200830815

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：96101324

※申請日期：96.1.12　　※IPC 分類：H04L 29/06

一、發明名稱：（中文/英文）

多點對多點網路通訊安全協定虛擬私有網路通道結構及其實現方法。

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

威創科技股份有限公司

代表人：（中文/英文）高育仁

住居所或營業所地址：（中文/英文）

新竹科學工業園區展業一路 9 號 5 樓之 3

國　籍：（中文/英文）中華民國 TW

三、發明人：（共 1 人）

姓　名：（中文/英文）

林南宏

國　籍：（中文/英文）

中華民國 TW

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

一種虛擬私有網路的結構及其實現方法，特別是關於一種多點對多點的 IPsec 私有網路的結構及其實現方法。

【先前技術】

虛擬私有網路(Virtual Private Network)是利用適用於特定中介網路之虛擬私有網路通道協定，建立一個單向或雙向的虛擬通道，將兩個沒有直接相連的區域網路連接起來，進而形成單一個虛擬區域網路的技術。較常見的虛擬私有網路通道協定有 PPTP、L2F、L2TP、IPsec、MPLS 等等。

目前全球最大、最廣為使用的網路是使用網際網路協定的網際網路。因此，當企業及機關有遠距建構虛擬私有網路之需求時，最常使用的中介網路也是網際網路。IPsec 就是因應這樣的需求而產生，適用於使用網際網路協定之中介網路的虛擬私有網路技術。由於網際網路是公開的全球性網路，對其上所傳送的資料也不提供保全的服務，針對此缺點，IPsec 利用 Authentication Header、Encapsulating Security Payload、Inetnet Security Association and Key Management Protocol、Internet Key Exchange Protocol 等等協定，提供存取控制、資料完整性、資料認證、抗重播保護、資料機密性、及有限度的流量機密性等等保全服務，以保全的虛擬通道來連接兩端的區域網路。利用網際網路及 IPsec 虛擬私有網路技術，企業及機關可以用極少的成本，建構出安全的、涵蓋全球的虛擬區域網路。因此，IPsec 虛擬私有網路技術在經濟及通訊上都十分重要。

在 IPsec 的架構中，Security Association (SA)是整個架構的核心。

SA 定義了傳送者、接收者、其間所傳送之封包所承載的資料類別，以及該套用哪些保全措施。多個 SA 間則以目的地 IP 位址、保全協定識別碼、以及保全參數索引來做區分。由於單一個 SA 只定義兩個網站或兩個閘道間的單向保全服務協議，因此一個雙向的虛擬私有網路通道必須使用兩個 SA。

由於區分 SA 時並未用到來源 IP 位址，所以除了一般常見的單點對單點單向虛擬私有網路通道，理論上也可以建構出多點對單點的單向虛擬私有網路通道。但是，由於用來區分 SA 的項目包含了目的地 IP 位址，所以無法建構出單點對多點及多點對多點的單向虛擬私有網路通道。因此，根據 IPsec 現有的技術及規範，無法建構出多點對多點的虛擬私有網路通道。

如第 1 圖所示，傳統利用單點對單點雙向虛擬私有網路通道連接起來的虛擬私有網路存在嚴重的缺點。假設閘道 G_A4 及 G_B8 間以網際網路位址 IP_{A1} 及 IP_{B1} 建立了一條用來連接區域網路 LAN_A2 及 LAN_B6 的虛擬私有網路通道。由於虛擬通道兩端的閘道 G_A4 及閘道 G_B8 只能使用位址 IP_{A1} 及 IP_{B1} 來相互通訊，因此閘道 G_A4 及閘道 G_B8 也就只能各自使用網際網路連線 WAN_{A1} 及 WAN_{B1} 來收送屬於該虛擬私有網路通道的封包。倘若網際網路連線 WAN_{A1}、WAN_{B1}、或其中介網路的路由發生線路傳輸品質下降或中介閘道發生壅塞等等狀況而造成該虛擬私有網路通道的封包遺失，虛擬私有網路的可靠度、可用度就會下降。倘若網際網路連線 WAN_{A1}、WAN_{B1}、或其中介網路有鏈路發生斷線的狀況，虛擬私有網路就會被破壞而分裂成原來的兩個獨立網路 LAN_A2 及 LAN_B6。

因應這個缺點，使用者必須以手動或自動的方式使用其它的網際網路

連線來建立新的 IPsec 虛擬私有網路通道，以重新建立虛擬私有網路。例如，當 WAN_{B1} 斷線時，可以用 IP_{A1} 與 IP_{B2} 或者 IP_{B3} 建立新的虛擬私有網路通道。這樣的做法使用上相當複雜及困難。以第 1 圖為例，為了縮短重新建立虛擬私有網路通道的時間，閘道 G_A4 及閘道 G_B8 都必須預先設定好 6 組虛擬私有網路組態，然後用手動選擇或依預先設定的優先順序自動選擇要使用的組態。另一方面，倘若 WAN_{A2}、WAN_{B2}、WAN_{B3}、只用做備援，這種做法會大量增加建置及維運成本。

再者，由於閘道在同一時間只能使用單一條網際網路連線來收送虛擬私有網路通道的封包，因此虛擬私有網路的頻寬便受限於單一條網際網路連線的頻寬。想要擴增虛擬私有網路的頻寬，只能換接更高頻寬的網際網路連線。但實際上，高頻寬的網際網路連線往往不成比例地，遠較一般常用的網際網路連線昂貴許多。此外，即使使用多點對單點虛擬私有網路通道連接起來的虛擬私有網路，在接收虛擬私有網路通道封包時仍只能使用單一條網際網路連線。對可靠度、可用度、頻寬、及成本等等並不能有所改善。因此，實際應用時不會採用多點對單點的方式建立虛擬私有網路通道，因此本發明提出一種技術來改善傳統的缺失。

【發明內容】

本發明是一種多點對多點 IPsec 虛擬私有網路通道結構及其實現方法，用以大幅提高廣域網路鏈路及路由容錯性。該結構包含一來源網路通訊安全協定虛擬私有網路閘道器與至少一目的地網路通訊安全協定虛擬私有網路閘道器，該來源通訊安全協定虛擬私有網路閘道器與該目的地通訊

安全協定虛擬私有網路閘道器並各自連結到各自的區域網路；一廣域網路，該來源通訊安全協定虛擬私有網路閘道器與該目的地通訊安全協定虛擬私有網路閘道器連接到該廣域網路，並配置不同的 IP 位址給每一個廣域網路連線，該來源網路通訊安全協定虛擬私有網路閘道器所配置且由網路管理者選定的多個 IP 位址將會透過該廣域網路連到該目的地網路通訊安全協定虛擬私有網路閘道器上所配置且由網路管理者選定的多個 IP 位址來構成一個多點對多點網路、全網式路由的 IPsec 虛擬私有網路通道來接收及傳送虛擬私有網路通道封包，同時封包傳送方式也是採用無耗消以相容於傳統的虛擬私有網路技術及設備。配合端點偵測技術及路徑演算法，能夠找出並避用傳送路徑中的不可靠的路由區段並妥善處理多點對多點架構所產生的封包順序錯亂。因此 IPsec 虛擬私有網路通道技術可以更可靠、更有彈性、且具備容錯及負載均衡特性。

【實施方式】

本發明是一種建構多點對多點 IPsec 虛擬私有網路通道的裝置及其實現方法。以多點對多點全網式路由的方式接收及傳送虛擬私有網路通道封包。

主要的概念就是將每個閘道的每一個連接到廣域網路連線的外部網路介面連結到另一個閘道的每一個連接到廣域網路連線的外部網路介面以構成全網式路由。第 2 圖為本發明的實施例之一，以一個含有兩個外部網路介面的閘道 G_A14 連接到含有三個外部網路的閘道 G_B18 為例。閘道 G_A14 以其內部網路介面連接到區域網路 LAN_A12，以兩個外部網路介面連接廣域網路

連線 WAN_{A1} 及 WAN_{A2}，並分別配置 IP 位址 IP_{A1} 及 IP_{A2}；閘道 G_B18 以其內部網路介面連接到區域網路 LAN_B16，以三個外部網路介面連接廣域網路連線 WAN_{B1}、WAN_{B2} 及 WAN_{B3}，並分別配置 IP 位址 IP_{B1}、IP_{B2} 及 IP_{B3}。因此，由 G_A14 經網際網路到 G_B18 的全網式路由包含[$IP_{A1}..IP_{B1}$]、[$IP_{A1}..IP_{B2}$]、[$IP_{A1}..IP_{B3}$]、[$IP_{A2}..IP_{B1}$]、[$IP_{A2}..IP_{B2}$]、及[$IP_{A2}..IP_{B3}$]等六個路由；由 G_B18 經網際網路到 G_A14 的全網式路由包含[$IP_{B1}..IP_{A1}$]、[$IP_{B1}..IP_{A2}$]、[$IP_{B2}..IP_{A1}$]、[$IP_{B2}..IP_{A2}$]、[$IP_{B3}..IP_{A1}$]、及[$IP_{B3}..IP_{A2}$]等六個路由。所以所需的路由數量可以從閘道與閘道連接到廣域網路連線的外部網路介面數量互乘來算出，例如 2x3=6。

第 3 圖為本發明的內部運作流程圖。傳統單點對單點 IPsec 虛擬私有網路閘道只由步驟 S1、S2、及 S3 所組成。本發明的多點對多點 IPsec 虛擬私有網路功能涵蓋步驟 S4 到 S13。首先，如步驟 S1 到 S2 所示，網路管理者必須先設定本地閘道及遠端閘道分別要用來建立單點對單點 IPsec 虛擬私有網路的本地端點及遠端端點，以及用來將其轉換成多點對多點 IPsec 虛擬私有網路所使用的本地端點群組及遠端端點群組。使用 IP 位址或網域名稱來指定端點皆可。以下敘述皆以使用 IP 位址為例。以第 2 圖為例，網路管理者可以選用端點 IP_{A1} 及 IP_{B1} 來建立單點對單點 IPsec 虛擬私有網路，並使用端點群組 IPG_A22(包含 IP_{A1} 及 IP_{A2})及端點群組 IPG_B24(包含 IP_{B1}、IP_{B2}、及 IP_{B3})，將單點對單點 IPsec 虛擬私有網路轉換成多點對多點 IPsec 虛擬私有網路。對閘道 G_A14 而言，IPG_A22 稱為本地端點群組，IP_{A1}、IP_{A2} 稱為本地端點；IPG_B24 稱為遠端端點群組，IP_{B1}、IP_{B2}、IP_{B3} 稱為遠端端點。

接下來是步驟 S4，維護本地及遠端端點群組定義、各端點群組中各端點的可用性、以及各本地端點和各遠端端點間之網際網路路由的可用度，供其它步驟查詢及更新。而步驟 S5 會持續監測本地端點的可用性，並在本地端點可用性發變動時更動步驟 S4 中本地端點群組裏對應端點的可用性，並主動發出端點狀態通報訊息給每一個遠端 IP 群組中的每一個端點。步驟 S5 也會定期送出端點狀態查詢訊息給每一個遠端端點群組中的每一個端點，查詢各個遠端端點群組中所有端點的可用性。在收到對端閘道送來的端點狀態查詢訊息時，步驟 S5 一方面會用訊息中的端點可用性來更新步驟 S4 中遠端端點的可用性，一方面也將本地端點群組中各端點的可用性放入端點狀態查詢回應訊息中，回報給遠端的閘道。若是收到的是對端閘道回送的端點狀態查詢回應訊息，步驟 S5 只會更新步驟 S4 中的遠端端點的可用性。

在傳送方向上，步驟 S6 使用步驟 S4 中的資訊，查驗進入的單點對單點 IPsec 虛擬私有網路封包是否需要轉換成多點對多點 IPsec 虛擬私有網路封包。若是，則進入步驟 S7；若否，則跳至步驟 S3，直接將封包傳送經由步驟 S3 傳送出去。在此假設封包的來源 IP 位址為 IP_{A1}，目的地 IP 位址為 IP_{B1}，屬於須要進行轉換的封包。步驟 S7 使用步驟 S4 所提供的本地及遠端端點群組、端點可用性、及路由可用度，配合選定的負載均衡演算法，以封包為單位，藉由逐個選定新的、可用、且適當的本地端點及遠端端點(假設分別為 IP_{A2} 及 IP_{B3})的方式，選擇一條適當的新路由。然後連同封包本身一併交給步驟 S8。舉例來說，根據第 2 圖如果本地及遠端都使用循環演算

法，則會依序使用 IP_{A1}、IP_{A2}做為新的本地端點；依序使用 IP_{B1}、IP_{B2}、IP_{B3}做為新的遠端端點。也就是依序使用[IP_{A1}..IP_{B1}]、[IP_{A2}..IP_{B2}]、[IP_{A1}..IP_{B3}]、[IP_{A2}..IP_{B1}]、[IP_{A1}..IP_{B2}]、及[IP_{A2}..IP_{B3}]等六條路由。步驟S8以新的本地端點IP位址(IP_{A2})及新的遠端端點IP位址(IP_{B3})取代封包中的來源IP位址(IP_{A1})及目的地IP位址(IP_{B1})，並進行必要的IP協定表頭維護。步驟S9負責將封包佇列到新的本地端點IP位址(IP_{A2})所對應的網路介面等待傳送，並將封包暫存至對應SA的時限暫存區中，以支援後續可能發生的封包重送須求。當封包暫存時間超過設定時限時，時限暫存區會將該封包丟棄。另外，發生滿溢時，時限暫存區則會將最舊的封包丟棄。步驟S3利用網路介面，經由IP_{A2}所對應的WAN_{A2}，將封包傳送到外部的網際網路。如果此封包沒有因為中介網路的路由發生線路傳輸品質下降、斷線、或中介閘道發生壅塞而遺失，則封包會經由網際網路路由[IP_{A2}..IP_{B3}]抵達閘道G_B18。

在接收方向上，閘道會將由對端閘道之步驟S5所送來的端點狀態查詢訊息交給本地的步驟S5。如果收到的是要求重送特定封包的訊息，則要求步驟S10進行指定封包重送。至於IPsec虛擬私有網路封包則交給步驟S11處理。步驟S10收到對端閘道送來的封包重送須求訊息時，會從步驟S9的封包暫存區中複製要重新傳送的封包交給步驟S7，由步驟S7重新給定新的本地端點及新的遠端端點後重新傳送。步驟S10同時也根據此封包重送須求訊息，更新所對應之網際網路路由的可用度。另外，當步驟S10收到本地步驟S13的封包重送須求時，步驟S10會產生新的封包重送須求訊息，

並將之傳送給對應的對端閘道。步驟 S11 使用步驟 S4 所提供的端點群組定義，辨別所收到的封包。若封包屬於多點對多點 IPsec 虛擬私有網路，則交給步驟 S12；若封包不屬於任何多點對多點 IPsec 虛擬私有網路，則直接交給步驟 S2 處理。步驟 S12 利用步驟 S11 傳來的端點群組資訊將封包 IP 協定表頭裏的來源及目的地 IP 位址改回原來的值(以前面的例子而言，是將來源 IP 位址由 IP_{A2} 改回 IP_{A1}，將目的地 IP 位址由 IP_{B3} 改回 IP_{B1})，並進行必要的 IP 協定表頭維護，然後交給步驟 S13。步驟 S13 依 SA 及 IPsec 協定表頭中的傳送序號將收到的 IPsec 虛擬私有網路封包重新排序，並佇列到所屬之 SA 的暫存區中等待送交步驟 S2 處理。需要這麼做的原因是因為使用不同本地端點或遠端端點的封包會從不同的網際網路路由(本例中，每個方向都有六個網際網路路由可用)到達對端閘道且各路由的傳送延遲各異，步驟 S13 接收到封包的順序會與封包在對端閘道從步驟 S2 進入步驟 S6 時的順序不同，無法保持同樣的順序性。在封包序號連續的情況下，步驟 S13 會依序將封包交給步驟 S2 處理。遇到不連續封包時，步驟 S13 會在不連續情況維持超過設定時限時，透過步驟 S10 傳送封包重送須求訊息給對端閘道的步驟 S10，請求其重新傳送所指定的封包。

惟以上所述者，僅為本發明之較佳實施例而已，並非用來限定本發明實施之範圍。故即凡依本發明申請範圍所述之形狀、構造、特徵及精神所為之均等變化或修飾，均應包括於本發明之申請專利範圍內。

【圖式簡單說明】

第 1 圖為單點對單點 IPsec 私有網路示意圖。

第 2 圖為多點對多點 IPsec 私有網路示意圖。

第 3 圖為內部運作流程示意圖。

【主要元件符號說明】

2　區域網路 A

4　閘道 A

6　區域網路 B

8　閘道 B

12　區域網路 A

14　閘道 A

16　區域網路 B

18　閘道 B

五、中文發明摘要：

本發明是關於一種多點對多點的網路通訊安全協定(IPsec)虛擬私有網路通道結構及其實現方法。以多點對多點全網式路由的方式接收及傳送虛擬私有網路通道封包來取代傳統的單點對單點。同時配合端點偵測技術及路徑演算法，可以在不變動原有的規格下，設計出較目前 IPsec 虛擬私有網路通道技術更可靠、更有彈性、且具備容錯及負載均衡特性的 IPsec 虛擬私有網路技術。

六、英文發明摘要：

十、申請專利範圍：

1．一種多點對多點網路通訊安全協定虛擬私有網路通道結構，包含：

一來源通訊安全協定虛擬私有網路閘道器與至少一目的地通訊安全協定虛擬私有網路閘道器，該來源通訊安全協定虛擬私有網路閘道器與該目的地通訊安全協定虛擬私有網路閘道器並各自連結到各自的區域網路；以及

一廣域網路，該來源通訊安全協定虛擬私有網路閘道器與該目的地通訊安全協定虛擬私有網路閘道器連接到該廣域網路，並配置不同的 IP 位址給每一個廣域網路連線，該來源網路通訊安全協定虛擬私有網路閘道器所配置且由網路管理者選定的多個該 IP 位址將會透過該廣域網路連到該目的地網路通訊安全協定虛擬私有網路閘道器上所配置且由網路管理者選定的多個該 IP 位址來構成一個多點對多點網路、全網式路由的 IPsec 虛擬私有網路通道。

2．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該來源閘道器與該目的地閘道器內部各含有一內部網路介面卡與至少一外部網路介面卡。

3．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器採用全網式路由傳送封包。

4．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器的替換封包來源和目的地 IP 位址、無耗消的封包傳送技術相容於傳統虛擬私有網路技

術的方式。

5．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器主動發布本地端點可用性至所有遠端閘道之每一個端點。

6．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器會對所有遠端目的地閘道器的每一個端點查詢該遠端目的地閘道器所有端點可用性。

7．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器以封包為單位，使用負載均衡演算法、端點可用性、及外部網際網路路由可用度，逐個選擇網際網路路由。

8．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器依不同的安全協會，各別對傳送封包做限時暫存來支援封包重送。

9．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器以網路通訊安全協定協定表頭中之封包序號解決多路由傳輸延遲差異所引發之封包順序錯亂問題。

10．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器以網路通訊安全協定協定表頭中之封包序號解決封包遺失及支援封包重送。

11．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器使用延遲式及指定式的封包重新傳送的方式。

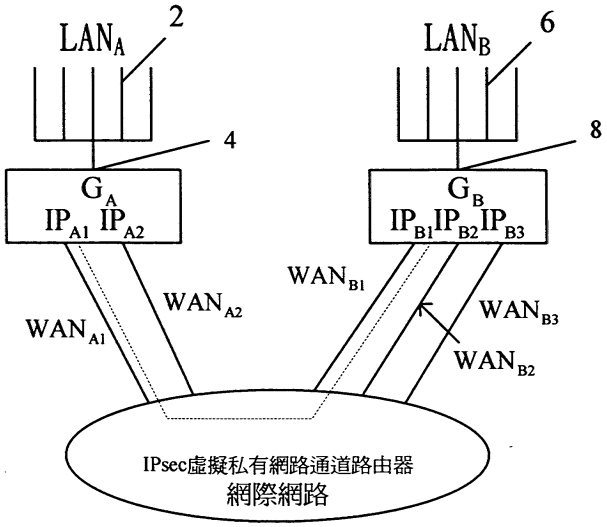
12．申請專利範圍第 1 項所述之多點對多點網路通訊安全協定虛擬私有網路通道結構，其中該網路通訊安全協定虛擬私有網路閘道器以封包重送來統計及計算路由可用度。

13．一種建構多點對多點網路通訊安全協定虛擬私有網路通道的方法，包含：

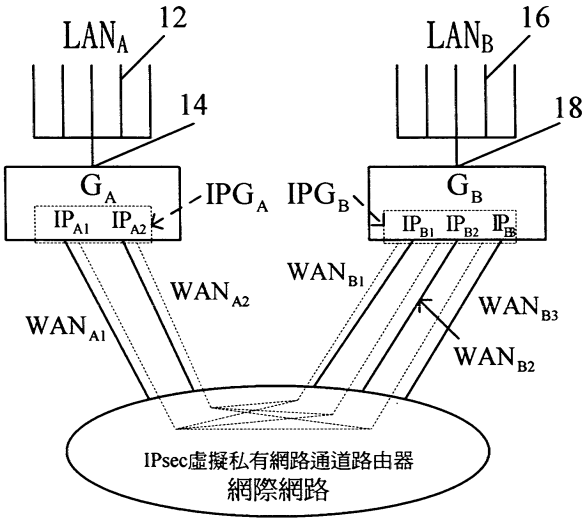
將一個來源網路通訊安全協定虛擬私有網路閘道器透過一個廣域網路連接到至少一個目的地網路通訊安全協定虛擬私有網路閘道器；

對每一個廣域網路的連線配置 IP 位址；以及

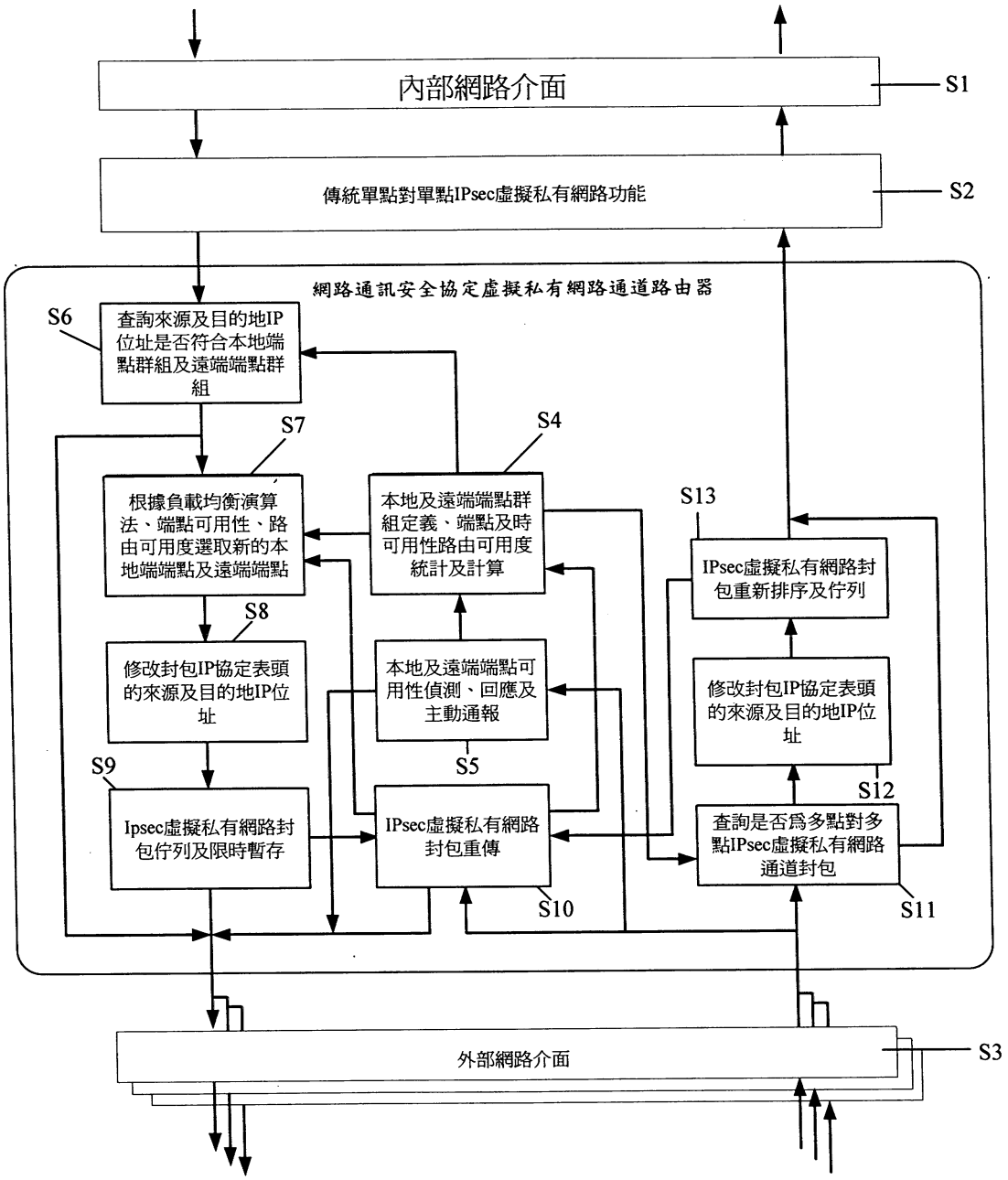
將該來源網路通訊安全協定虛擬私有網路閘道器裡所配置且由網路管理者選定的多個 IP 位址連到該目的地網路通訊安全協定虛擬私有網路閘道器所配置且由網路管理者選定的多個 IP 位址來構成全網式路由。


LAN$_A$
2
LAN$_B$
6
4
8
G$_A$
IP$_{A1}$ IP$_{A2}$
G$_B$
IP$_{B1}$IP$_{B2}$IP$_{B3}$
WAN$_{B1}$
WAN$_{A2}$
WAN$_{B3}$
WAN$_{A1}$
WAN$_{B2}$
IPsec虛擬私有網路通道路由器
網際網路

第1圖（先前技術）


LAN$_A$
12
LAN$_B$
16
14
18
G$_A$
IPG$_A$
IPG$_B$
G$_B$
IP$_{A1}$ IP$_{A2}$
IP$_{B1}$ IP$_{B2}$ IP$_{B3}$
WAN$_{B1}$
WAN$_{A2}$
WAN$_{B3}$
WAN$_{A1}$
WAN$_{B2}$
IPsec虛擬私有網路通道路由器
網際網路

第2圖


內部網路介面
S1
傳統單點對單點IPsec虛擬私有網路功能
S2
網路通訊安全協定虛擬私有網路通道路由器
S6
查詢來源及目的地IP位址是否符合本地端點群組及遠端端點群組
S7
S4
根據負載均衡演算法、端點可用性、路由可用度選取新的本地端端點及遠端端點
本地及遠端端點群組定義、端點及時可用性路由可用度統計及計算
S13
IPsec虛擬私有網路封包重新排序及佇列
S8
修改封包IP協定表頭的來源及目的地IP位址
本地及遠端端點可用性偵測、回應及主動通報
修改封包IP協定表頭的來源及目的地IP位址
S9
S5
S12
Ipsec虛擬私有網路封包佇列及限時暫存
IPsec虛擬私有網路封包重傳
查詢是否爲多點對多點IPsec虛擬私有網路通道封包
S10
S11
外部網路介面
S3

第3圖

七、指定代表圖：

(一)、本案代表圖為：第 2 圖

(二)、本代表圖之元件符號簡單說明:

2　　區域網路 A

4　　閘道 A

6　　區域網路 B

8　　閘道 B

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：