可行性與效能，本研究針對相關資料庫與運作流程進行複雜度分析，並與傳統之虛擬私有網路系統架構進行比較。由於實際的系統效能評估多半在系統建置時才能有效進行，利用複雜度分析較能在現階段取得具備參考意義的可行性評估，並有助於系統建置時分析與設計工作的進行。關於與企業內部資訊系統的整合難易程度，需要參考實際的企業資訊安全控管系統，利用統計方法進行相關課題的調查與分析擬作為的未來研究方向。

（一）資料庫複雜度

本研究針對系統中所使用的重要資料庫進行分析，包括(1)角色與政策關聯資料庫、(2)政策範本資料庫、(3)企業內職務角色控管系統之角色資訊、以及(4)虛擬私有網路系統之安全政策資料庫（SPD）。假設虛擬私有網路系統的使用者數量為 N，根據職務角色控管機制的精神，使用者可能被賦予的角色種類為 n 種（其中 $n<N$），也就是說企業內的角色資訊複雜度為 $\Theta(n)$；在角色與政策關聯資料庫中，資料項以成對的角色關係進行對應，由於在虛擬私有網路技術中，傳輸雙方的關係為單向，因此對於 n 個角色，共有最多的關係為 $C_2^n \times 2$，因此角色與政策關聯資料庫的資料項最大將同等於角色的關係數，相當於 $O(n^2)$ 之複雜度；政策範本資料庫的複雜度與系統管理者所設定的安全等級數目 L 相關，就一般狀況而言，安全等級數目大幅低於可能產生的傳輸關係數目（即 $L<n^2$），因此政策範本資料庫的複雜度亦可估計為 $O(n^2)$；在本系統中，虛擬私有網路系統之安全政策為動態產生，並與參與的角色數目相關，複雜度為 $O(n^2)$。由以上的推論得知，本研究所提出之系統架構其資料庫複雜度為 $O(n^2)$。傳統上僅透過安全政策資料庫來進行安全等級的控管所需要的資料複雜度和使用者或網路位置相關，若不考慮系統管理者的系統控管複雜度，其所需要的資料庫複雜度為 $O(N^2)$，因此當 $n<N$ 時，本研究所提出之系統架構具有較低的資料庫複雜度。

（二）系統運作複雜度

本研究所提出之系統運作流程主要包括以下數項關鍵點：(1)角色的查詢與驗證、(2)角色與政策範本的對應、(3)安全政策的建立、驗證、與引入、以及(4)安全政策的查詢。安全政策的查詢在傳輸需求產生以及新政策建立後發生，延續上一節的定義，由於安全政策資料庫的複雜度為 $O(n^2)$，其排序與查詢所需要的複雜度為 $O(n^2 \lg n)$；角色的查詢與驗證與角色的數目 n 相關，就一般狀況而言，其所需要的複雜度包括排序與存取的複雜度為 $O(n \lg n)$；角色與政策範本的對應與角色關係數目以及政策範本數目相關，在前面對於 $L<n^2$ 的假設下，其總體的複雜度為 $O(n^2 \lg n^2) \times 2 = O(n^2 \lg n)$；新建立的安全政策需要與舊有的安全政策進行驗證（verification）、簡化（decorrelation）等，由於簡化的演算法與安全政策的索引欄位數目有關，若不考慮實際的簡化演算法複雜度，相關的驗證、簡化所需要的複雜度為與舊有安全政策進行比對的量，即 $O(n^2)$。由以上的推論得知，本研究所提出之系統運作流程其總體複雜度為 $O(n^2 \lg n)$。傳統上僅透過安全政策資料庫來進行安全等級的控管需要針對 $O(N^2)$之資料複雜度進行排序與查詢，其複雜度為 $O(N^2 \lg N)$，從系統運作的複雜度來看，本研究所提出之系統運作模式並沒有增加額外的複雜度，但由於傳統的運作模式僅需要進行安全政策的排序與查詢工作，就系統效能觀點來看，即使不考慮系統管理者的系統控管複雜度，仍無法保證本研究所提出之系統運作模式具有較低的系統運作複雜度。根據系統運作複雜度的比較，當使用者與角色的數目差別較大時（即 $n<<N$ 時），本研究所提出之系統架構將大幅降低系統管理者的控管工作量，理論上具有較低的系統運作複雜度與較高的效能，適於運用在職務階層清楚、人員眾多的企業組織。

（三）分析與比較

本節針對本研究所提出之系統架構與自動化安全政策管理機制進行分析，探討相關課題之優缺點並與傳統之安全政策管理模式進行比較。由於相關的虛擬私有網路的基礎技術如訊息加解密的方式和驗證機制等，在兩者之間並無明顯之相異處，故分析與比較的著眼點以安全政策的管理模式為主。茲將相關分析與比較示列於表 4。

表 4：安全政策管理模式之分析與比較

分析課題	傳統之虛擬私有網路安全政策管理模式	本研究所提出之自動化安全政策控管機制
資料庫	1. 對於每一個安全閘道器（security gateway）僅需要一個 SPD。 2. 所有的安全政策為系統管理者自行設定，必須佔用較大的資料庫空間儲存所有的安全政策。	1. 集中式管理的 SPMS 必須包含角色與政策關聯資料庫、政策範本資料庫、以及安全政策資料庫。 2. 區域之 LPMS 僅暫存安全閘道器需要參考之安全政策。 3. 集中管理之 SPD 其內容為自動產生，僅儲存系統運作時所需要參考之安全政策。
運作模式	1. 根據傳輸需求查詢位於 SPD 中對應之安全政策。	1. 與角色控管機制結合，利用角色關係以及政策範本的對應，自動建立需要之安全政策。 2. 新增的安全政策在引入之前還必須進行驗證與簡化。
系統控管課題	1. 系統管理者必須針對所有之使用者或網路位置制訂必要之安全政策。 2. 當分散之安全閘道器分屬不同管理者進行控管，必須相互協調以免分散之安全政策產生衝突。 3. 當 SPD 較為龐大，為了控管的方便與正確性，仍需要開發安全政策的驗證與簡化等控管機制。	1. 系統管理者透過集中式的 SPMS 即可對整體之安全政策進行控管。 2. 系統管理者僅需針對角色關係與政策範本的對應進行控管，其變動的機率比針對使用者控管為低。 3. 所有安全政策的內容透過對安全政策範本的設定達成，較容易結合企業組織整體的政策並便於控管。
可行性	1. 系統運作模式較為單純，適用於使用者較少，且在傳輸應用的分類上上與使用者關係較低之組織。	1. 系統運作模式具有多個單元與階段，能解決較複雜的控管課題，適用於使用者較多，且職務角色與安全政策分級較具相關性的組織。
效能	1. 直接對 SPD 進行安全政策的查詢與存取，在運作上具有較高的效能。 2. 系統管理者需要面對較為繁複的控管工作，並需要解決分散之 SPD 所產生的協調問題。	1. 傳輸需求發生時，系統需要進行安全政策的自動產生過程，回覆傳輸需求的時間較長。 2. 系統管理者僅需專注於角色與政策範本的對應，以及透過政策範本的設定建立安全等級；系統控管的複雜度大為降低。

陸、結論

本研究以政策管理為出發點，整合企業組織之職務角色控管機制，進而提出一個整合性的虛擬私有網路系統架構。綜合前面章節所探討之研究理論，本研究以職務角色、政策管理與虛擬私有網路技術為基礎，針對虛擬私有網路中實際的企業組織之安全管理的需求，建立一個貼近實際組織管理，且更具彈性的安全管理模式，並提出一個可行的虛擬私有網路系統架構，此架構以安全政策管理系統為核心，所有安全政策都可經由安全政策管理系統作適切的管理，虛擬私有網路管理者可以根據既定的安全規則設定適當的安全政策，再透過安全政策協定，將安全政策傳送到各區域虛擬私有網路系統以供執行。

在與企業組織職務角色控管機制的整合方面，本研究運用職務角色與安全政策的關聯性，透過適當的機制與企業內專屬的安全管理系統相互配合，達成自動化的安全政策產生機制。總括而言，本研究所提出之虛擬私有網路安全管理架構具有下列特性：

1. **保障政策的一致性**：在建立新的安全政策時，安全政策管理系統會進行對政策一致性的確認工作，避免衝突的政策存在於系統中。
2. **分散式的政策管理**：本研究提出集中式的政策管理模式用以管理整體網路的安全政策，以集中管理而分散儲存的設計理念，形成一分工負責的分散式安全管理機制。
3. **政策管理的自動化**：本架構根據安全政策與職務角色的關聯性，與企業內專屬或已存在的職務角色控管機制整合，形成一個安全政策產生的自動機制，以簡化繁複的系統控管工作。
4. **適當的管理機制**：本研究所提出的虛擬私有網路架構結合職務角色控管機制，有助於落實企業組織制度化的安全控管環境的建立，並提供更具彈性的管理模式。
5. **結合企業內部資訊安全之政策**：虛擬私有網路的傳輸安全需求多半與企業內部的資訊安全政策相關，當企業內部的資訊安全政策使用角色控管機制為基礎時，本研究所提出之虛擬私有網路系統能夠透過安全政策範本與職務角色的對應關係，使得資訊傳輸的安全政策與企業內部資訊安全政策具備一致性，有助於系統管理者對企業內部資訊系統的資訊安全課題進行整體的探討與控管。

本研究探討了職務角色、政策管理與虛擬私有網路概念的整合模式，提出了以安全政策管理系統為其核心的虛擬私有網路系統架構，提供企業組織在安全管理上更具彈性的虛擬私有網路管理模式。

參考文獻

1. 邱士哲，2002，運用職務角色控管機制在以政策為基礎之虛擬私有網路，國立交通大學資訊管理研究所碩士論文。
2. 羅濟群、莊秉文等，1999，『虛擬私有網路簡介及其應用』，資訊安全通訊，第五卷・第三期。
3. Clercq, J. D., Paridaens, O., "Scalability Implications of Virtual Private Networks," IEEE Communications Magazine (40:5), 2002.
4. Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)," IETF RFC 2409, 1998.
5. Jeong, M. S., Baek, S. J., et al, "Policy-based Hybrid Management Architecture for IP-based VPN," *Proceedings of IEEE Symposium Record on Network Operations and Management, 2000.*
6. Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol," IETF RFC 2401, 1998.
7. Kent, S., Atkinson, R., "IP Authentication Header," IETF RFC 2402, 1998.
8. Kent, S., Atkinson, R., "IP Encapsulating Security Payload," IETF RFC 2406, 1998.
9. Kosiur, D., "Building and Managing Virtual Private Networks," Wiley & Sons, 1998.
10. Mazzocchi, D., Baltatu, M., et al, "Security Policy System: status and perspective," Proceedings of IEEE International Conference on Networks, 2000.
11. Sanchez, L. A., Condell, M. N., "Security Policy Protocol," IETF Internet Draft, 2000.
12. Sanchez, L. A., Condell, M. N., "Security Policy System," IETF Internet Draft, 1999.
13. Sandhu, R. S., Coyne, E. J., et al, "Role-based Access Control Models," IEEE Computer Magazine, 1996.
14. Wang, C. K., "Policy-based Network Management," WCC-ICCT, 2000.