第十二章 虛擬私有網路 - IPSec

『重兵部署各地關口，進可攻、退可守』、『縱橫面、垂直線聯合作戰』；此為國際商場的大戰略，之間聯絡網即是『虛擬私有網路』。

12-1 虛擬私有網路簡介

『虛擬私有網路』(Virtual Private Network, VPN) 是網路安全另一個重要的措施，概括而言，它是希望在不安全的『公眾網路』(Public Network) 上建立一個具安全性較高的『私有網路』。然為何稱之為『虛擬』？是因安全網路是利用軟體或硬體附加在原本不安全網路上，可隨時依其需要建立一個安全通道，使用完畢之後，該安全連線立即消失，並未改變原來的網路架構，故而稱之。

目前所指『公眾網路』大多以 Internet 網路為代表，其組成是經由一些不相干的網路連結而成，網路之間並無特別的管理機制，任何人不經授權都可以自由存取網路上所提供的資源。所以公眾網路的管理既鬆散又不安全，所傳輸的資料除了不具保密性之外，也不保證可以安全到達目的地。一般所指『私有網路』皆是屬於機關行號自行建構的網路，此網路大多僅提供組織內的需求，如工廠自動化、電子化辦公室等等。私有網路內所傳輸的資料較具機密性，多半不願意給外人知曉，因此，私有網路必須經過特殊保護其安全性，且不輕易與外界網路相連。

當公司規模還不是很大時，私有網路大多只侷限於某一區域內，因此只要利用防火牆管制公眾網路與私有網路之間的通訊即可。一旦公司組織擴充至全球各地時，如何結合各地分屬機構網路成為一個安全性較高的私有網路，則非仰賴『虛擬私有網路』技術不可。早期私有網路上大多僅提供檔案伺服功能，應用系統多侷限於 NetBEUI 上開發，譬如，Novel Netware 或 Microsoft Network 等『區域網路作業系統』(NOS)，此時建構的防火牆只要將 NetBEUI 過濾掉，避免跨越防火牆到公眾網路，即可達到內部網路的防護功能，倘若需要建構 VPN 時，也只需將 NetBEUI 訊框經過包裝後，再經由公眾網路傳遞到另一個私有網路即可，比較典型的 VPN 技術為『點對點通道協定』(Point-To-Point Tunneling Protocol, PPTP) 與『第二層通道協定』(Layer 2 Tunneling

Protocol, L2TP)【注意：上述兩協定也可以封裝轉送 IP、IPX、X.25、Frame Relay、ATM 協定】。

近幾年來，許多私有網路已將應用系統轉移到 TCP/IP 協定上，也就是將 Internet 的連結技術應用到一般的電子化辦公室裡，客戶端只需使用瀏覽器（Web-based）便可處理一般事務，這就是所謂的『網域內網路』(Intranet)。如此說來，公眾網路與私有網路已使用同樣的通訊協定（TCP/IP），之間的連結效率會比原來包裝（如 PPTP）後再傳送還高。另外，目前很多公司的分屬機構散落全球各地，出差人員必須隨時繞著地球跑，且必須和總公司或各分公司隨時保持連絡，擷取所需的資料（通常具機密性），如果網路上還是利用安全性較低的 TCP/IP 協定，那幾乎是不可行的。因此，需仰賴安全性較高的 IP 協定，這就是所謂的『IP 安全協定』(IP Security Protocol, IPSec)。本書將利用三個章節分別介紹如何利用 IPSec 協定，建立虛擬私有網路的相關技術；首先本章介紹 IPSec 協定的運作程序，第十六章再介紹協議安全機制的 ISAKMP 協定，最後於第十七章介紹如何建立通訊實體之間會議金鑰的 IKE 協定。

12-2 VPN 網路型態

簡而言之，整合各地的區域網路成為一個安全性較高的網路系統，即為『虛擬私有網路』的基本概念。隨著時代的變遷，虛擬私有網路主要有兩種基本型態：WAN-VPN 架構與 Internet-VPN 架構。

12-2-1 WAN-VPN 架構

欲連結各地區域網路成為一個安全性較高的私有網路，最簡單的方法就是向電信公司（如中華電信公司）承租『專線』連接（或稱專屬鏈路），此種網路型態稱之為『廣域網路的虛擬私有網路』(WAN-VPN)，如圖 12-1 所示。基本上，電信公司只提供固定連線，沒有路徑選擇功能，並依照傳輸速率與連線距離計費，傳輸速率可介於 64 Kbits 至數百 Gbits 之間。計費方式與傳輸量無關，完全依照傳輸速率與距離計算月租費，如果傳輸距離較近（如圖 12-1，網路之間的地理位置），費率尚可接受，一旦距離過遠（如台北與高雄之間），則月租費已貴得嚇人，更何況跨越國際之間，那幾乎是不可行。再說，WAN-VPN 僅侷限於事先固定的地理位置之間傳輸訊息，無法隨時移動位置。換句話說，

出差人員所到達的地方，除非是架設 VPN 的地區，否則無法與原公司的私有網路通訊。早期為了克服這個問題，大多利用電話撥接來達成，但電話網路傳輸速率慢，而且電話費也很貴，並不完美。由此可見，WAN-VPN 已無法滿足目前國際化的商業環境使用。

但話說回來，WAN-VPN 專屬網路的安全性最高，因為與外界網路完全隔離，閒雜人等不易入侵。因此，WAN-VPN 無需特殊的防護設施，其應用範圍也多侷限於安全防護要求較高的組織單位，如國防部軍事管理的網路系統。

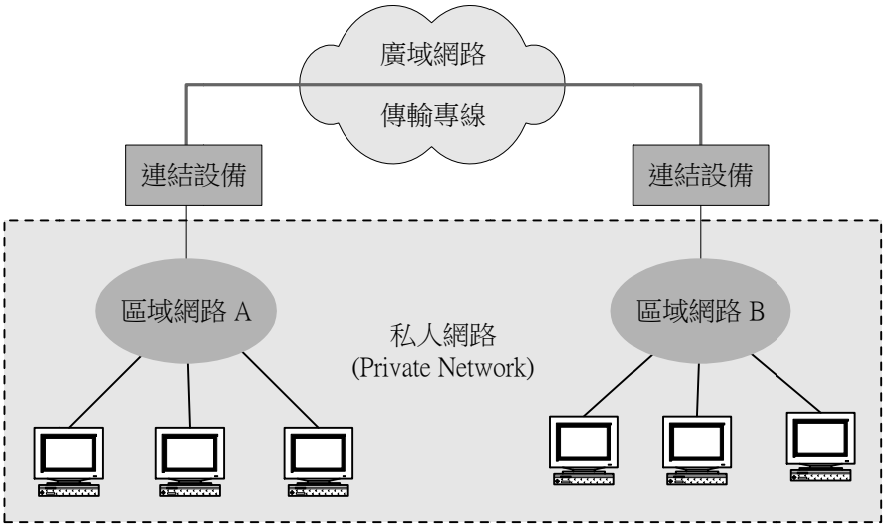

圖 12-1 WAN-VPN 網路型態

其實 WAN-VPN 網路在市場上已使用了不算短的時日，早期 Internet 網路尚未流行時，各公司行號只能向電信公司承租專線連接，但礙於費用高，租用的傳輸速率都不會太高。目前專屬連線大多使用於距離較近的區域網路，或是私有網路與 ISP 機房之間的連線（大都會網路連接）。

12-2-2 Internet-VPN 架構

如前所述，承租沒有路由功能的專線不但價格昂貴，而且也受限於架設位置。"俗擱大碗"乃是一般人們所欲追求的目標，目前盛行於全球的 Internet 可說是不二人選。利用 Internet 建構 VPN 網路，不但價格便宜，還可藉 Internet 網路的路由功能，將訊息傳送到世界上任何角落，如此一來，所連結的私有網路就不再受地理位置所限。圖 12-2 是利用 Internet 網路所架設的 VPN，可稱之為『Internet-VPN 架構』。在 Internet-VPN 網路之下，區域網路之間是利用公眾網路來連接，之間傳輸訊息須經過多個路由器所建立的『虛擬鏈路』轉送，如果沒有特殊處理，其安全性值得堪虞。我們簡單說明一下它的

傳送方式，假設區域網路 A 某一工作站欲連結到區域網路 B 內的工作站，當它將封包（IP 封包）送到 Internet 網路上時，該封包便依照目的位址尋找可到達的路徑，一個網路跨越到另一網路，必須經由許多路由器的轉送才到達區域網路 B，因此，資料在 Internet 網路上傳送時，任何一個網路端點都可竊取或竄改其內容，所以可靠度非常的低，這正是我們發展『IP 安全協定』（IP Security, IPSec）的主要原因。

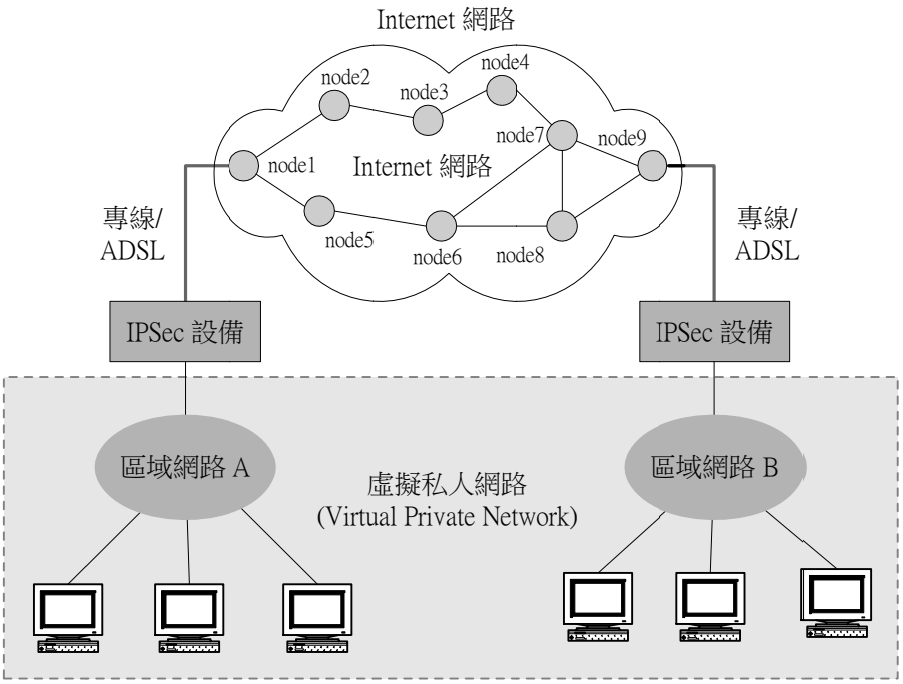

圖 12-2 Internet-VPN 網路型態

有一個簡單的做法，只要將圖 12-2 中私有網路對外連接的設備，改換成具有 IPSec 功能的連結設備，就可以達到虛擬私有網路的功能，此連結設備即稱為『安全閘門』（Secuirty Gateway, SG）。如圖 12-2 的 VPN 網路成員（雙方的 SG 閘門），必須協議雙方可能採用的安全套件（包含『鑰匙』）。其中某一網路有訊息欲傳送到另一網路時，當 SG 閘門收到封包後，則將該封包加入安全措施並重新包裝，譬如訊息加密或認證的處理，之後再將新的封包發送到 Internet 網路上；另一方的 SG 閘門收到封包後，則依照雙方之前所協議的安全套件，將封包回復原來格式，再發送給內部的私有網路。私有網路內工作站發送訊息給另一個工作站時，則不需考慮該工作站是否在本區域網路或其他網路上。攻擊者不了解安全套件內容，或沒有雙方協議的『鑰匙』，也無法盜取或偽造訊息內容。

如此一來，我們只要承租較便宜的傳輸線路將私有網路連結到公眾網路上，就可以

達成安全性較高的私有網路連結。一般規模較小的公司行號只要承租 ADSL 傳輸線路即可，即使承租的傳輸速率在 3 Mbits 以上也不會太貴；至於較大的組織單位可以租用最近距離之 ISP 公司的專線，雖然費率較貴一點，但總比遠距離的專線便宜許多。

12-2-3 防火牆與 VPN 架構

但話說回來，VPN 是藉由 Internet 網路所構成，意指內部網路可能會暴露於 Internet 網路上；攻擊者可能會透過公眾網路來入侵私有網路，因此一般 VPN 網路都必須配合防火牆裝置，圖 12-3 是一個典型的網路架構。VPN 設備大多安裝在外部路由器上，所以外部路由器除了具備原來封包過濾的功能外，還具備 VPN 的處理能力。譬如，區域網路 A 的使用者想要和區域網路 B 的工作站通訊，它的 IP 封包經由外部路由器（具有 VPN 功能）處理後，再傳送到 Internet 網路上；當區域網路 B 的外部路由器（具有 VPN 功能）收到該封包後，經過適當處理後再轉送給內部網路。另一方面，區域網路如想要和 Internet 上的其他網路通訊，雖不經由 VPN 處理，但也需要依照其安全政策由外部路由器過濾，或經由防禦主機來代理轉送，如此需結合防火牆和 VPN 的功能。也就是說，內部使用者可以選擇是否透過 VPN 處理和外部通訊，VPN 設備也需分辨出所進入的封包是否有經過 VPN 處理，如果有，則表示來自其他所屬機構網路的封包；否則可能是一般外部使用者的訊息。

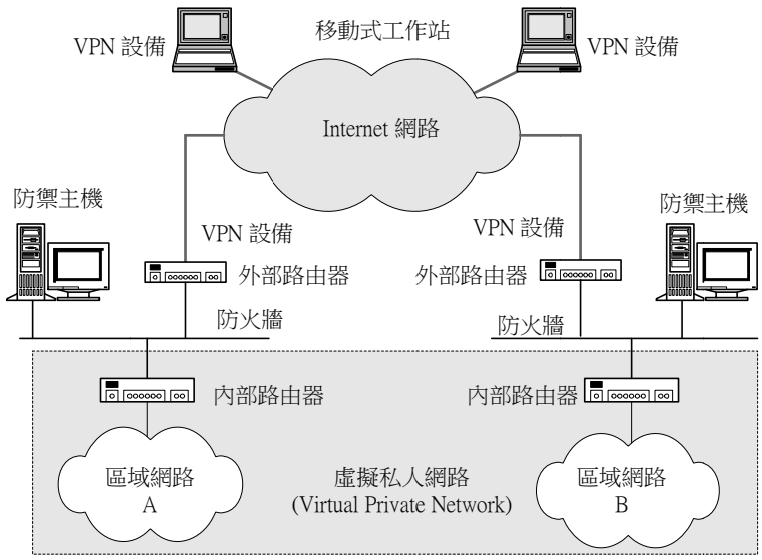

圖 12-3 防火牆型之 VPN 網路

Internet-VPN 的另一個重要功能是，許多出差人員或 SOHO 工作人員在外，可能

需要連結到公司的私有網路來存取資源，但此類人員所使用的電腦大多屬於客戶端功能，我們只要在其電腦上安裝 VPN 軟體，就可以透過 Internet，並以 VPN 方式連結到公司內部網路。由圖 12-3 可以發現，不管是區域網路 A 或 B，還是移動式工作站的位置，並不限制其地理位置，只要 Internet 可以到達的地方，都可以建立 VPN 網路，完全合乎企業全球化的需求，至於圖 12-3 的 VPN 設備，目前大多是指具有 IPSec 功能的路由器或主機設備。

12-3 IP 安全協定

12-3-1 IPSec 協定簡介

『IP 安全協定』(IP Security Protocol, IPSec)是 ITEF(Internet Engineering Task Force) 特別對 VPN 網路所制定的規範 RFC 2401，亦分別對 IPv4 (IP Version 4) 與 IPv6 (IP Version 6) 兩個版本制定規範，在此我們會分別介紹之。

在 Internet 網路上，除了 ARP 與 RARP 有獨立的封包傳輸外，其它通訊協定(如 TCP、UDP、ICMP、IGMP) 皆是以 IP 封包來傳送。也就是說，這些通訊協定都是經過 IP 封包封裝後，再以 IP 協定在網路上傳輸。傳送端發送 IP 封包時，並無法預估該封包會經過那些路徑，其間需透過網路上一個接一個路由器轉送始可到達目的地。轉送過程中，每一個路由器收到封包後，由封包上讀取該封包上所註明的目的位址，並尋找可能到達的路徑再傳送出去。如此一來，IP 封包內所承載的訊息很容易被有心人士窺視，或是偽造另一個封包傳送給接收端。由此可見，利用 IP 協定來傳輸資料是非常不可靠的。另一方面，既然所有通訊協定都是利用 IP 協定來傳輸，只要我們能將不可靠的 IP 傳輸，經過安全性機制處理之後，使所承載的任何協定就可達到安全性的保護，換言之，經由 IPSec 協定傳輸的任何應用系統，都可以達到安全性的需求，由此可見，IPSec 協定是解決 Internet 網路上安全性需求的根本之道。

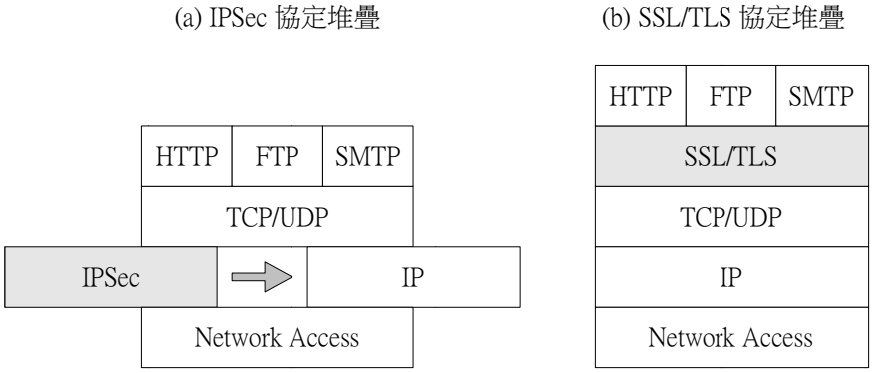

圖 12-4 IPSec 與 SSL/TLS 協定堆疊

圖 12-4 (a) 為 IPSec 的協定堆疊，只要將不可靠的 IP 協定轉換成具有安全性的 IPSec；如此一來，透過 IPSec 協定所傳輸的訊息，就可以達到安全性目的。除了 IPSec 安全協定之外，其他安全協定大多屬於 TCP/UDP 協定層次，如 SSL 或 TLS 協定，其協定堆疊如圖 12-4 (b) 所示。這類協定並不修改 IP 協定，它只針對通訊中某筆訊息（TCP 連線）做安全性的保護，保護措施大多是短暫的，對於與陌生人通訊方面比較方便，因此大多使用於電子商務的應用上，兩者的應用有很大的區別（請參考第十一章說明）。

12-3-2 IPSec 相關技術

談到『安全性』(Security) 總是離不開兩個主題，一則為『加密』，其目的是要保持資料的隱密性，讓他人無法窺視資料的內容；另一則為『認證』，是驗證通訊中的對方身份，是否遭受他人冒名頂替。為了達到上述目的，還是必須仰賴密碼學中加解密演算法，這又牽涉到交換鑰匙的問題。圖 12-5 為 IPSec 的相關技術，我們在這裡先概略性的介紹，讓讀者有一個簡單的概念，接下來再詳細介紹，如此可讓讀者較易進入狀況。

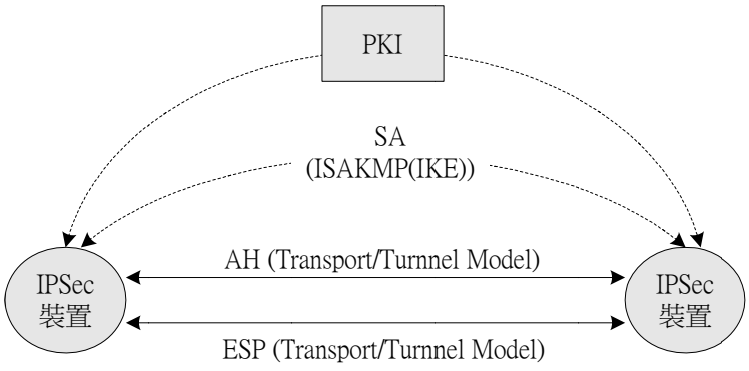

圖 12-5 IPSec 相關技術

由圖 12-5 中，可將 IPSec 相關技術歸納如下：

(1) IPSec 裝置（IPSec Device）：安裝有 IPSec 協定的設備者稱之（或可從事 VPN 功能的設備），它不僅是一個安全裝置，還可以代表一個使用者個體、使用者群組、或組織單位（具有身分憑證）。一般 IPSec 裝置設備可分為下列兩種：

- 『安全主機』（Security Host, SH）：主機安裝有安全協定者稱之，但必須提供傳輸與通道模式等兩種操作模式（容後介紹）。
- 『安全閘門』（Security Gateway, SG）：路由器安裝有 IPSec 協定者稱之。因為 SG 充當內部網路與外部網路之間的進出閘門，因此，僅提供通道模式。如果使用傳輸模式的話，僅能使用於網路管理協定（如 SNMP 協定）。

(2) 安全關聯（Security Association, SA）：規範通訊實體之間的安全政策，以及某一安全政策之下的相關安全參數，譬如，兩通訊實體之間的安全協定（AH 或 ESP）、封包模式（傳輸模式或通道模式）、以及加密演算法等等。

(3) 網際網路安全關聯金鑰管理協定（Internet Security Association Key Management Protocol, ISAKMP）：通訊實體之間係利用 ISAKMP 協定協調及建立所需的 SA，其協議內容包含安全協定、加密演算法、或認證演算法等等。

(4) 『網際網路金鑰交換』（Internet Key Exchange, IKE）：當雙方利用 ISAKMP 協議出所欲採用演算法之後，還必須協議出雙方的會議金鑰，此鑰匙可能使用於加密或認證系統。IPSec 為了使 ISAKMP 能符合各種環境需求，並不固定某一特定的金鑰交換協定，而由另一個 Internet 網路上較普遍的 IKE 協定來完成。

(5) 公鑰基礎架構（Public Key Infrastructure, PKI）：PKI 發給每一個 IPSec 身份驗證的數位憑證，作為進入 VPN 網路的身份證明，其中包含個體的公鑰（Public Key）與私鑰（Private Key）。通訊實體之間就是利用 PKI 所發給的鑰匙互相確認身分，並交換鑰匙材料以建立會議金鑰。相關技術請參考第九章介紹。

(6) 認證標頭（Authentication Header, AH）：認證標頭是 IPSec 的兩種安全協定之一。IPSec AH 主要認證封包標頭是否有遭受竄改或偽裝，其中有『傳輸模式』與『通道模式』兩種封包模式。

(7) 封裝安全承載（Encapsulation Security Payload, ESP）：ESP 是 IPSec 的另一個安全協定。IPSec ESP 將原 IP 封包經過加密後，重新封裝成另一個 IP 封包，以達到資料隱密性的功能，同樣也有『傳輸模式』與『通道模式』兩種封包模式。

(8) 操作模式（Operating Mode）：IPSec 協定有『傳輸模式』（Transport Mode）與『通道模式』（Tunnel Mode）兩種操作模式，無論 AH 或 ESP 協定都可以使用這兩種操作模式來傳輸訊息；因此，IPsec 協定有四種訊息封包格式，如圖 12-6 所示。

(9) 演算法（Algorithm）：無論認證（Authentication）或加密（Encryption）都需要相對應的演算法。基本上，IPSec 並不規定標準演算法，而是雙方利用 ISAKMP 協定協議而成。

	IPSec AH	IPSec ESP
Transport Mode	AH with Transport Mode	ESP with Transport Mode
Tunnel Mode	AH with Tunnel Mode	ESP with Tunnel Mode

圖 12-6 操作模式

12-3-3 IPSec 運作概念

有了上述相關技術之後，接著來探討它們之間的關聯性，如此可讓讀者稍微瞭解 IPSec 的運作概念，至於詳細的運作程序將會在相關協定中說明，簡述如下：

- IPSec 協定包含 IPSec AH 與 IPsec ESP 兩種安全協定，這兩種安全協定都有傳輸模式和通道模式等兩種封包格式；
- 至於通訊雙方是要採用何種安全協定及封包格式？視安全關聯（SA）的規範而定；
- 如何制定 SA 的安全規範？係由通訊雙方利用 ISAKMP 協定所協議完成的；
- 在 ISAKMP 協議當中若需交換鑰匙作為身份確定或制定會議金鑰，可利用 IKE 協定來完成；
- 在雙方認證身分或交換鑰匙時，必須有代表身份的公鑰，然而此公鑰可由 PKI 系統中的憑證授權（CA）中心發給。

乍看之下，IPSec 好像很複雜的樣子，這是因為它必須結合許多安全措施（如 PKI、

ISAKMP、IKE）才能達成。在此假設每一參與 VPN 運作者都已取得數位憑證（有關憑證認證與身份識別的議題，請參考第七、八章介紹）。首先介紹 AH 與 ESP 安全協定的運作程序，接著再介紹 SA 的安全參數；至於如何利用 ISAKMP 協定建立 SA，將保留在第十六章介紹；第十七章再介紹建立會議金鑰的 IKE 協定。

12-4 IPSec AH 協定

『認證標頭』（Authentication Header, AH）是 IPSec 最基本的安全協定，它是針對 IP 封包標頭做安全認證，提供有『非連接導向的完整性』、『資料來源認證』、以及『反重播』等保護服務（12-6-1 節介紹）。另外 AH 並未對所承載的資料作任何保護，基本上，IP 封包在 Internet 網路上，乃經由路由器（或網路閘門）層層轉送才會到達目的地，每經過一個路由器轉送時，路由器便拆解該封包的標頭，根據標頭上所標示的目的位址，繼續往下一個路徑傳送；當然每一路由器都會重新包裝該封包，並製作新的封包標頭，所以有心人士非常容易去竄改封包標頭，或從事重播攻擊的行為。AH 的功能是對 IP 封包提供認證，確保遭受竄改的封包可以被偵測出來。

AH 使用密碼學的『訊息認證碼』（Message Authentication Code, MAC）來認證 IP 封包標頭。簡單的說，傳送端將 IP 封包標頭經過雜湊演算法得到一個訊息摘要（Message Digest, MD），再將此訊息摘要經過秘密金鑰加密，得到一個 MAC 碼，最後將此 MAC 碼（製作 AH 標頭）與 IP 封包一併傳送給接收端；接收端收到此封包後，以同樣的演算法與秘密金鑰產生另一個 MAC 碼。如果兩者 MAC 碼相同的話，表示封包未遭受竄改或偽造；否則需拋棄此封包。目前最常用的 MAC 演算法是 HMAC（Hash Message Authentication Code），主要原因是，它可以配合不同的雜湊演算法，譬如，MD5、SHA-1、RIPEMD-160 或 Tiger 等雜湊函數。另外加密時所需的秘密金鑰是在安全關聯（SA）裡所制定，在此暫時不去討論它如何產生。

12-4-1 AH 標頭格式

認證標頭（AH）是 IPSec AH 協定所產生的一個新認證標頭，主要功能是認證原封包標頭是否遭受竄改，並將它置放於原封包標頭的後面。AH 標頭包含五個固定長度的欄位和一個不定長度的認證資料欄位，如圖 12-7 所示，各欄位功能如下：

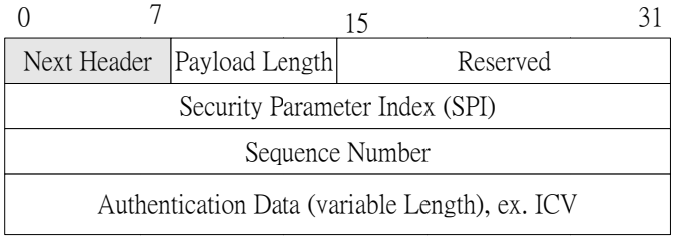

圖 12-7 認證標頭格式

- 下一個標頭(Next Header, NH): 8 位元欄位。標示 AH 標頭後面緊接著的封包格式。各種通訊協定的編號是由 IANA (Internet Assigned Numbers Authority) 所制定 (RFC 1700)，譬如，TCP 封包為 6；IP 包裝的 IP 封包是 4。如果後面緊接著 ESP 標頭，則為 50，而 AH 的編號是 51。

- 承載長度 (Payload Length): 8 位元欄位。表示整個 AH 標頭欄位的長度，計算方式是以 32 位元字組為單位，再除以 2，因為 IPv6 封包標頭是以 64 位元字組為單位。

- 保留 (Reserved): 16 位元保留欄位。目前皆設定為 0，還未指定使用方式。

- 安全參數索引 (Security Parameter Index, SPI): 32 位元欄位。SPI 是通訊雙方事先協議完成的安全關聯 (SA) 索引值，它必須配合目的位址和安全協定 (AH 或 ESP) 來查詢相關安全參數。也就是說，由 SPI、目的位址、與安全協定等三個欄位值，作為索引並查詢相關的安全參數 (12-6-4 節介紹)，安全參數有協定操作模式 (傳輸或通道模式)、加密演算法、加密鑰匙、以及使用期限等等。目前 1 ~ 255 的 SPI 值由 IANA 保留未來使用，0 為特殊用途，256 ~ 2^{32}-1 可以任意使用。

- 序號 (Sequence Number): 32 位元的無號整數值，是一個計數器的數值，主要防止重播攻擊 (Replay Attack)，容後再介紹。

- 認證資料 (Authentication Data): 不定長度的欄位。此欄位所存放的便是原來 IP 封包標頭的『完整性檢查值』(Integrity Check Value, ICV)，即 IP 封包標頭經過 HMAC 運算後的值。如果是 IPv4 封包，則 ICV 的長度必須是 32 的整數倍，而 IPv6 必須是 64 的整數倍。AH 協定規定 IPSec 裝置至少必須提供 HMAC-MD5 與 HMAC-SHA-1 等兩個以上的 HMAC 演算法。

接下來，我們來討論 AH 協定如何利用『序號』防止重播攻擊。它是利用『滑動視窗』(Sliding Window) 的運作方式，當 SA 被建立時，傳送者與接收者的序號計數器都必須清除為 0 開始，傳送者每發送一筆封包出去便將序號計數器加一 (不一定是給某一個固定接收者); 接收者再利用滑動視窗法檢視哪一個序號的封包已經接收過，將所收到的封包號碼以環狀佇列排放，進入的封包序號依序填入佇列的前方 (由前端指標指引)，而佇列的後端表示已經回應過的序號 (由後端指標指引)。在正常的情況下，接收端不斷接收與回應封包，前端指標與後端指標將會不停的滑動，因此稱之為滑動視窗法。當防止封包重播攻擊的功能啟動時，接收端收到封包後，將檢測封包序號是否小於後端指標所指引的數值，如果較小的話，表示該封包已回應過，可不予理會，如此便能避免重播攻擊。

12-4-2 AH 操作模式

IPSec AH 協定有『傳輸模式』(Transport Mode) 與『通道模式』(Tunnel Mode) 兩種操作模式，其不同點在於 AH 標頭所存放的位置。AH 可以利用通道模式重疊使用，也可以和 ESP 一起使用 (12-6-2 節介紹)，以下先介紹這兩種操作模式。

【(A) AH 傳輸模式】

AH 傳輸模式是將認證標頭放置於 IP 封包標頭與傳輸層協定 (TCP、UDP 或其他協定)的標頭之間，有 IPv4 與 IPv6 兩種不同封包格式。圖 12-8 (a) 為原 IPv4 封包，經過 AH 傳輸模式包裝後的格式如圖 12-8 (b)所示，IP 標頭的長度可以由 20 Bytes 到 60 Bytes 之間，之所以不定長度是因為有可能在標頭後面加入選項 (Options) 資料，如果沒有選項資料，則 IP 標頭長度為 20 Bytes。

(a) 原 IPv4 封包格式

(b) AH 傳輸模式的 IPSec (IPv4) 封包格式

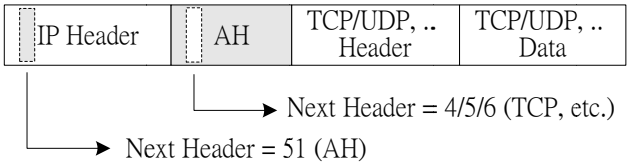

圖 12-8 IPv4 的 AH 傳輸模式包裝

基本上，原來 IPv4 封包標頭是不用修改的，只要將 AH 標頭加入即可，但因原 IP 封包所承載的協定已變成 AH 協定，而非原來的協定，因此還是需要將 IP 標頭內的『協定』(Protocol) 欄位內容設定為 51 (AH 協定)，並將原來的值置於 AH 標頭的『Next Header』欄位上。譬如，原來 IP 封包所承載的是 TCP 協定(Protocol=5)，經過 AH 傳輸模式包裝後，IP 標頭上的 Protocol 欄位便成為 51 (AH 協定)，而 AH 標頭上的 Next Header 欄位則需設定為 5 (TCP 協定，如圖 12-8 (b) 所示)。

【(B) AH 通道模式】

所謂『通道模式』(Tunnel Mode)，即是隱藏原來的 IP 標頭，而另外製作一個新的封包標頭，並且利用 AH 標頭保護原來的 IP 標頭。圖 12-10 為 IPv4 與 IPv6 AH 通道模式的封包包裝，新的封包標頭稱之為『外部標頭』(Outer Header)；而原來封包標頭稱之為『內部標頭』(Inner Header)。基本上，外部標頭的封裝格式與原 IP 標頭一樣，但它的目的位址與來源位址，可能和內部標頭不同，不相同的原因是該 AH 通道所扮演的角色有所不同 (連接主機或安全閘門，容後介紹)。外部標頭的內容也可以被所經過的路由器修改，譬如 TTL 或標頭檢查碼等欄位。

(a) AH 通道模式的 IPSec (IPv4) 封包格式

New IP Header	AH	Original IP Header	TCP/UDP, .. Header	TCP/UDP, .. Data

(b) AH 通道模式的 IPSec (IPv6) 封包格式

New IP Header	New Extesion Header	AH	Original IP Header	Orig Extesion Header	TCP/UDP, .. Header	TCP/UDP, .. Data

* 假設 Extension Header 存在

圖 12-10 IPv4 與 IPv6 AH 通道模式的封裝格式

我們用一個簡單的範例來說明 AH 通道模式的特殊用途，相信可讓讀者更容易瞭解 AH 通道模式的特性。一般在 VPN 網路上，都希望將內部的網路位址隱藏起來，並透過 NAT (Network Address Translator) 將內部位址轉換到外部位址，如圖 12-11 所示。兩區域網路 (192.168.1.0/24 與 192.168.2.0/24) 是透過 Internet 網路做 VPN 連接，並且將 IPSec AH Tunnel 與 NAT 軟體安裝於雙方網路的『安全閘門』(Security Gateway,

SG）上，連結到外部的合法位址分別是 163.17.8.141 與 163.20.9.5。當內部網路 A 的工作站（工作站 M，位址為 192.168.1.52）欲傳送封包給內部網路 B 的工作站（工作站 N，位址為 192.168.2.121）時，SG-A 將工作站 A 所發送的封包經由 IPSec AH Tunnel 包裝。在包裝當中，內部標頭的目的位址將會是 192.168.2.121；而外部標頭的目的位址是 163.20.9.5。區域網路 B 的 SG-B 收到封包後，再拆解外部標頭，並從事認證的工作，如果認證無誤的話，便捨棄外部標頭，恢復原來封包格式，並發送到內部網路；工作站 B 再由網路上收到該封包。如此，對雙方工作站而言，並不知道有 VPN 網路的存在，猶如在同一區域網路上運作一樣，也就是說，好像在公眾網路上建立一個秘密通道，故稱為『通道模式』。

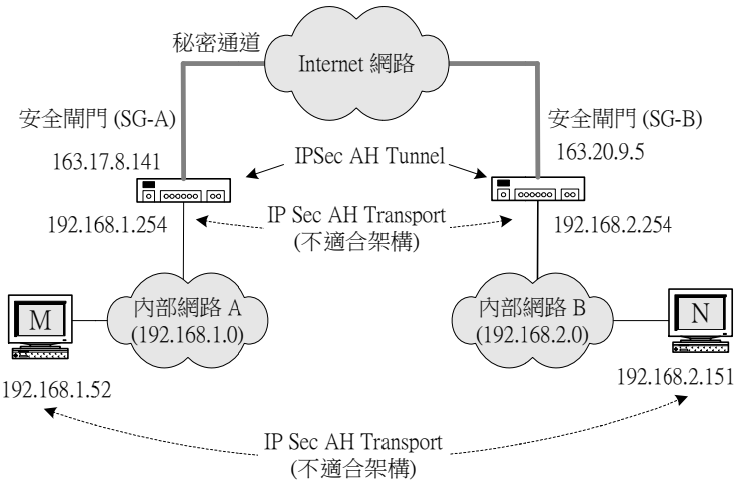

圖 12-11 AH 通道模式範例

就另一方面而言，AH 傳輸模式並不適合圖 12-11 網路使用，我們用兩種安裝架構說明它不適合的原因：(1) 如果將 IPSec AH Transport 安裝於雙方工作站（工作站 M 和 N）上，而由工作站 M 計算 AH 標頭，並重新包裝 IP 封包，但該封包到達 SG-A 時，會經由 NAT 更改目的位址（成為合法位址）、重新計算檢查值後再傳送出去。當工作站 N 收到此封包後，會依照封包標頭重新計算認證資料，但標頭已被修改，當然會發生認證失敗而拋棄該封包。(2) 第二種情況是將 IPSec SH Transport 安裝於雙方的安全閘門（SG-A 與 SG-B）上，安全閘門會依照原封包標頭計算 AH 標頭，再將原封包位址轉換到合法位址，如此也會變更到原 IP 封包標頭，同樣會造成接收端認證失敗的結果。

12-4-3 AH 認證欄位

AH 認證欄位是傳送端選擇原來 IP 封包標頭上某些欄位的值，並將這些值經過 MAC 演算法計算，產生一個『完整性檢查值』(Integrity Check Value, ICV)，再將此 ICV 值存放於 AH 標頭的認證資料欄位 (如圖 12-7 所示) 上；接收端收到 IPSec AH 封包後，選擇同樣欄位計算出 ICV，如果該 ICV 與 AH 標頭上 ICV 相同的話，則表示該封包是正確的，但必須滿足下列三個需求：

1. 必須協調出針對 ICV 加密的秘密金鑰；
2. 必須協調出採用何種認證演算法 (如 HMAC-SHA-1)；
3. 必須協調出選擇哪些欄位來計算 ICV 的值。

基本上，這三個需求都必須在通訊之前，透過 SA 連線協議而成。但就第三個需求而言，除了雙方可協議出採用哪些欄位外，我們同時必須了解選擇欄位的原因。有些欄位的內容會隨時改變，並不適合做 AH 認證使用，否則會發生許多無謂的困擾。如以 TTL 與 Header Checksum 欄位為例，IP 封包每經過一個路徑 (或路由器)，則 TTL 的值便會被減一，之後路由器會再重新計算標頭檢查值 (Header Checksum)，因此這兩個欄位隨時會遭受修改其內容。如果傳送端將隨時變更欄位的值加入計算的話，接收端在做認證檢查時，將很困難去辨別是正常變更或是遭受破壞。因此，我們必須先了解 IP 封包標頭上有哪些欄位容易變更、以及哪些欄位較不容易變更。在協調雙方通訊參數時(SA 連線)，便可參照這些訊息來決定哪些欄位可加入認證範圍。當然，加入愈多的欄位則認證的安全性愈高，但這必須視通訊雙方的需要而定。

【(A) IPv4 易變更的欄位】

以下列出 IPv4 封包標頭較容易變更的欄位：

◈ 服務類別 (Type of Service, TOS)：此欄位是說明該封包所要求的服務等級，此服務等級是由延遲時間、效能或可靠度的要求程度來分級。一般 IP 網路都將此欄位視為不易變更的，但是 IPSec 網路還是將它視為易變更欄位，因為還是有一些路由器會去更改它的內容。

◈ 旗號 (Flags)：IP 封包標頭有三個位元的旗號，分別是 DF、MF 和另一個未使用的位元 (0DM)。如 DF (Don't Fragment) 旗號被設定 (DF=1)，則表示此封包是

禁止被分段的；如 MF（More Fragment）旗號被設定（MF=1）的話，則表示該封包還有其他分段會緊接著送過來；如 MF=0，則表示本封包是最後的分段封包（或未分段封包）。基本上 IPSec AH 是不允許 IP 封包再被分段，因此此欄位的值必須都是零。

◈ 存活時間（Time To Live, TTL）：此欄位是用來限制封包的存活時間，以避免封包在網路無窮的環繞。傳送中的封包每經過一個路由器，該路由器自動將 TTL 值減一，再存回欄位上，如果該欄位的值等於零，則拋棄封包。因此，TTL 的值隨時會改變，多半不適合納入計算 ICV 的範圍。

◈ 分段偏移位址（Fragment Offset）：此欄位（13 位元）是說明本封包是原來 IP 封包經由分段後的位址。基本上 IPSec AH 是不允許 IP 封包再被分段，因此此欄位的值必須都是零。

◈ 標頭檢查碼（Header Checksum）：此欄位是計算 IP 封包標頭的檢查值。如果封包在傳送當中，有任何欄位被修改時，則此欄位的值將會隨之改變，因此計算 ICV 值時，都將此欄位設定為零。

◈ 選項（Options）：此欄位是不定長度，也許會攜帶某些選擇性的訊息，但目前路由器大多忽略該欄位上的訊息，所以大部份的 IPSec 也都不會將該欄位加入 ICV 計算。

【(B) IPv4 不易變更的欄位】

IPv4 封包標頭在傳輸當中，不容易被變更欄位有：

◈ 版本（Version）：IP 封包版本，應該為 4。

◈ Internet 標頭長度(Internet Header Length, IHL): 封包標頭的長度(包含 Options 與 Padding 欄位)

◈ 總長度(Total Length): 封包的總長度，其中包含封包標頭與承載資料(Data 欄位)。

◈ 識別（Identification）：如果所承載的資料（如 TCP 封包）有經過分段後，再分別由不同的 IP 封包承載，則此欄位登錄該資料的分段號碼。

◈ 通訊協定(Protocol): 表示封包所承載資料是屬於何種通訊協定，譬如 TCP、UDP、或 ICMP 等等。

◈ 來源位址 (Source Address): 封包的來源位址。

◈ 目的位址 (Destination Address): 封包的目的位址。

基本上，選擇那些欄位計算 ICV，是由雙方協議的 SA 來決定，我們將 IPv4 的封包標頭顯示於圖 12-12，其中有底色的欄位表示有可能被選取的機會。如果沒有被選取的欄位，在計算 ICV 時都會被設定為零。

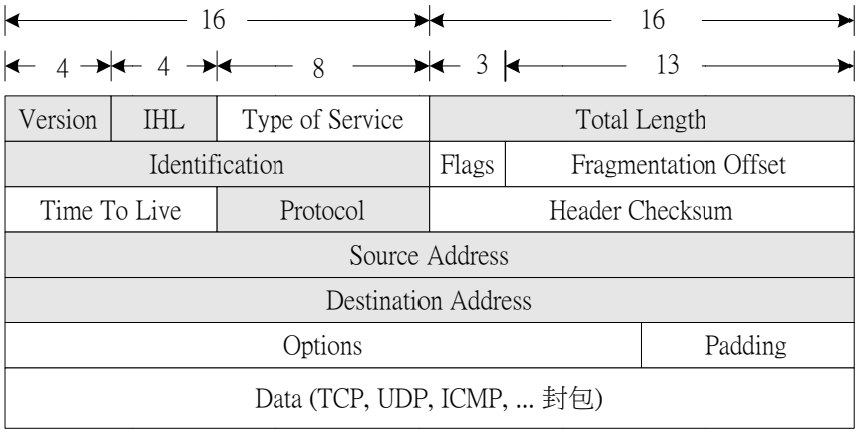

圖 12-12 IPv4 標頭可參與計算 ICV 欄位 (有陰影部份)

我們用兩個簡單的範例，說明選擇那些欄位計算 ICV，可能會對 AH 認證能力產生影響。一者將總長度欄位加入計算，倘若傳輸當中封包所承載資料遭受替換，雖然攻擊者也可以修改總長度欄位的內容，來蒙騙接收者；但接收端還是可以由 ICV 計算出認證封包長度是否被變更，如此一來，表示 IPSec AH 不但可以保護封包標頭，也可認證整個 IP 封包，此即稱為『非連接導向的完整性』功能。另一者，倘若將來源位址加入 ICV 計算，則可以避免中間人攻擊，其原因是中間人將封包接收後，再發送新的封包給接收端，則新的封包的來源位址勢必遭受變更，接收端便可依此驗證出該封包的正確性，此即稱為『資料來源認證』功能。

12-4-4 AH 運作程序

執行 IPSec AH 的裝置可能是主機或路由器，如果在路由器上執行 IPSec 的功能的話，就稱它為『安全閘門』(Security Gateway, SG)。一般 VPN 網路都是透過安全閘門

對外通訊。另外，外部漫遊主機為了要與 VPN 網路通訊，也可以在主機上安裝 IPSec 軟體。我們將 IPSec AH 的運作模式（主機或安全閘門）以圖 12-14 的流程圖表示。還未介紹其運作程序之前，我們必須強調 IPSec 運作完全依照雙方所協議『安全關聯』(SA) 的安全參數而定，然而安全閘門則利用下列兩個資料庫來決定是否給予 IPSec 處理，以及 SA 相關安全參數，如下：

- 『安全政策資料庫』(Security Policy Database, SPD)：登錄那些通訊連線需要經過 IPSec 處理，因此它的搜尋關鍵字是由目的位址、通訊協定與通訊埠口等三個欄位所組成 (又稱為連線識別，可表示連接何種應用系統)。至於 SPD 資料庫是如何建立而成？多半是由系統管理員依照安全政策以人工輸入而成。

- 『安全關聯資料庫』(Security Association Database, SAD)：登錄已協議完成的 SA，並儲存相關安全參數。然而，SAD 資料庫是由 ISAKMP 協定所建立而成。

以下分別以發送與接收的處理流程來介紹。

【(A) 送出 IPSec AH 封包的運作程序】

在防火牆架構的 VPN 網路上，當安全閘門 (SG) 收到一個往外送的封包，它必須決定是否給予該封包 IPSec 處理，直接通過或者過濾該封包不予通過。這裡我們暫不考慮防火牆功能，只針對 VPN 網路安全閘門的運作程序來介紹，如以下步驟：(如圖 12-14 (a) 所示)

- 步驟 1：當安全閘門 (SG) 收到一個外送封包，則利用該封包的訊息 (如目的位址、通訊協定、通訊埠口) 搜尋 SPD 資料庫，決定是否給予 IPSec 處理；倘若需要 IPSec 處理的話，則可查詢出相對應的『安全參數索引』(Security Parameter Index, SPI)，並接下一步驟；否則直接轉送 (或過濾) 該封包。

- 步驟 2：SG 依照 SPD 上的索引值搜尋 SAD 資料庫，查閱是否有相對應的 SA。如果沒有或者該 SA 已經過期的話，則 SG 發動 ISAKMP 連線和接收端共同建立 SA 及相關參數 (第十六章介紹)；如存在或已建立完成則接下一步驟。

- 步驟 3：增加或起始 AH 序號 (如圖 12-7 Sequence Number 欄位)，以避免重播攻擊。

- 步驟 4：依照 SA 內的參數（如選擇哪些欄位驗證），計算 ICV 值。
- 步驟 5：建立 AH 認證標頭，並依照 SA 參數來包裝 IPSec 封包（傳輸或通道模式）。
- 步驟 6：發送 IPsec AH 封包（或分段發送）。

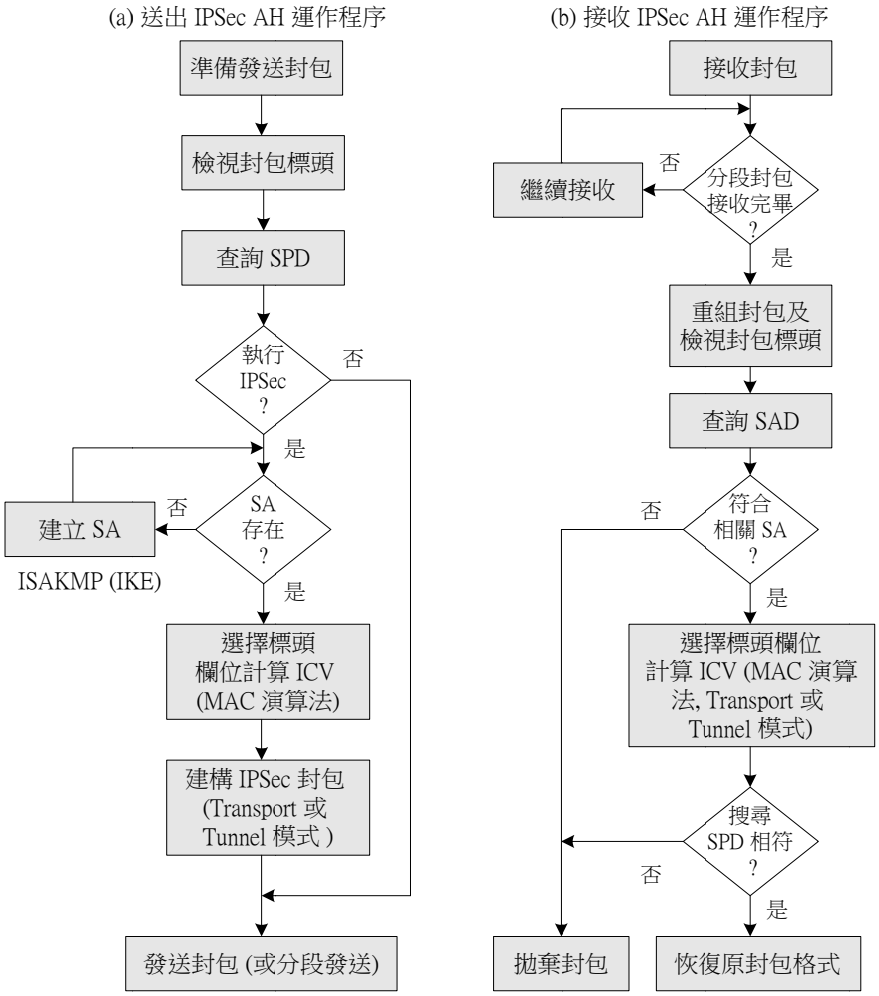

圖 12-14 IPSec AH 的運作程序

【(B) 接收 IPSec AH 封包的運作程序】

基本上，IPSec 協定不允許封包在傳輸中途被分段，所有分段必須在發送端的安全閘門(SG)上完成，然而安全閘門傳送封包之前，並不瞭解網路狀態(譬如 MTU 大小)，因此它必須經由測試才知道是否需要分段。測試分段方法如下：首先將封包標頭的 DF 旗號設定成『不允許分段』(Don't Fragment)，傳送封包當中遇到 MTU 較小的路徑，而需要分段時，則該路徑的路由器便會回應 ICMP Destination Unreachable（Type 3） 之 Fragmentation Needed and DF Set（Code 4）封包給原傳送端（即是安全閘門）；安全閘門

收到 ICMP 封包之後，便了解需要分段才能傳送封包，則分段該封包並分別傳送出去；並且將所有分段封包標頭上的 MF (More Fragment) 設定為 1 (MF = 1)，但最後分段封包設定為 0(MF = 0)。倘若所有路徑都不需要分段的話，當然安全閘門就不會收到 ICMP 封包，亦表示傳送正常。

也就這樣，接收端收到 IPSec AH 封包後，必須由封包標頭上的 MF 觀察是否有其他分段封包緊接在後，如果 MF=0，則表示本封包是最後分段或未經分段封包。IPSec AH 接收端運作程序如下：(如圖 12-14 (b) 所示)

- **步驟 1**：判斷封包標頭的 MF 是否為零，若 MF≠0 則繼續接收封包；如果 MF=0，則表示已接收完封包，並將其組合回原封包格式，然後接下一步驟。
- **步驟 2**：利用 IPSec AH 封包標頭的 SPI、目的位址、以及 IPSec 協定(AH 或 ESP) 等欄位作為關鍵字，查詢 SAD 資料庫中的相關 SA，如果查詢得到便接下一步驟；否則拋棄該封包。其中 IPSec 協定是採用 IP 封包標頭上的『下一個標頭』(Next Header) 欄位；倘若採用通道模式的話，則由『外部』(Outer) 標頭上查詢。
- **步驟 3**：利用所查詢出來的 SA 相關參數，以及封包所承載的 ICV，驗證封包標頭是否正確，如不正確，則拋棄該封包；否則接下一步驟。
- **步驟 4**：利用封包內某些訊息(如目的位址、通訊協定、通訊埠口)為索引，查詢 SPD 資料庫，是否合乎相對應的安全政策，如果不符合，則拋棄該封包；否則接下一步驟。
- **步驟 5**：查詢 AH 標頭內的序號 (Sequence Number) 是否在認證範圍內，如果已超出範圍則表示已認證過，即是重播封包，並拋棄該封包；否則接下一步驟。
- **步驟 6**：恢復原來封包格式 (IPv4 或 IPv6)，並發送給接收工作站。

12-5 IPSec ESP 協定

12-5-1 IPSec 協定簡介

IPSec 另一個安全協定為『封裝安全承載』(Encapsulation Security Payload, ESP)，同樣包含 IPv4 與 IPv6 兩種規範。ESP 協定是將原來封包所承載的資料經過加密處理

之後，再重新封裝一個新的封包（ESP 封包）才傳送給接收端；接收端拆解 ESP 封包後，先將資料解密，再組合回原封包格式，故稱之為『封裝安全承載』，其特性歸納如下：

- ESP 提供資料的隱密性、資料來源認證、非連接方式完整性、反重播攻擊能力、以及有限度的流量機密性等功能。
- 具有傳輸模式（Transport Mode）和通道模式（Tunnel Mode）等兩種封包格式。
- 利用封包序號作為防禦重播攻擊（如同 IPSec AH）。
- 對所承載的資料可進行加密，以達到隱密性功能。一般都採用對稱加密法，針對加/解密所需的秘密金鑰，以及加密演算法皆是由 SA 參數而定。基本規範有 DES 的 CBC 模式與 NULL 編碼演算法。
- 可利用 ICV 驗證整個封包資料，以達到資料來源驗證。認證的範圍（亦是所選用的欄位）可由雙方協議的 SA 參數而定，認證演算法有 HMAC-MD5、HMAC-SHA-1 以及 NULL。
- 必須採用通道模式才具『有限度的流量機密性』的功能。
- 可配合 AH 協定使用，以達到較完整的封包標頭驗證，與資料隱密性的功能。

相較於 AH，ESP 好像增加了資料隱密性和有限的流量機密性功能，但對於資料來源的認證，就沒有 AH 協定那麼完整。簡單的說，AH 協定主要是提供封包標頭的認證，任何有修改或偽裝封包將被偵測出來，但對於資料是否認證功能，完全取決於所選用的認證欄位而定；當然 ESP 協定除了提供簡單的封包標頭認證之外，並將所承載的資料加密，以達到資料隱密性的功能。

12-5-2 ESP 封包格式

ESP 封包格式與 AH 有很大的不同點，AH 是將認證標頭插入原封包標頭的後面或前面，基本上還是保留原來的封包格式；然而 ESP 為了達到資料的隱密性，會將原封包所承載的資料重新包裝成另一個『ESP 封包格式』，並依照操作模式(傳輸或通道模式)處理原封包標頭。譬如，傳輸模式就是將 ESP 封包放置於原封包標頭的後面；而通道模式是新建立一個的封包標頭，放置於最前面（容後詳細介紹）。

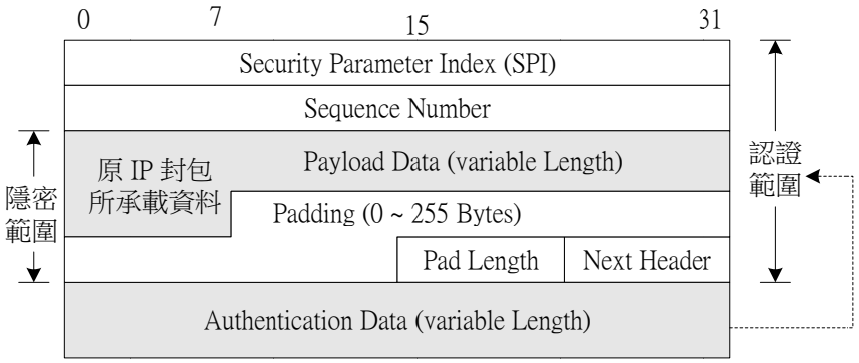

圖 12-15 IPSec ESP 封包格式

圖 12-12 為 ESP 封包格式（未包含原封包標頭），它是將原封包所承載資料經過加密（或未加密）後，再重新包裝的格式。一般將 SPI 與 Sequence Number 稱之為『ESP 標頭』（ESP Header），而 Payload Length 與 Next Header 兩個欄位稱之為『ESP 標尾』（ESP Trailer），各欄位功能如下：

- 安全參數索引（Security Parameter Index, SPI）：32 位元長度。SPI 的功能和 AH 協定中的 SPI 相同，都是雙方事先協議完成安全關聯（SA）的索引值，但它必須配合目的位址和安全協定（AH 或 ESP）來查詢相關安全參數。
- 序號（Sequence Number）：32 位元長度。如 AH 協定中的序號一樣，都是作為反重播攻擊使用（12-4-1 節介紹）。
- 承載資料（Payload Data）：為不定長度的欄位。當有啟動隱密性資料功能時（SA 參數決定），ESP 協定先將原來 IP 封包所承載的資料（TCP、UDP 或其他協定），經過某一加密演算法編碼後，再存入此欄位上傳送；如果沒有啟動隱密性功能，則填入原來 IP 所承載的資料。另一方面，如所選用的加密演算法需要『初始向量』（Initial Vector, IV）的話，則必須將 IV 值填入此欄位。基本上，無論是只有密文或密文附帶 IV 值，資料都必須是一個可以被 8 整除的長度。
- 填補（Padding）：此欄位是選項的不定長度。主要作用於對齊資料長度是否是 32 位元長的整數倍，但它的長度可以由 0 到 255 位元組。
- 填補長度（Pad Length）：8 位元長度。此欄位是表示所加入的填補資料的長度，有效值是 0 ~ 255 之間。

◈ 下一個標頭（Next Header）：8 位元長度。此欄位是用來辨識封包裡所承載資料的協定，譬如，Next Header = 6，表承載資料為 TCP 協定的資料封包。

◈ 認證資料（Authentication Data）：不定長度欄位。此欄位所存放的是『完整性檢查值』（ICV），認證範圍可以由 SPI 到 Next Header 欄位，這可由雙方協議的 SA 參數而定。

由上述的介紹，可以分辨出 AH 和 ESP 兩協定之間最大的不同點，AH 協定較著重於封包標頭認證，因此對於封包來源認證功能較強；然而 ESP 協定則偏重於承載資料的隱密性及認證，對於資料的保護較為嚴密。使用者可依照環境需求選擇 AH 或 ESP 協定，甚至也可以整合 AH 與 ESP 協定使用。

12- 5-3 ESP 操作模式

如同 AH 協定一樣，ESP 協定也分為『傳輸模式』與『通道模式』兩種操作模式，其最大的不同點在於 ESP 標頭（SPI 與 Sequence Number 欄位）所存放的位置，以及是否重新建立新的封包。以下分別就 IPv4 與 IPv6 來介紹這兩種運作模式。

【（A）IPv4 ESP 傳輸模式】

圖 12-16 為 IPv4 ESP 傳輸模式的封包格式，它是將 ESP 標頭（SPI 與 Sequence Number 欄位）插在原 IP 封包標頭之後，並對原封包所承載的資料編碼加密，再存放於 ESP 承載欄位上；緊接著是 ESP 標尾（Padding、Pad Length 與 Next Header 等欄位），最後才是 ESP 認證資料的欄位（ICV 資料）。其中經加密編碼欄位是否包含 ESP Trailer、或所提供的認證範圍（ESP 標頭到 ESP 標尾之間），皆由雙方協議之 SA 而定。

(a) 原 IPv4 封包格式

(b) ESP 傳輸模式的 IPSec (IPv4) 封包格式

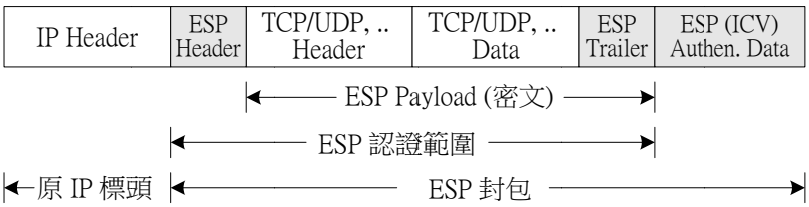

圖 12-16 IPv4 ESP 傳輸模式之封包格式

【(C) IPv4 ESP 通道模式】

之前我們利用圖 12-11 說明傳輸模式與通道模式之間的不同點，其中表示通道模式可使用於 NAT 網路環境裡，方法是將內部網路位址包裝在『內部標頭』(或稱原 IP 標頭) 之內隱藏起來，再將『外部標頭』(或稱新的 IP 標頭) 設定為合法網路位址。也就是說，IPSec ESP 封包封裝時，是將原來 IP 標頭包含進去 (傳輸模式沒有)，並且另外建立一個新的 IP 標頭 (外部標頭)。圖 12-18 (a) 為 IPv4 封包經由 IPSec ESP 通道模式封裝的格式，加密編碼與認證範圍如同傳輸模式一樣 (ESP 封包範圍如同圖 12-16、17 一樣)。

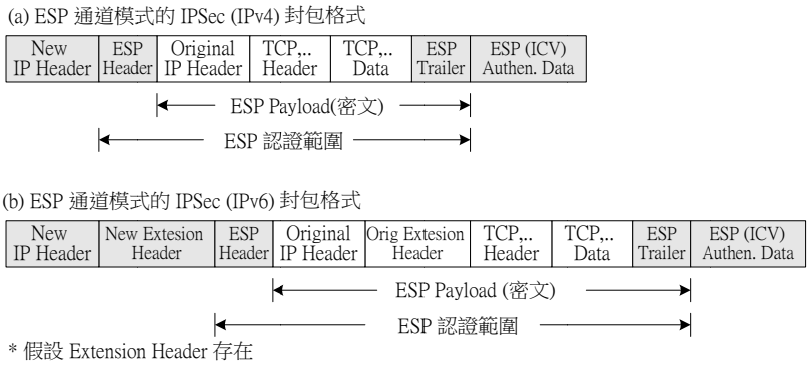

圖 12-18 IPv4 與 IPv6 的 IPSec ESP 通道模式封包

12-5-3 ESP 加密及認證演算法

基本上，ESP 都使用對稱加密演算法。這是因為公開金鑰演算法必須耗費較長的加密/解密時間，這對於一般通訊而言效率太低。另一方面，IPSec 只建議 VPN 系統至少需具備有 DES 與 NULL 兩種編碼演算法，其中 NULL 表示所承載的資料是沒有經過編碼的，亦即選用 NULL 編碼演算法，則表示沒有加密的功能。除了上述兩種編碼系統外，通訊雙方也可以經由 SA 連線來協議雙方的編碼系統 (如 AES 演算法)。

同樣的，IPSec 並沒有強制規定一定要用何種認證演算法，但規定至少要有：HMAC-MD5、HMAC-SHA-1 與 NULL 等演算法，其中 NULL 表示沒有認證功能的意思。無論所採用的加密系統、驗認演算法或演算法中所需的秘密金鑰，都必須雙方經由 ISAKMP 協定協議出來，如果在協議之中需要交換雙方鑰匙，就會使用到 IKE 協定。

12-5-4 ESP 運作程序

基本上，在 RFC 2406 中並沒有規定標準的運作程序，因此，不同的實作也許會有不一樣的程序，我們在此僅列出其應有功能的運作程序。

【(A) 封包外送處理程序】

執行 IPSec ESP 功能的裝置也許是移動式主機或安全閘門，當它收到一個往外送的 IP 封包時，其處理 ESP 功能的運作程序如圖 12-19 (a) 所示，步驟如下：

- 步驟 1：當 ESP 裝置收到一個往外送的封包，首先由封包標頭的某些欄位 (如目的位址、通訊協定、傳輸埠口) 作為搜尋關鍵，檢視『安全政策資料庫』(SPD) 是否給予 IPSec 處理 (是否可得到 SPI 值)，如果沒有安全措施，便直接讓封包通過；否則接下一步驟。
- 步驟 2：利用 SPI 搜尋 SAD 資料庫，是否有得到相關的安全關聯 (SA)，如沒有則啟動 ISAKMP 協定建立所需的 SA；否則依照 SA 參數封裝 IPSec ESP 封包。其中相關參數可能有：安全協定 (AH 或 ESP)、操作模式 (傳輸或通道模式)、驗證演算法、編碼演算法 (加/解密)、共享秘密金鑰等等。
- 步驟 3：增加序號 (Sequence Number)，做為反重播攻擊使用。
- 步驟 4：倘若隱密性功能啟動的話，便執行加密處理，又如果加密演算需要初始向量 (IV)，則將初始向量放置於承載資料的最前面。如果是傳輸模式的話，則加密範圍可由原承載資料 (TCP 或 UPD 標頭及資料) 到 ESP 標尾；如果是通道模式，則必須再包括原 IP 封包標頭。
- 步驟 5：倘若啟動認證功能的話，則計算完整性檢查值 (ICV)，計算範圍除了原封包所承載資料外，還包含 ESP 標頭。
- 步驟 6：封包分段：依照封包到達目的位址之間的最大傳輸量 (MTU)，決定是否給予封包分段，如封包長度大於 MTU 時，便需要分段傳輸。

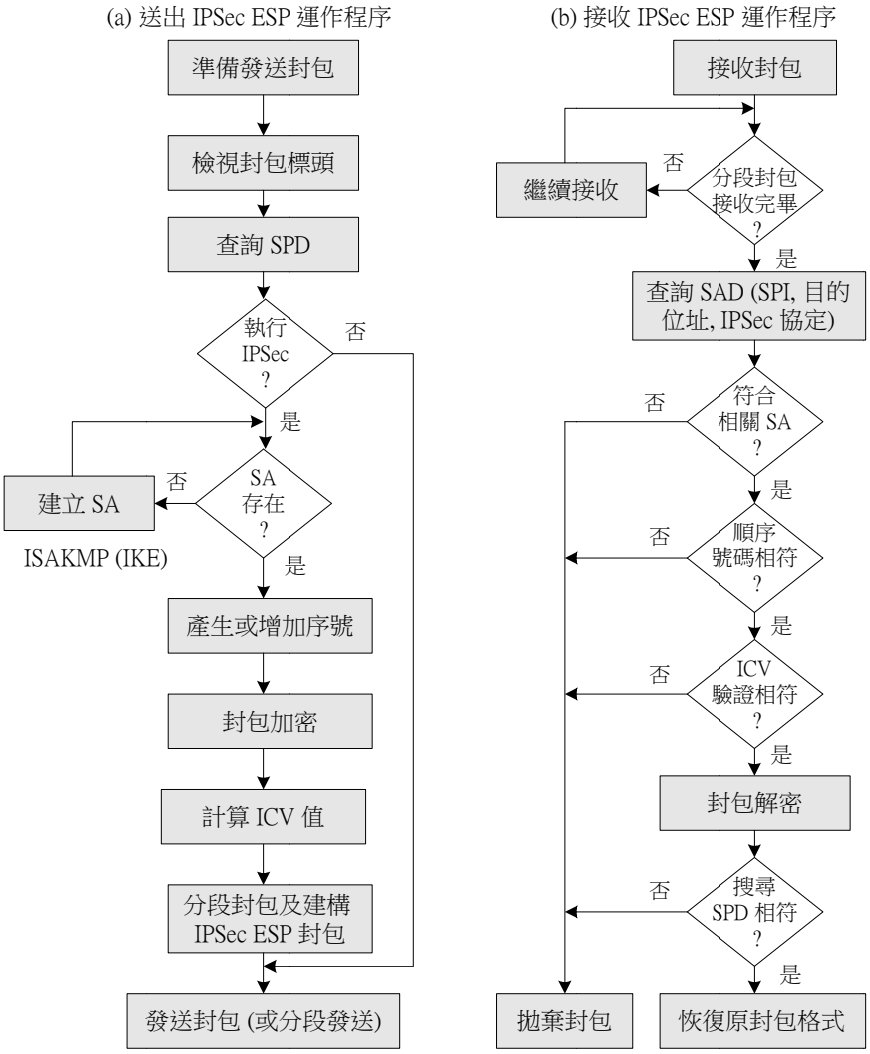

圖 12-19 IPSec ESP 協定的運作程序

【(B)封包接收處理程序】

當安全閘門或主機收到 IPSec 封包後，處理程序如下：(如圖 12-19 (b) 所示)

- 步驟 1：封包完整接收，如果封包有經過分段，必須全部收完才可以做適當處理，這是因為原封包是經過 IPSec 處理後再分段。
- 步驟 2：利用封包標頭的目的位址、SPI 與協定欄位作為索引，查詢『安全關聯資料庫』(SAD)，是否有相關的安全連線(SA)，如果搜尋不到便拋棄該封包；否則接下一步驟。
- 步驟 3：查詢順序號碼(SN)是否在回應範圍內，以避免重播攻擊。如果該序號已回應過，便拋棄該封包；否則接下一步驟。
- 步驟 4：如果已啟動認證功能，便依照 SA 參數計算完整檢查值(ICV')，再和封包

內的完整檢查值（ICV）比較，如果兩者不相同（ICV≠ICV'），則拋棄該封包；否則接下一步驟。

- 步驟 5：如果資料隱密功能已啟動的話，便依照 SA 參數將封包解密。
- 步驟 6：利用封包標頭某些欄位，搜尋 SPD 資料庫，是否有相關的政策規定。如不符合政策規定，便拋棄該封包；否則便將該封包轉送到適當的主機或網路閘門上，其中搜尋關鍵字可能是 IP 封包標頭或所承載協定（TCP 或 UDP）標頭上的欄位，譬如目的位址、TCP/UDP 協定或傳輸埠口等等。

12-6 安全關聯

12-6-1 安全關聯簡介

『安全關聯』（Security Association, SA）是 IPSec 中重要的觀念。由前面所介紹的 AH 與 ESP 協定當中，可以發現所有通訊行為都必須依照雙方事先所協議的 SA 安全參數；到底 SA 是何種東西？相信是讀者最迫切想知道的答案。其實 SA 是資料庫（SAD）中的某一筆記錄，登錄所需的安全機制，譬如，安全協定（AH 或 ESP）、操作模式（傳輸或通道模式）、認證演算法（HMAC-MD5, …）、加密系統（DES-CBC, …）、或共享秘密金鑰等等。至於 SA 是如何建立的，將於下一章再介紹，在此先介紹 SA 的特性及相關參數，其特性歸納如下：

- 單工性：每一筆 SA 所描述的『通訊連線』都是單向的。也就是說，對於 IPSec 裝置而言，『外出』訊務與『進入』訊務都必須有獨立的安全關聯。
- 重複使用：當某一筆 SA 建立之後，可在有效期間內重複被使用，所以每一筆 SA 都會限制有效期間。
- 獨立通訊協定：每一筆 SA 僅能描述一種通訊協定(如 AH 或 ESP 協定)。倘若通訊連線需要使用到兩種協定，則必須有兩筆 SA 分別描述之。
- 安全關聯束（SA Bundle）：一條通訊連線可能需要一個以上的 SA 來描述其安全機制，因此，安全閘門（或安全主機）必須多次搜尋相關的安全關聯；而由多筆 SA 所構成的安全機制稱之為『安全關聯束』。

◈ 唯一識別值：安全關聯的唯一識別值是由『安全參數索引』(Security Parameter Index, SPI)、IP 目的位址、以及安全協定 (ESP 或 AH) 等三者所構成，其中目的位址可以是單一位址、廣播位址、或群組位址。

◈ 操作模式：SA 定義傳輸模式 (Transport Mode) 與通道模式 (Tunnel Mode) 等兩種操作模式，前者的 SA 主要應用於『主機對主機』(Host-to-Host) 之間的安全通訊，後者則主要應用於『網路對網路』(Network-to- Network) 之間的通訊。

12-6-2 安全關聯功能

依照 IPSec 協定的特性，安全關聯 (SA) 提供有下列功能：

◈ 『資料原始認證』(Data Origin Authentication)：透過 IPSec 協定可確認資料的來源位址，以避免接收到偽裝資料。譬如 AH SA 協定可認證資料的來源。

◈ 『非連接完整性』(Connectionless Integrity)：倘若以原來 IP 封包方式傳輸，接收端無法確認資料是否已發生錯誤，或已遭他人竄改。IPSec 協定可利用『完整性檢查值』(ICV) 來確認資料的完整性。AH SA 與 ESP SA 都具有此功能。

◈ 『反重播攻擊』(Anti-Replay)：IPSec SA 利用封包內的『順序號碼』(Sequence Number)，判斷該封包是否已接收過，如果是重複性封包，便將它拋棄。

◈ 『隱密性』(Confidentiality)：ESP SA 協定提供有資料編碼的功能，傳輸中的資料可經由加密以達到資料隱密的功能。

◈ 『部份訊務流量機密性』(Partial Traffic Flow Confidentiality)：如果通訊連線採用 ESP SA 協定、通道模式封裝、以及啟動資料隱密性功能時，真正的目的位址是包裝在內部標頭 (Inner Header)，並且內部標頭是經過加密處理的。在這種情況下，由網路上竊取此封包也很難知曉該封包的真正目的位址，如此便可達到目的主機訊務流量的隱密性。換句話說，也許目的主機是一個重要的伺服系統，它管理許多重要的資料 (或資料庫)，相對其訊務必定非常忙碌，ESP SA 協定便可以隱藏它的訊務流量，以減少此主機暴露的危機。

由以上的介紹，我們可以做簡單的結論：AH SA 協定主要是訴求來源資料認證；而

ESP SA 較著重於資料隱密性功能；但是 AH 與 ESP 都具有資料完整性的功能。如果通訊連線需要資料來源認證與資料隱密性功能，則必須由 AH SA 與 ESP SA 兩個安全關聯來描述，亦即必須同時經過 AH 與 ESP 封裝包裝。

12-6-3 安全關聯組合

IPSec 不僅有 AH 與 ESP 兩種協定，而且每一種協定又有兩種操作模式，因此 IPSec 協定就有 AH 傳輸、AH 通道、ESP 傳輸、ESP 通道等四種運作模式，其中每一種運作模式都需要獨立的 SA 來制定其安全政策。至於一個通訊連線也許需要多個 SA 來描述其安全機制，這多筆 SA 就稱為『安全關聯束』(SA Bundle)，不同環境需求，可能出現不同的組合方式，基本上可歸納為『傳輸串接』(Transport Adjacency) 與『反覆通道』(Iterated Tunneling) 兩種組合方式，以下分述之。

【(A) 傳輸串接】

『傳輸串接』是針對同一個 IP 封包做多次傳輸模式的操作，其中並沒有實現通道模式。在這種模式下，通訊連線也許會經由多個 AH 與 ESP 協定的傳輸模式包裝，每一層次的包裝皆是針對一個特殊路徑。圖 12-20 (a) 為傳輸串接組合的範例，其外層的安全關聯是利用 AH Transport 包裝，而內層是 ESP Transport 包裝，如果由封包結構來看，就好像傳輸模式的封包標頭串接起來的樣子，如圖 12-20 (b) 所示。

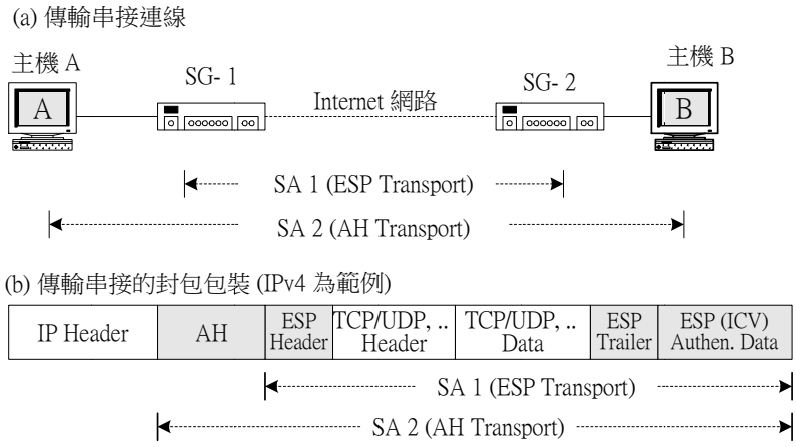

圖 12-20 傳輸串接組合之範例

【(B) 反覆通道】

『反覆通道』是利用多層次的 IPSec 通道 (Tunneling) 做安全防護，這種多層次是

以巢狀包裝方式。也就是說，最外層包裝內層協定封包，下一層再包裝下一個內層的協定封包，依此類推，達成反覆的（Iterated）封包包裝。反覆通道的安全關聯模式有下列三種：

1. 雙方端點的安全關聯相同：表示通訊雙方安全關聯都在相同的端點上，如圖 12-21 (a) 所示。內部（Inner）與外部（Outer）的安全關聯都可以使用 AH 或 ESP 安全協定。圖 12-21 (b) 封包包裝範例是外部（SA 2）採用 AH Tunnel 協定，而內部安全關聯（SA 1）為 ESP Tunnel 協定，內部的安全協定被包裝在外部安全協定之內。

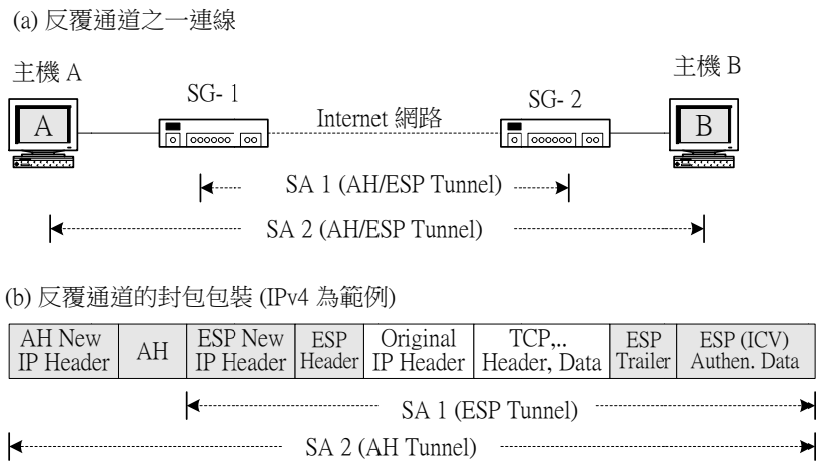

圖 12-21 反覆通道 SA 模式之一

2. 單一端的安全關聯相同：表示通訊雙方之中，一邊的安全關聯在同一端點上，而另一方不在同一端點上。以圖 12-22 為例，一邊的安全關聯是建立在主機 A 上，而另一方的安全關聯則是分別建立在安全閘門（SG 2）與主機 B 上，其中 SA 1 與 SA2 可分別採用 AH 或 ESP 協定。

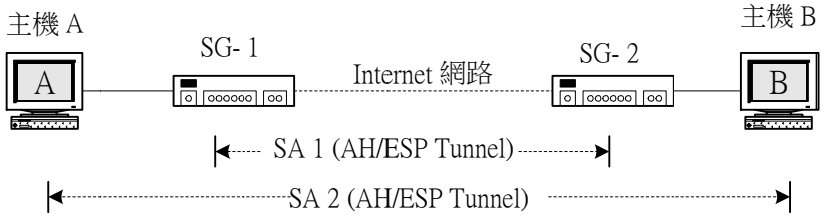

圖 12-22 反覆通道 SA 模式之二

3. 雙方端點的安全關聯不相同：表示通訊雙方的安全關聯都不是建立在同一端點上。這種模式是一般防火牆虛擬私有網路最常用的連結型態，其中外部或內部的安全關聯都可分別選用 AH 或 ESP 協定，但內部安全關聯則採用 ESP 協定似乎較為適

當，如 12-22 所示。

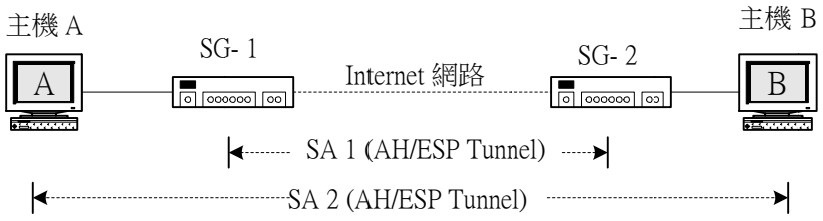

圖 12-23 反覆通道 SA 模式之三

12-6-3 安全政策資料庫

在 IPSec 協定上，係利用兩個資料庫來實現安全關聯的措施，一者為『安全政策資料庫』(Security Policy Database, SPD); 另一者為『安全關聯資料庫』(Security Association Database, SAD)。另外針對外出 (Outbound) 與進入 (Inbound) 訊務，兩種資料庫也分別以不同的資料庫系統來處理，即『外出資料庫』(Outbound Database) 與『進入資料庫』(Inbound Database)，分別處理進入與外出訊務。兩者資料庫係安裝在有處理 IPSec 協定的裝置上，可能是主機或安全閘門(Security Gateway)上。本節將介紹 SPD，至於 SAD 將會在下一小節介紹。

基本上，『安全政策資料庫』(SPD) 是依照組織單位政策來建立，可選擇某些訊務 (Traffic) 是否給予安全機制的措施。因此，SPD 資料庫大多是利用人工輸入方式來建立，並且一般安全裝置都必須提供輸入 SPD 的介面。在 SPD 資料庫上，每一筆記錄都有相對應的指標到安全關聯資料庫的某一筆記錄，即索引到一個安全關聯 (SA)。但是一個通訊訊務可能符合一個或多個安全政策，相對會搜尋到一筆或多筆安全關聯 (或稱 SA Bundle)，所以必須分別針對每一個安全關聯做處理 (如 IPSec 協定包裝)。

【(A) 外出處理】(Outbound Processing)

當安全閘門 (或安全主機) 收到一個外出的訊務時，必須針對這筆訊務做：啟動安全機制、直接轉送、或拋棄該訊務等三項之一的處理。至於應該給予何種處理，這必須由人工輸入建立各種規則，但我們在建立這些規則時，必須考慮到如何由該訊務上得到判斷的訊息，當然這些可判斷的訊息大多來自封包各欄位上的資料，我們也將這些訊息稱之為『選擇因素』(Selectors)。在 RFC 2401 列有下列選擇因素：

- ◈ 目的 IP 位址（Destination IP Address）：表示此封包的目的位址（IPv4 或 IPv6）。
- ◈ 來源 IP 位址（Source IP Address）：表示此封包的來源位址（IPv4 或 IPv6）。
- ◈ 名稱（Name）：表示發出此訊務的使用者或系統名稱，表示方法可以是網域名稱（Domain Name）或是以 X.500 DN。基本上，由 IP 封包是無法觀察出使用者或系統的名稱，這需仰賴其它安全機制系統才可以達成，譬如 Kerberos 管理系統。
- ◈ 資料靈敏性層次（Data Sensitivity Level）：表示此封包所承載資料的靈敏度，這可能需要其他系統來輔助。
- ◈ 傳輸層協定（Transport layer protocol）：表示此封包所承載的傳輸層協定（TCP 或 UDP）。IPv4 封包是由 Protocol 欄位來判斷，而 IPv6 是以 Next Header 欄位。
- ◈ 來源埠口（Source Port）：此封包的來源傳輸埠口（TCP Port 或 UDP Port）。
- ◈ 目的埠口（Destination Port）：此封包的目的傳輸埠口。

一般 Internet 網路上的應用系統都以傳輸埠口來分辨，譬如，Web Server 位於 80 埠口（TCP 或 UDP），因此，選擇因素參考到 IP 封包上所承載資料的機會非常大，也就是說，安全裝置為了搜尋安全政策，會將 IP 封包拆解到 TCP/UDP 協定的層次。也就這樣，IPSec 協定不允許 IP 封包被中途再分段，所有分段動作必須在原發送端完成；然而接收端也必須接收完所有的分段封包，才可繼續做其他安全機制的處理。

【（B）進入處理】（Inbound Processing）

另一方面，一個安全性的訊務可能由多個 IPSec 封包所構成，安全閘門（或安全主機）是利用每一個 IPSec 封包標頭的目的位址、安全協定（AH 或 ESP）、以及安全參數索引（SPI）等三個參數來分辨所屬的安全關聯；並且將該訊務所屬的 IP 分段組合回原 IP 封包。接下來，接收端的安全閘門再依照各種『選擇因素』（Selectors），搜尋 SPD 資料庫，是否符合相關安全政策，如果符合則接受此訊務；否則便將之拋棄。一個訊務所屬的安全政策也是經由許多安全關聯所構成，因此，可能需要多次的搜尋 SPD 資料庫才能完成。

12-6-4 安全關聯資料庫

『安全關聯資料庫』(Security Association Database, SAD) 記錄著每一筆安全關聯 (SA) 的相關參數，這些參數也許是經由人工輸入，或是通訊雙方經由 ISAKMP 協定建立而成。基本上，每一筆安全訊務都必須依照安全關聯的參數來製作；也就是說，在 SAD 資料庫上至少有一個以上的記錄 (SA 記錄)。對於外出訊務而言，是利用『選擇參數』來搜尋 SPD 資料庫，而得到一個進入 SAD 資料庫的進入點 (Entry)，每一個進入點表示一個安全關聯，同時記錄著外出的相關安全參數；對於進入訊務而言，係利用 IPSec 封包上的目的位址、安全協定 (AH 或 ESP) 以及安全參數索引 (SPI) 等三個參數，來搜尋 SAD 資料庫，以得到相關的安全參數。

至於 SAD 資料庫上有哪些欄位來描述各種安全參數，完全依廠商的實作有所不同，在 RFC 2401 上列出下列安全參數，可供各家廠商參考使用：

- 序號計數器(Sequence Number Counter): 32 位元整數，是用來存放於 AH 或 ESP 標頭上的序號欄位，每次該 SA 被參考使用時，便計數一次。此序號是做反重播使用。
- 序號計數溢位 (Sequence Counter Overflow): 此為計數溢位的旗號。如果序號計數器已計數溢位時 (表示 32 位元計數完)，此旗號便會被設定，此時，系統必須經過稽核才可以繼續啟動序號計數器。
- 反重播視窗 (Anti-Replay Window): 此為 32 位元計數器及位元對應 (bit-map)，是用來確認進入的 AH 或 ESP 封包是否是重播的。
- AH 認證 (AH Authentication): 包含 AH 認證演算法、秘密金鑰等等。
- ESP 加密 (ESP Encryption): 包含 ESP 加密演算法、金鑰、IV 模式等等。
- SA 壽命(Lifetime of SA): 表示此筆 SA 的存活時間。在這存活時間內，此 SA 可連續重複使用。
- IPSec 協定模式(IPSec Protocol Mode): 此欄位是記錄此 SA 的安全協定(AH 或 ESP) 所採用的操作模式，可能是傳輸模式、通道模式、或任意。
- 路徑的最大傳輸量 (Path MTU): 此欄位記錄著此 SA 的最大傳輸量 (Maximum Transfer Unit, MTU)。如果 IP 封包的長度超過這個量，就必須經由分段傳輸。

其中 SA 壽命參數表示該筆 SA 的存活時間，這也表示並非每次通訊時都必須重新建立安全關聯（人工輸入或 ISAKMP 協定建立），在這有效期間內安全關聯是可以重複使用的。另一方面，當某一筆安全關聯被參考使用時，序號計數器便會增加計數，因此計數器除了接收端可以避免重複攻擊外，傳送端也可依此計數內容，了解安全關聯被使用的情況。