IPSec 安全機制之探討

作者/林育生 中校・李武耀 上尉・歐品蘭 少校

提要

隨著通資科技與網際網路應用於電子商務的日趨發達與相對複雜化，網路系統安全性亦日趨受到重視。尤其在實施機敏性資料的傳送過程中，如何確保資料的「保密性」已成為最基本的要求要項。除外，對於整體系統之「完整性」、「有效性」、「確認性」及「不可否認性」亦等同重要。

IPSec 係由網際網路工程小組（Internet Engineering Task Force ,IETF）所制定的一系列關於 IP 層安全協定的標準。其制定的目的則是在於改善網際網路資料通訊的安全性，其內容大體包含 IPSec 架構、身份驗證、資料加解密及金鑰管理等。也由於該機制係於第三層（網路層）所制定，故亦可以提供更高階層協定（TCP、UDP、ICMP）所使用，此安全模式之運用亦有別於 PGP、S-HTTP 或 SSL 等應用層所制定的安全機制。故利用 IPSec 將密碼技術多方應用於網路層，將提供「認證」、「完整」、「存取控制」、「機密性」等安全性服務，此將有助於整體網路資訊安全之提昇。

壹、前言

近來，由於「Internet」的快速發展，透過公眾網路與私有網路的連結已足供各電腦用戶端彼此建立一個有效的資傳作業環境。但也由於網路間係多以 TCP/IP 協定為主，在「Internet」網路上，除 ARP、RARP 具獨立封包外，各 IP 封包標頭上均清楚地標示著「來源位址、目的位址、資料承載」等資料，只要是有心人利用如 sniffing 等工具，即可透視窺知 IP 封包的各項訊息資料，故在「安全」議題上將是有所爭議的。

「IPSec」係為 IETF 針對虛擬私有網路 (Virtual Private Network, VPN)所制定的規範，主要是將不可靠的 IP 協定轉換成具安全性的「IPSec」協定，於是藉此機制便得以在公共 Internet 上使用一安全管道及運用加密技術建立起一個私有的安全網路。本文撰寫之目的即著墨於 IPSec 安全機制的介紹，首先說明當前通資系統安全威脅模式，及私有虛擬網路，進而探討 IPSec 安全機制成員 AH（認證標頭）、ESP（加密封裝承載）、安全群組（SA）以及 ISAKMP（網際網路安全關聯金鑰管理協定）運作方式、最後介紹 IKE（金鑰交換）協議以及 IPSec 於 Windows2000 之實作探討，期對國軍資訊安全課題作為上有所助益。

貳、通資系統安全威脅模式

國軍在建構各式通資系統，供各級指揮官及幕僚各項情資傳遞及訊息交流，主要是以考量通資三大要求為著眼，即「迅速、確實、安全」，然隨著近來各式通資科技的發展及新一代通裝整合運用，利用外在的軟、硬體設備建構一個「即時性」的通資系統已成為代表單位內通資數位化能力建構的指標之一。但相對地，身處於一個越是整合型、越複雜的通資環境，越是容易陷入一個虛擬的通資安全迷霧中，試想處在一個可能是「爾虞我詐」的通資網路環境裡，敵人正無所不用其極，以「破壞、截取、偽冒、監聽」等各種手段，欲從中獲取相當的利益為目的。故如何確保情資傳遞時安全無虞，則是在發展通資科技時另一個必需嚴肅面對的課題。畢竟，今日國軍一再強調正視「通信暨資訊傳輸工具使用保密與管制規定」，其目的無非在於防制我軍於通資傳遞過程中若為敵方偵測、截收、分析，甚而偽冒、欺騙時，仍得以確保我軍機安全。因此，在考量整體通資建構環境上，將實質面對的安全威脅模式歸納如下[1](如圖一)。

一、通資系統安全威脅分類

欲探討通資系統安全威脅可從檢視整體通資系統所能提供之功能服務及資訊流之流向為著眼，而一般遭受攻擊的分類區分如下：

(一)中斷(interruption)

使系統資源遺失、不得取用、不堪使用或是利用惡意攻擊手段予以破壞硬體設備、刪除程式及資料檔或使作業系統阻絕服務(denial of services)等。此種安全威脅模式係針對系統之「有效性」進行攻擊行為。例如：實體層攻擊(有線電經路破壞、電台摧毀、檔案管理系統失效等均屬之)。

(二)截取(interception)

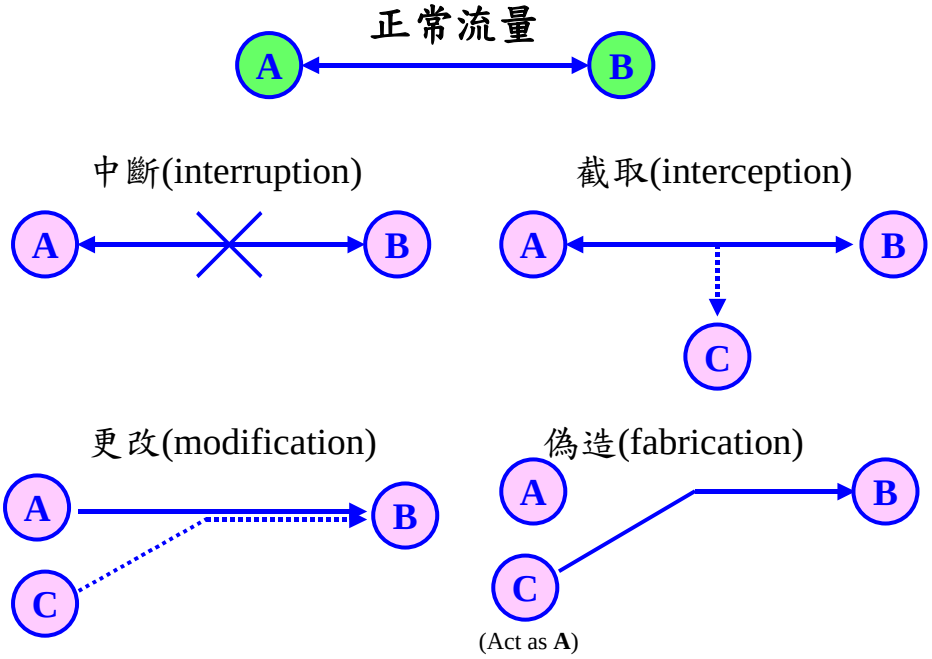
未經合法授權的第三者利用非法的手段截取系統資源或以非法方式拷貝程式或資料、網路截聽等。此種安全威脅模式係針對系統之「保密性」所做的攻擊行為，所謂未經授權的第三者可為單一個體或是一部電腦。例如利用無線電系統保密性較差的弱點，進行傳遞情資的竊取或是以網路監聽程式進行資料竊取或非法複製系統檔案或程式等均屬之。

(三)更改(modification)

未經合法授權的第三者不但可以利用非法的手段存取系統某項資源外，更得以更改系統資源、竄改內容，或有效改變系統儲存及傳輸資料之數值、更改程式以執行額外運算等。此種安全威脅模式係針對系統之「完整性」所做的攻擊行為，例如更改通信資料、電腦病毒感染等均屬之。

(四)偽造(fabrication)

未經合法授權的第三者將偽造資料加入系統中，使得資料使用者無法分辨真偽或於系統內額外加入訊息、增刪資料記錄等。此種安全威脅模式係針對系統之「確認性」所做的攻擊行為，例如更改通信資料內容。



圖一 通資系統安全威脅模式

二、通資安全性服務功能

無論是軍事安全需求或是一般電子商務，莫不以強化通資安全的維護，保障機敏性資料的安全為首要工作。故欲完成通資安全效能，實應考量達至下列目標[1-2]：

(一)機密性(confidentiality)

提供資料之秘密性與維護使用者隱私性。即只有經合法授權者才得以接收相關訊息。

(二)真確性、完整性(integrity)

此部分包含「資料」與「系統」兩層面，即「資料真確性」在於防制人為刻意竄改或自然雜訊干擾，即只有經過合法授權者才得以更改情資內容。而「系統完整性」主要防制假冒或未授權方式存取系統資源進行資料之處理或更改。

(三)有效性(availability)

主針對「系統服務」對合法之使用者或個體不能阻絕服務，另亦將提供即時回應與系統服務。

(四)確認性(authentication)

主要確認情資訊息之來源是可信賴的，即能有效確認發送者身分無疑。

(五)不可否認性(nonrepudiation)

無論發送端或是接收端均不能否認曾傳送情資訊息的事實。

參、VPN 虛擬私有網路簡介

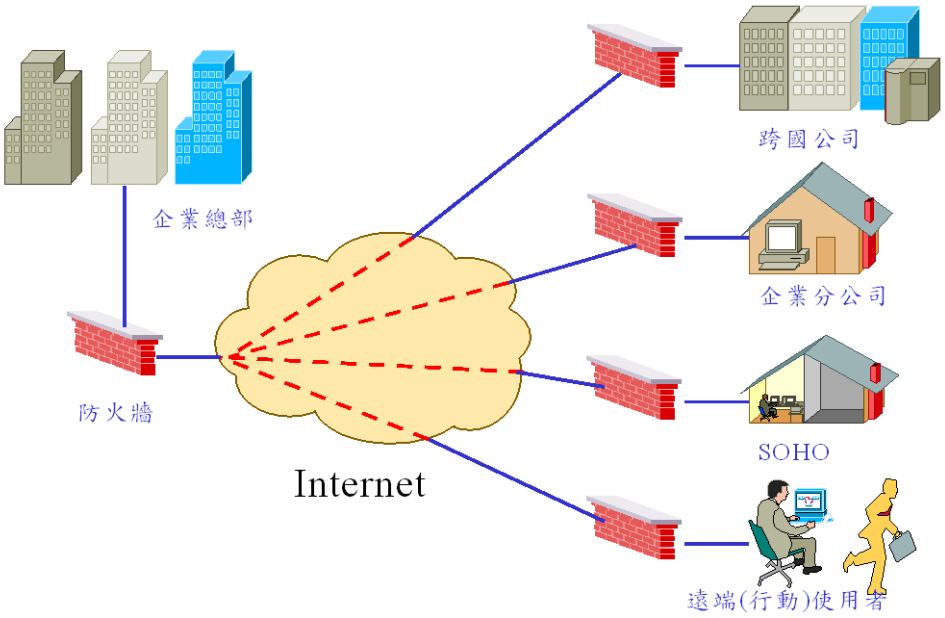
一、VPN 虛擬私有網路

「虛擬私有網路」(Virtual Private Network ,VPN)主要是期望在一個不安全的「公眾網路」上能夠建立一個安全性較高的「私有網路」。當前「公眾網路」莫過於以「Internet」為代表，在此一可能不設防的公眾網路中，網路上任何一個心存企圖的有心份子是可以以多重不法的手段，對系統進行資料存取，例如 sniffer 或 man-in-the-middle 均是常見的攻擊行為，故如何維護系統「保密性」及「確認性」以防杜系統遭受各式安全威脅，的確是在享受 Internet 所帶來便利之餘，所應嚴正面對的議題，因此「虛擬私有網路」的觀念技術因應而生。

但由於私有網路多已應用建架於 TCP/IP 協定上，用戶端只要利用瀏覽器便可進行一般性系統資源存取，故企業界莫不期望能夠真正建構一條完全專屬於自己企業內部的安全網路連線，以免除遭受如上述所述的各種安全威脅，甚而解決過去為求建架 VPN 網路必需花費大筆金錢向 ISP 業者租用專線的昂貴成本。因此，Internet VPN 與傳統專線相較之下，除在成本上將大幅降低外，其最大的優點則在於建立動態兩端點私有化通道，以求在共享的共同介質上建立資料傳送，其效果亦相當於在專線上實施傳輸，並建立一個加、解密及認證機制，以同時達到「認證、存取、機密及完整性」之安全要件[3-4]。如圖二，虛擬私有網路示意圖。

二、VPN 通道資料加密

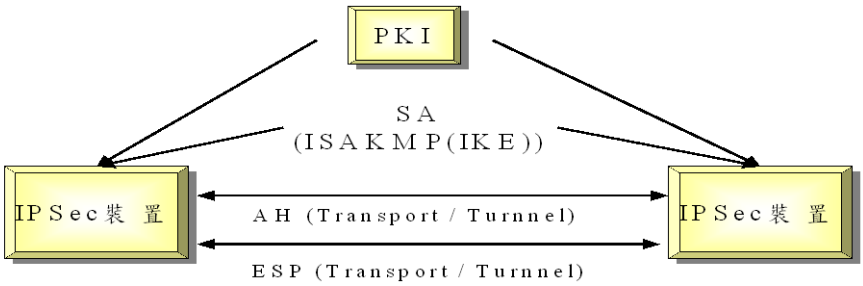
VPN 是利用 Internet IP 的技術，在 Internet 上建立一個加密通道(Tunneling)來架構網際網路上安全的網路環境，IP 網路的擴充性良好，所使用的加密技術是標準的 IPSec(IP Security)方式，IPSec 係結合了加密(Encryption)、認證(Authentication)、密鑰管理(Key Management)、數位檢定(Digital Certification)等相關安全保障，具有高度的資料私密保護能力，訊息資料的內容從傳送端到接收端都不會遭到修改，將可有效防制欲藉由對 IP 封包附加標頭所進行的各項攻擊，而其運用相關工具(技術)則包括：Authentication Header、Encapsulation Security Protocol，以及像是 MD-5 或 Secure Hash 等雜湊演算法，故廣泛應用於遠端使用者可於全世界各地利用公眾網路連接回企業公司內部網路，也讓全球運籌管理概念得以實現，並使資訊網路兼具開放、彈性與資料私密性之安全環境。



圖二 虛擬私有網路示意圖

肆、IP 安全協定（IPSec）

過去於制定 TCP/IP 之初壓根没有考量任何通訊安全機制，為因應 Internet 電子商務快速發展。IETF 始訂定 VPN 網路規範（RFC2401），IPSec（實際是應用於 IP 層上一組安全協定的通稱）係針對網路層中端點對端點所制定的安全通訊第三層協定，它主要的成員架構是以 IP 認證標頭(Authentication Header, AH)以及 IP 封裝安全承載(Encapsulating Security Payload, ESP)。IP AH 提供資料的「完整性」和「認證性」，而 IP ESP 原則上只提供「機密性」，但也可在 ESP Header 中訂定適當的演算法及模式來確保資料的完整性及認證性，IP AH 和 IP ESP 可以分開使用或一起使用。完整的 IPSec 還應包括 IP AH 和 ESP 中所使用金鑰的交換和管理，也就是安全群組(Security Association, SA)和金鑰管理 (Internet Key Exchange , IKE)，IPSec 相關技術架構，如圖三。現就依 IPSec 所屬成員逐一介紹：



圖三 IPSec相關技術架構圖

一、IPSec AH 協定

(一)IPSec AH 標頭

藉由 IPSec AH 主要可以認證原封包標頭是否遭受竄改，其位置置放於原封包標頭的後面，IPSec AH 標頭格式[1][3-4]，如圖四。

1.下一個標頭(Next Header)：標示 AH 標頭後面緊接的封包資料類型。

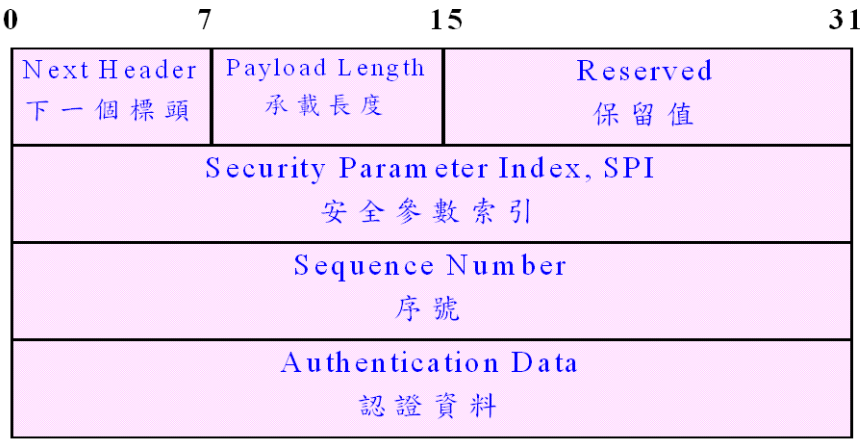
2.承載長度(Payload Length)：標示整個 AH 標頭欄位的長度。

3.保留值(Reserved)：為一 16 位元保留欄位供未來使用，目前設定為 0。

4.安全參數索引(Security Parameter Index, SPI)：代表通訊雙方事先協議完成安全關聯(SA)之索引值，主要可藉由「SPI、目的位址與安全協定」等欄位值作為索引並查詢相關安全參數，安全參數包括：協定操作模式（傳輸、通道模式）、加密演算法、加密金鑰及金鑰使用期限等。

5.序號(Sequence Number)：為一單調遞增的計數值，可防止重送攻擊（Replay Attack）。

6.認證資料(Authentication Data)：一個可變長度之欄位（必須為 32 位元的整數倍），存放原來 IP 封包標頭的「完整性檢查值」（Integrity Check Value, ICV），即 IP 封包標頭經過「雜湊訊息認證碼（HMAC）」識別演算法運算後的數值。

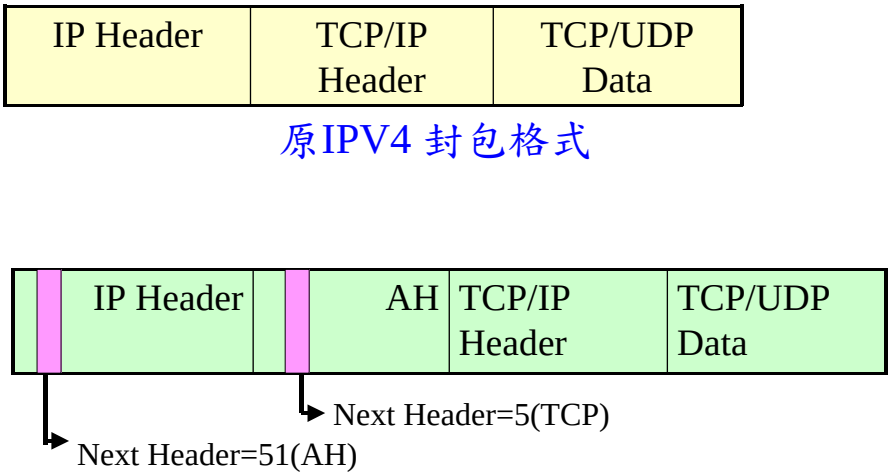


圖四 IPSec AH 標頭格式

(二)IPSec AH 操作模式

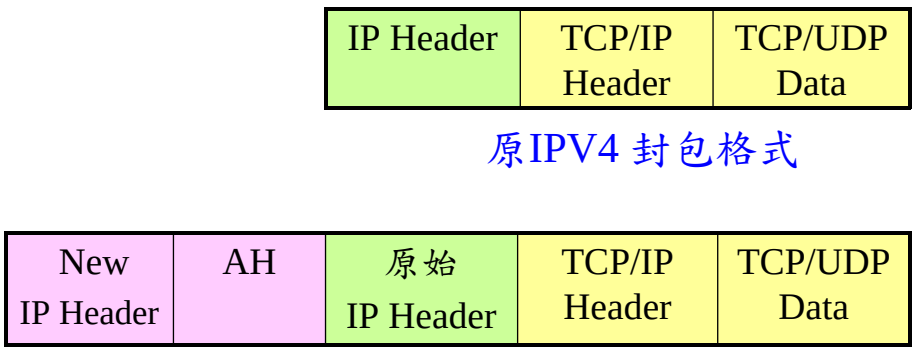
IPSec AH 協定可區分「傳輸模式」及「通道模式」兩種，其差別端賴於 AH 標頭置放的位置而有所不同。

1.AH 傳輸模式（Transport Mode）：將認證標頭置放於 IP 封包標頭與傳輸層協定（TCP/UDP）標頭之間，如圖五，IPV4 AH 傳輸模式封裝。但由於原 IP 封包所承載的封包協定欄位此時已更改為「AH」，故原 IP 封包「Protocol」應更改為「51」，本編號係由 IANA（Internet Assigned Numbers Authority）針對 AH 協定所訂定的協定編號，而 AH 標頭上「Next Header」欄位則應更改為原 IP 封包所承載的封包協定（如 TCP：5）。



圖五 IPV4 AH傳輸模式封裝

2.AH 通道模式（Tunnel Mode）：隱藏原 IP 標頭。另外製作一新封包標頭，利用 AH 標頭保護原來 IP 標頭，唯新、舊 IP 封包標頭內有關目的位址及來源位址將有所不同。圖六，IPV4 AH 通道模式封裝。



圖六 IPV4 AH通道模式封裝

(三)IPSec AH 運作模式

當傳送端送出資料後，為確保「正確性」與「認證性」，首先得依據 SA 值知悉所運用的演算法 AH 認證欄位，由傳送端選擇原 IP 封包標頭上某些欄位值，

並將這些數值經由「訊息認證碼」(Message Authentication Code ,MAC）演算法計算，產生「完整性檢查值」(ICV)，再將 ICV 值存放於 AH 標頭認證資料欄位(Authentication Data)，接收端收到 IPSec AH 封包後，亦選擇相同之欄位值計算 ICV 值，再比較傳送與接收雙方之 ICV 值是否相同，如兩者 ICV 值相同時，即代表該封包正確無誤，亦確保了資料的「正確性」與「認證性」。然值得注意的是在完成上述相關認證作業程序時，得事先協調對 ICV 加密密鑰、認證演算法、決定選擇那些原 IP 封包標頭（包括：版本、標頭長度、總長度、識別、通訊協定、來源位置、目的位址）欄位值拿來作為認證之依據，而這一切全然得事先藉由 SA 完成先前協商訂定，然而目前最常用的 MAC 演算法為 HMAC，主要是因為其可配合不同的雜湊演算法，如 MD5、SHA-1 等[3][5]。

二、IPSec ESP 協定

(一) IPSec ESP 標頭

IPSec ESP 主要是將原封包所承載的資料經過加密處理，再重新封裝一個新的封包（ESP）後，再傳送至接收端；俟接收端拆解 ESP 封包後，再將資料實施解密，予以組合恢復還原成原封包格式。故 IPSec ESP 兼具資料真確性與私密性之功能，但不提供「不可否認性」。另外，如果使用之演算法適切時亦同時兼具「驗證」之功能，ESP 標頭格式如圖七，其中 IPSec ESP 協定係以「SPI」與「Sequence Number」作為「ESP 標頭」，以「Pad Length」與「Next Header」作為「ESP 標尾」[3]。

1.安全參數索引(Security Parameter Index ,SPI)：傳送與接收雙方事先協議訂定之安全關聯(SA)索引值，其將配合目的位址及安全協定（AH 或 ESP 實施查詢）。

2.序號(Sequence Number)：為一單調遞增的計數值，可防止重送攻擊。

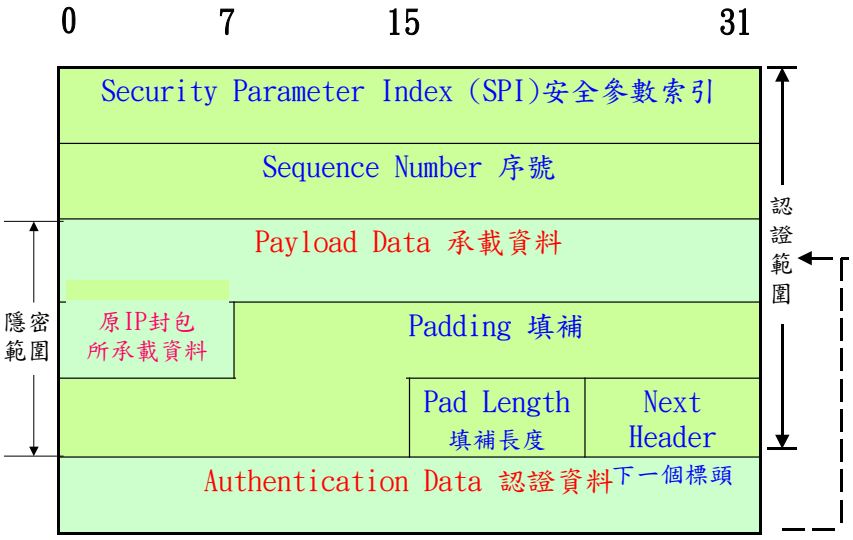
3.承載資料（Payload Data）:由 ESP 先將原 IP 封包所承載的資料（如 TCP/UDP），經某加密演算法計算後，存入該欄位。

4.填補（Padding）：作為資料是否為 32bits 長度之整數倍。

5.填補長度（Pad Length）：填補資料之長度。

6.下一個標頭(Next Header)：用以辨識封包內所承載資料之協定。

7.認證資料（Authentication Data）：存放「完整性檢查值（ICV）」，認證範圍由 SPI 到「Next Header」欄位，由雙方協議中之 SA 參數所訂定。

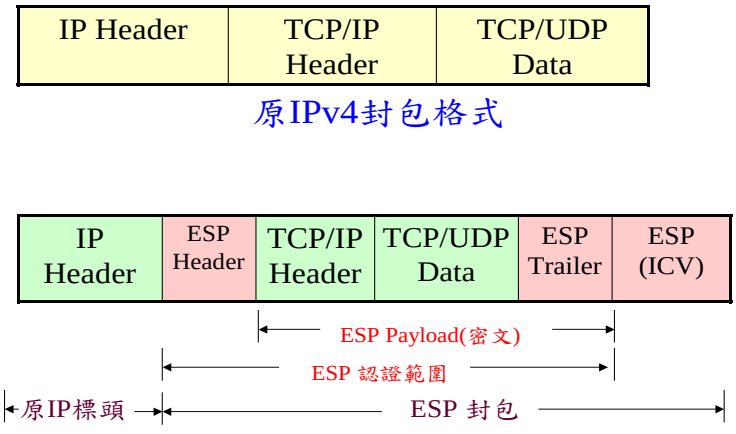


圖七 IPSec ESP 標頭格式

(二)IPSec ESP 操作模式

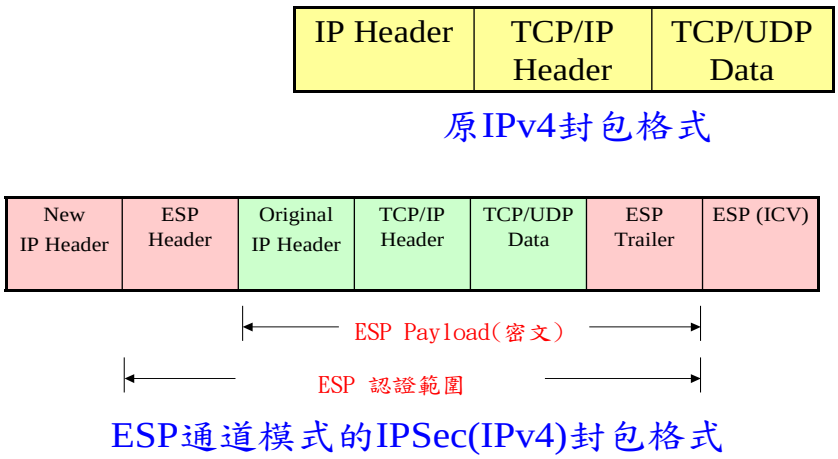
IPSec ESP 協定亦可區分「傳輸模式」及「通道模式」兩種，其分別在於 ESP 標頭所存放之位置，以及是否重新建立新封包而訂定。

1.ESP 傳輸模式（Transport Mode）：主要 是將 TCP/UDP 等上層協定予以封裝，不需對原本 IP header 作加密動作，也因此較不會浪費頻寬。ESP 標頭置放於 IP 封包標頭之後，並對原封包所承載的資料編碼加密後，再存放於 ESP 承載欄位上；再接續 ESP 標尾，最後才為 ESP 認證資料欄位，如圖八，IPV4 ESP 傳輸模式封裝。



圖八 IPV4 ESP傳輸模式封裝

2.ESP 通道模式（Tunnel Mode）：主將內部網路位址包裝在「內部標頭」之內隱藏起來，再將「外部標頭」設定為原來合法之 IP 位置，如圖九，IPV4 ESP 通道模式封裝。



圖九 IPV4 ESP 通道模式封裝

(三) IPSec ESP 運作模式

IP ESP 保密技術係採數據保密標準 DES（Data Encryption Standard）或是 Triple-DES 模式，DES 係為區塊加密法，每次加密處理資料單位採 64bits，金鑰長度訂定為 56bits，在加密演算法輸入部份由明文區塊與前一段加密區塊進行 XOR 運算，而每一區塊所使用的加密金鑰均相同。當 ESP 機制收到一個外送封包時，先由封包標頭某些欄位（目的位址、通訊協定、通信埠）作為搜尋關鍵，檢索 SPD 是否給予 IPSec 處理（確認 SPI 值）。若是，則利用 SPI 值關聯 SAD 資料庫尋得安全關聯（SA），若原先該系統尚未建立安全關聯（SA）時，則依 ISAKMP 協定建立起一個 SA 關聯。再依照 SA 參數執行 IPSec ESP 封包，其內容包括：安全協定（AH、ESP）、操作模式（傳輸模式、通道模式）、驗證演算法、編碼演算法、共享金鑰等[3-6]。

三、安全關聯(SA)

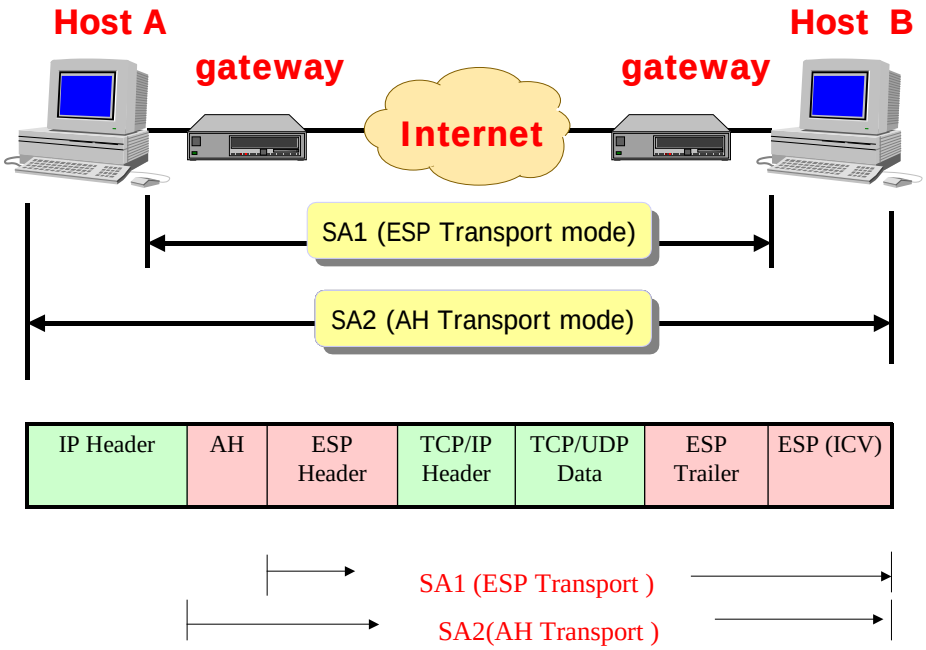
當傳送及接收端欲開始建立連線通訊時，彼此之間便須協商出一組共通的參數作為規範，此規範均具單向性及獨立性。而 SA 係為資料庫(SAD)中之某一筆記錄，登錄所需求之安全機制，包含：安全協定（AH、ESP）、操作模式（傳輸、通道模式）、認證演算法、加密系統等，每一筆 SA 記錄僅能描述一種通訊協定（如 AH、ESP 協定）；而每一通訊連線可能需要一個以上 SA 來描述其安

全機制時，即構成「安全關聯束」，並藉由「安全參數索引（SPI）」作為系統識別值[3-5]。

在 IPSec 協定中亦區分 AH 傳輸、AH 通道、ESP 傳輸、ESP 通道四種運作模式，每一種運作模式亦分別搭配不同的 SA 作為安全政策。組合方式可區分為兩種：

(一)傳輸串接

「傳輸串接」針對同一 IP 封包作多次傳輸模式之操作。如圖十所示，即外層之 SA 是利用 AH Transport 包裝，內層之 SA 則利用 ESP Transport 包裝，就整體封包結構即彷彿封包標頭串接。



圖十 「傳輸串接」組合模式

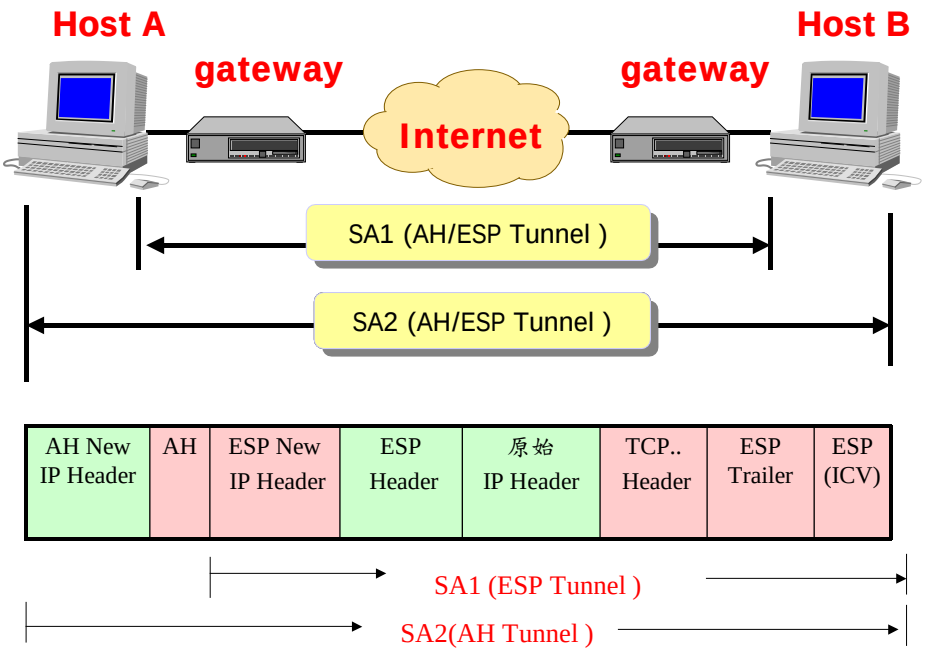
(二)反覆通道

「反覆通道」是利用多層次 IPSec 通道實施安全防護，由最外層包裝內層協定封包，如圖十一，即為反覆通道組合模式，由 SA2 採用 AH Tunnel 協定，內部安全關聯 SA1 為 ESP Tunnel 協定，內部安全協定主要藉由外部安全協定封裝。

四、ISAKMP 協定

網際網路安全關聯金鑰管理協定（ISAKMP）係為一安全性的基礎架構，主要在於建立、修改、刪除 SA，其中包含協議雙方的加密鑰匙、認證鑰匙及各種演算法。亦即為資料庫(SAD)中之某一筆記錄，登錄所需求之安全機制，但亦包含：安全協定（AH、ESP）、操作模式（傳輸、通道模式）、認證演算法、加密系統等。也由於為符合未來環境實際需求，由各不同之應用系統得以自行選擇

所需之金鑰交換協定，以及為克服未來新攻擊技術的產生，故 ISAKMP 則僅提供一個安全性的基礎架構，而不直接規範鑰匙交換程序。



圖十一 「反覆通道」組合模式

(一) ISAKMP 封包標頭

ISAKMP 封包以 UDP 協定（UDP：500）傳送，其內容除包含以一個封包標頭外，另亦包含若干筆 ISAKMP 承載，每一筆 ISAKMP 承載都是由承載標頭記錄所承載的訊息型態及承載資料所組成。如圖十二，ISAKMP 封包標頭。

1.發起者 Cookie：表示建立 SA、通知 SA、刪除的發起者，亦可防止「重送攻擊」。

2.回應者 Cookie：針對發起者 Cookie 作回應。

3.Next Payload(下一個承載)：表示緊接於標頭後方的第一個承載的型態。

4.Major Version(主要版本)、Minor Version(次要版本)：指定所使用 ISAKMP 主、次要版本。

5. Exchange Type（交換類型）：選用訊息交換類型。

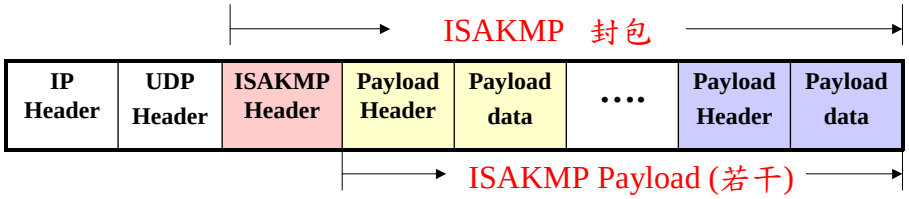
6.Flag（旗標）：標示後續連接的承載是否為密文和 ISAKMP 協商狀態。

7.Message ID（訊息 ID）：訊息識別碼，使 Responder 可依編號作回應。

8.Length（長度）：整串 ISAKMP 傳輸訊息的長度，即 Header+Payload 之總長度。

Initiator Cookie(1)				
Initiator Cookie(2)				
Responder Cookie(1)				
Responder Cookie(2)				
New **Payload**	Major	Minor	Exchange Type	Flags
Message ID				
Length				

ISAKMP封包標頭格式



IP 的ISAKMP封包包裝

圖十二 ISAKMP封包標頭

(二) ISAKMP 承載類型

ISAKMP 總計定義了 13 種承載類別，每種承載分別表示不同的特殊訊息，且 ISAKMP 協定即運用這些訊息作為協議雙方可以接受的安全機制。ISAKMP 承載類型，如表一。

表一 ISAKMP 承載類型

種類	參數	表示值	說明
安全連結承載(Security Association ,SA)	解釋區域、狀況	1	協調安全性之屬性，以及指定協商時所處的 DOI 與狀況
提案承載(Proposal ,P)	提案編號、提案 ID、SPI 大小、轉換個數、SPI	2	在 SA 的協調過程中，指定所採用的協定與轉換方式的個數
轉換承載(Transform ,T)	轉換編號、轉換 ID、SA 屬性	3	在 SA 的協調過程中，指定轉換方式及 SA 相關屬性
鑰匙交換承載(Key Exchange ,KE)	鑰匙交換資料	4	各種鑰匙交換技巧
身份標示承載 (Identification ,ID)	ID 類型、ID 資料	5	交換身份資訊
認證承載 (Certification ,CERT)	憑證編碼、憑證資料	6	傳送憑證及其他與憑證相關的資訊

憑證索取承載(Certification Request ,CR)	憑證類型個數、憑證類型、認證中心個數、認證中心	7	索取憑證，指定索取憑證類型
雜湊值承載(Hash)	雜湊值資料	8	由雜湊值函數所產生的資料
簽章承載(Signature ,SIG)	簽章資料	9	由數位簽章函數所產生的資料
臨時亂數承載(Nonce)	臨時亂數資料	10	臨時亂數
通知承載(Notification ,N)	DOI、提案 ID、SPI 大小、通知訊息類型、SPI、通知資料	11	傳送通知資料
刪除承載(Delete)	DOI、提案 ID、SPI 大小、SPI 個數、SPI(一個或多個)	12	指定某個 SA 為無效值
製造商標示承載 (Vender ,VID)	製造商編號	13	製造商標示承載

(二) ISAKMP 運作程序

ISAKMP 協定制訂溝通雙方建立連線時所需要的 SA，亦即透過 ISAKMP 協定的其他程序來管理 SA；然 SA 必須支援多種不同的加密演算法、認證演算法、及 Key 值建立演算法。通訊雙方欲建立通訊連線時，第一步驟先會互傳某些基本屬性以建立 SA，包含讓對方認證自己的資料與 Pre-Share Key 資料。用以確認對方身份並建立一安全通道。然而在確認身份認證方法有二：一為經由交換「未加密」的認證資料來確認對方之身分，然若因其 Key 選用不當，致易遭「暴力攻擊法」破解，故安全性較差；另一為利用「數位簽章」方式為基礎，由公正的第三者發出憑證，以確認對方身份，故可免受 man-in-the-middle 攻擊。當完成第一步驟雙方建立起一個安全通道後，接下來第二步驟則運用此一安全通道，進行 ESP 或 AH 所需 SA 資料交換，且此建立的安全通道，則可以重複利用，以進行多次 AH 或 ESP SA 資訊交換。其運作程序如下[1][3][6-7]：

1.先將建立起安全通道的資料放置於 ISAKMP Header 中的 I-Cookie 傳給 Responder。

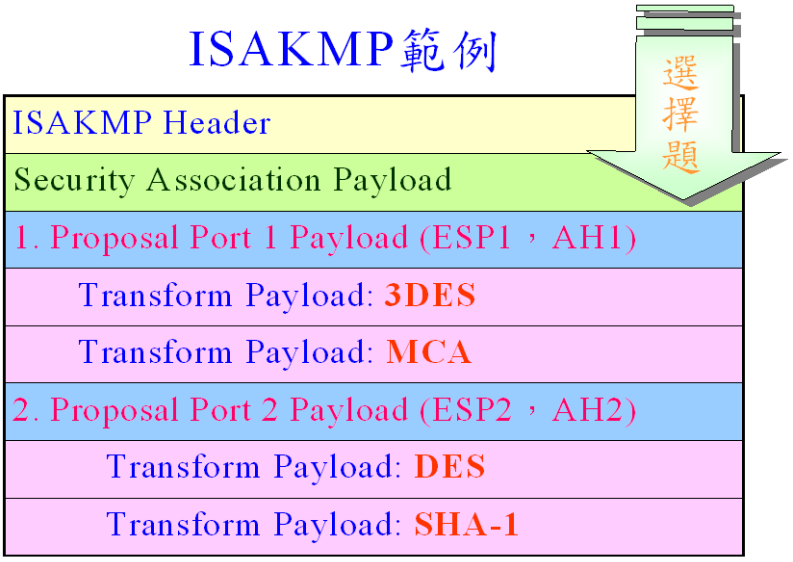
2. Responder 亦將資料傳送給 Initiator 所送來的資料，以確定無誤。

3.由 Initiator 將可用的 AH 或 ESP 演算法，進行金鑰產生演算法或傳遞時所需用到的相關參數製成「多組選擇題」，傳送給 Responder，如圖十三。

4.由 Responder 選擇其中一組參數，決定 AH、ESP、金鑰產生演算法後，

傳回 Initiator，並將這些參數存回 SA。

5.再次確定全部使用的參數。



圖十三 ISAKMP SA建置程序選擇(範例)

五、IKE 協定

「網際網路金鑰交換」(Internet Key Exchange ,IKE）乃將 Oakely 與 SKEME 兩個鑰匙交換協定結合於 ISAKMP 協定上，主因在 ISAKMP 協定僅訂定鑰匙交換的架構，而金鑰交換實作則實際交由 IKE 來實現。換言之，IKE 即是利用 ISAKMP SA 中與鑰匙交換相關的承載或交換型態，實際作為鑰匙交換的工作。然而 IPSec 內定的自動鑰匙管理協定即是為 ISAKMP/Oakley；而 ISAKMP 最早版本中所指定的鑰匙交換演算法即是 Oakley。

(一)IKE 特性

為配合 ISAKMP 協定運作，IKE 區分兩階段協商（包括：加密演算法、雜湊演算法、認證方法、Diffie-Hellman 演算法所需的訊息群組），第一階段協商建立安全通訊連線；第二階段執行鑰匙交換程序。

1.協商建立安全通訊連線：作為傳送與接收雙方協議安全機制外，還必須相互確認對方身份，在作法可以有「簽章認證」、「公開鑰匙認證」、「修正型公鑰認證」、「預定共享鑰匙認證」等方法。

2.執行鑰匙交換程序：傳送與接收雙方待完成第一階段後，可確認雙方身份，並協議出共享密鑰及加密、認證密鑰，並以此作為第二階段安全通道之建立。

(二) Oakely 金鑰產生

在 IKE 的協定上多半是以 Diffie-Hellman 演算法來產生會議鑰匙，Diffie-Hellman 演算法為一種對稱式金鑰加密法，為 Whitfield Diffie 及 Martin Hellman 所發明，用以溝通共同金鑰方式，其程序如下，如圖十四。

1.A 自行隨機產生 X_A。

2.B 自行隨機產生 X_B。

3.A 自行算出 $Y_A= \alpha^{X_A} \bmod q$，再將 Y_A 傳送給 B。

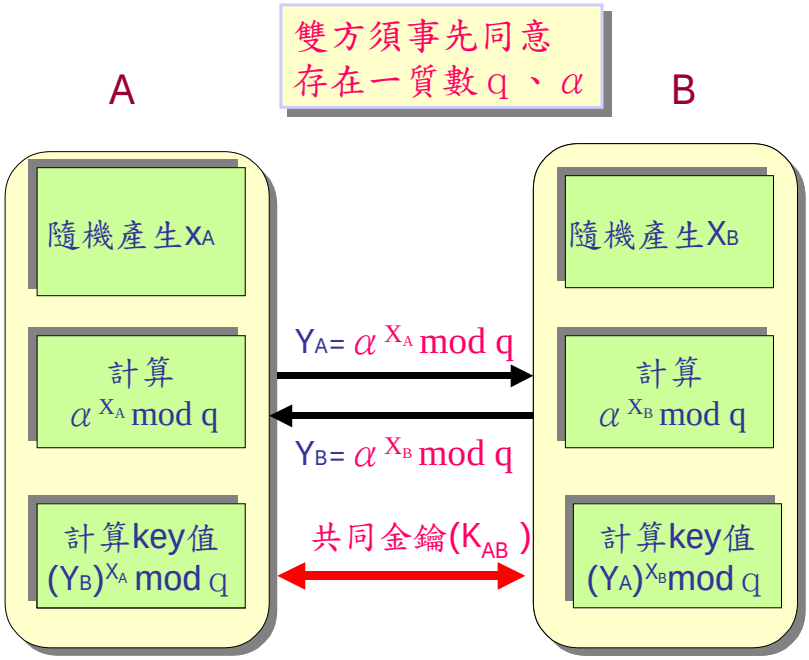
4. B 自行算出 $Y_B= \alpha^{X_B} \bmod q$，再將 Y_B 傳送給 A。

5.A 將 B 送來的 Y_B，再配合自己產生 X_A，計算出 K_{AB}。

6. B 將 A 送來的 Y_A，再配合自己產生 X_B，計算出 K_{AB}。

7. $K_{AB}=(Y_B)^{X_A} \bmod q =(Y_A)^{X_B} \bmod q$，而 K_{AB} 即為 A 及 B 共同產生的金鑰。

而 Oakely 即是 Diffie-Hellman 演算法的改良版，其主要是因為 Diffie-Hellman 演算法易遭中間人（man-in-the-middle）攻擊威脅，也就是 C 可能分別冒充 A(B)與 B(A)通訊，A 與 B 分別會與 C 協商一只鑰匙，而 C 再利用此鑰匙分別假冒 A 或 B 與對方通訊，C 進而從 A 與 B 的通訊中從中攔截，並加以更改訊息內容，然 A 與 B 卻可能混然不知。

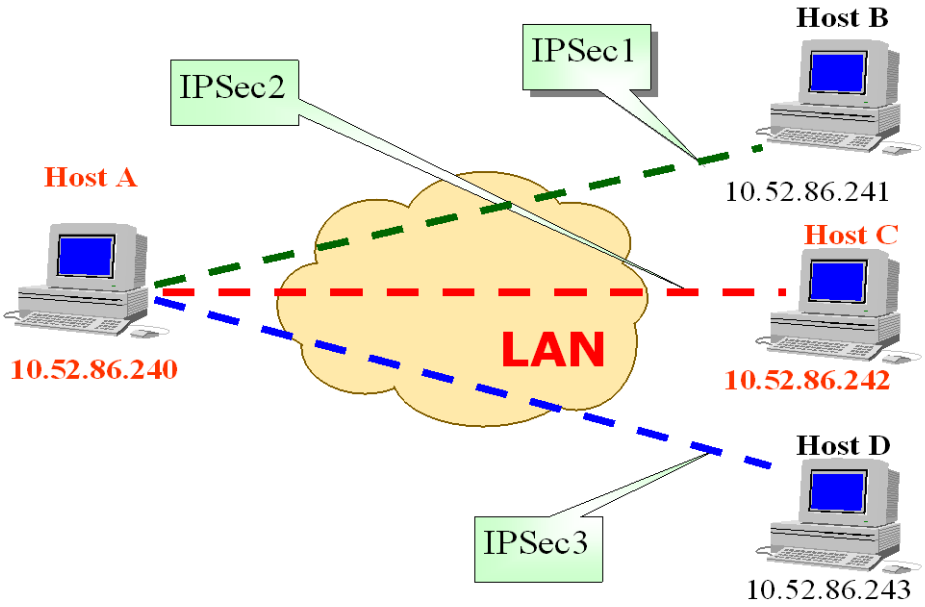


圖十四 Diffie-Hellman演算法

伍、IPSec 實作

IPSec 機制已於 Windows2000 作業系統中實作，系統使用者可以依資訊的敏感性（機敏性）或傳輸媒介的相對弱點，以及特定等級加密模組的輸出限制，

以指定符合相對的 IPSec 設定或屬性予以對應，在實作中每一組 IPSec 之屬性設定被視為「安全性原則」，其被建構於相關的協商原則與 IP 篩選器上，現即以簡易點對點安全連線模式實施介紹[8]，如圖十五，系統實作架構圖，其執行程序如下：



圖十五 IPSec實作系統架構

(一)首先設定管理 IP 篩選器清單和篩選器動作；管理 IP 篩選器清單步驟：

1.開啟 Host A 程式集中的「本機安全性原則」，操作步驟：開始→程式集→系統管理工具→本機安全性原則。

2. 選擇本機電腦上的的 IP 安全性原則，並在右邊的視框空白處按滑鼠右鍵，選擇管理 IP 篩選器清單和篩選器動作。

3.點選「管理 IP 篩選器清單」，再按「新增」。

4.輸入 IP 篩選器的名稱，再按「新增」。

5.出現篩選器精靈，按「下一步」。

6.目的地位址，請選擇「特定 IP 位址」，再按「下一步」。

7.輸入與此台電腦作通聯的特定 IP 位址，再按「下一步」；IP 通訊協定類型選擇任一，不勾選編輯內容，即按「完成」。

8.完成後，可以在 IP 篩選清單中看到新增的選項。

(二)設定篩選器動作

1.選擇管理篩選器動作，並按「新增」。

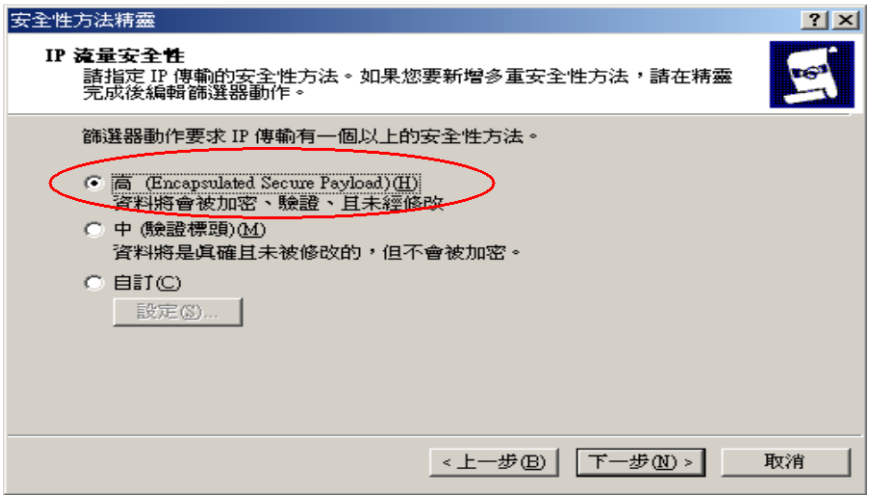
2.出現篩選器動作精靈，按「下一步」，再輸入篩選器動作名稱，再按「下

一步」。

3.選擇「交涉安全性」，再按「下一步」。

4.只允許與支援 IPSec 的電腦進行通訊，以確保通訊安全，再按「下一步」。

5.因為我們希望進行高安全性的 IP 傳輸方法，故可以選擇高安全的加密方式，再按「下一步」，如圖十六。



圖十六 IP篩選器安全性方法選擇

6.將編輯內容勾選起來以利以後實施編輯修改，再按「完成」。

7.完成後可以看到新增的篩選器動作的內容，可以按「編輯」實施修改。

8.完成管理篩選器動作設定。

(三)建立安全性原則：

1. 選擇本機電腦上的的 IP 安全性原則，並在右邊的視框空白處按滑鼠右鍵，選擇「建立安全性原則」。

2. 進入「IP 安全性原則精靈」，按「下一步」。

3. 輸入安全性原則的名稱，再按「下一步」。

4.不使用預設的回應規則，再按「下一步」。

5.請將編輯內容勾選起來以利以後實施編輯修改，按「完成」。

6.按新增建立一個 IP 安全性規則。

7.進入安全性規則精靈，按「下一步」。

8.選擇不使用通道來做 IPSec，再按「下一步」。

9.依實際線路選擇網路通訊類型，再按「下一步」。

10.透過 window 2000 做認證，故選擇預設值。

11.選擇建立的 IP 篩選器清單。

12.選取設定好的篩選器動作。

13.請將編輯內容勾選起來以利之後再做編輯修改，再按「完成」。

14.可看見設定好的 IP 安全性原則。

15.可看見設定好的本機電腦上的 IP 安全性原則。

16.設定設定好的原則為指定的狀態，在設定好的 IP 安全性原則上按滑鼠右鍵，選取「指派」。

(四)系統驗證

待 Host B、C、D 亦完成分別與 Host A 相對應建立之 IPSec 通道時，其相關程序亦如上所述，隨即便得以"Ping"指令分別予以驗證系統是否相通。然若啟動「IP 安全性監視器」時，將可以提供已建立的「安全性關聯」及「IPSec 統計」與「ISAKMP/Oakley」統計資訊，供系統使用者進階參考。

陸、結論

隨著各項通資安全議題廣泛地受到重視，在整體通資安全發展亦多朝向「整合性」防護發展，然強調如何利用各種資安技術以抵擋多數通信情資免於受制駭客的竊取與破壞確保其安全性，更是國軍整體資訊發展最重要的一環。但我們必須確認天下間無所謂「絕對安全」，在維護情資安全考量前提下，至少必須達至兩項要求標準，一則「破解密文所需的成本超過被加密訊息本身的價值」，二則「破解密文所需的時間遠超過這個密碼的有效壽期」，此亦為通資三大要求「迅速、確實、安全」中，何以「安全」最為重要的主要原因。

IPSec 協定相關技術包含加密、認證、存取控制、私密性、完整性、身分認證、防止重送等功能，又因其核心技術函蓋「加密」與「認證」等密碼學機制，再加上協定本身建架於 IP 層，可廣泛應用於傳輸層以上階層使用，故可期待於國軍未來資訊安全實務上，亦不失為一項可供考量運用的方法之一。

註釋

1. Stallings, W., Cryptography and Network Security, Second Edition, Prentice Hall International, Inc.,1999.

2.陳彥學，資訊安全理論與實務(台北：文魁資訊公司，2000)。

3.粘添壽，吳順裕，資訊與網路安全技術(台北：旗標，2004)。

4.懷恩等，「網際網路安全協定 IPSec 技術探討」，電腦與通訊，第 74 期(台北， 1998 年 11 月) 。

5.高笙庭，「利用 IPSec 達成封包傳輸隱匿之目的」，國立台灣大學資訊工程研究

所 88 年碩士班論文。
6.羅濟群等，「虛擬私有網路簡介及其應用」，資訊安全通訊，第五卷第三期（台北，1999 年 6 月）。
7.楊慶隆，IPSec 機制探討，網路通訊（台北，1999 年 8 月）。
8. Jan Mclean 著，安人玉，廖穎芝譯，Windows2000 網路安全深度探索(台北：旗標，2001 年)。