申請日期：89. 11. 23	案號：89124867	公告本
類別：G06F 13/00 G06F 15/16 H04L 9/00		

（以上各欄由本局填註）

發明專利說明書 494301

一、發明名稱	中文	使用區域網際網路通訊協定位址及不可移轉之位址埠於區域網路的網路位址轉換途徑
	英文	NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA ENTWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE PORT ADDRESSES
二、發明人	姓名（中文）	1.以色列・丹尼爾・蘇丹
	姓名（英文）	1.Israel Daniel Sultan
	國籍	1.法國
	住、居所	1.法國巴黎 75013 西羅路 9 號
三、申請人	姓名（名稱）（中文）	1.能聯有限公司
	姓名（名稱）（英文）	1.NEXLAND, INC.
	國籍	1.美國
	住、居所（事務所）	1.美國佛羅里達州 33180 邁阿密市 20801 比斯肯大道 403室
	代表人姓名（中文）	1.葛瑞格・S・拉威
	代表人姓名（英文）	1.GREGORY S. LEVINE

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
美國 US	2000/03/03	09/518,399	有

有關微生物已寄存於　　寄存日期　　寄存號碼

無

五、發明說明 (1)

[發明背景及習知技術]

使用傳輸控制通訊協定/網路通訊協定(Transmission Control Protocol/Internet Protocol，簡稱TCP/IP)的虛擬私有網路(Virtual Private Networking，簡稱VPN)能夠安全、快速的在遠端電腦網站間通訊，該等電腦網站使用網際網路做為通訊媒介。在遍布於網際網路的網站間所傳輸的資訊能夠被保護防止不受歡迎的攔截者或惡意的電腦駭客以種種安全手段攔截，有效的安全措施至少必須包含能夠確保任何或所有以下保護的功能：資料完整性-在資料傳輸時防止無意的或惡意的修改、使用反重覆(Anti-repeat)手段以避免遭到拒絕服務攻擊(Denial-of-service Attacks)、來源確認、傳輸時來源位址及其它資訊標頭之保密及封包承載保護以防止不受歡迎的攔截。提供網際網路安全的一種標準模式是網際網路通訊協定安全群組(Internet Protocol Security suite，簡稱IPSec)，IPSec與TCP/IP通訊協定運作能夠提供連結網際網路或與網際網路連接之私有區域網路(Local Area Network，簡稱LAN)的裝置間的安全通信。

TCP/IP協定群組使用網際網路通訊協定(Internet Protocol，簡稱IP)位址確認在電腦網路上的每一個裝置，一個全域IP位址唯一地表示在網際網路上的一個裝置，此裝置可以是電腦、印表機、路由器、交換器、閘道或其它網路裝置，裝置擁有全域IP位址能夠被直接參考當作在網際網路上的來源或目的地，然而此TCP/IP通訊協定

五、發明說明 (2)

不是專有的被限制在網際網路上，而同樣的能夠被使用在私有區域網路上。私有區域網路使用TCP/IP通常使用「區域」IP位址於網路裝置，儘管在私有區域網路上沒有兩個裝置能夠共用相同的區域IP位址，但私有區域網路是被從網際網路隔離出來的，在區域網路上的區域裝置是無法從網際網路顯示。因此，區域裝置之IP位址不必須是"全域"唯一的。使用區域IP位址的區域網路將被透過閘道連結到網際網路，該閘道是一種可以過濾或遞送區域網路與網際網路間訊息的裝置。因為閘道是直接指定到網際網路上，且是在網際網路上可顯示的，所以閘道必須於整個網際網路通訊有一個全域唯一的IP位址，然而，因為區域網路無法直接從網際網路顯示，所以在區域網路上的區域裝置不需要全域唯一的IP位址。

TCP/IP是一種使用於網際網路上之通訊協定，使用TCP/IP傳輸的資訊是被包含在資料封(Datagram)中，一個資料封是由一個被貼上一個或多個標頭的分離資訊封包(Packet)所組成，標頭包含TCP/IP指定封包到其所預定的目的地及確保其傳輸時適當的操作所需的資訊，每一個資料封獨立地可尋找位址的，且可為一個連接導向傳輸TCP之資料封或一個無連接傳輸模式使用者資料封通訊協定(User Datagram Protocol，簡稱UDP)之資料封。每一個UDP資料封包含一IP標頭及一UDP標頭。IP標頭包含至少一"來源"IP位址及一"目的地"IP位址，而UDP標頭則包含來源及目的地服務位址(埠位址-以數字表示)。在IPv4方

五、發明說明 (3)

面，IP位址長度為32位元且為目前常用的xxx.xxx.xxx.xxx格式。在此格式中，每三個數字段為一二進位八位元，係表示一個介於0至225間的數。一個完整的IP位址結合了一邏輯網路或網路段位址與網路上的結點(裝置)位址，網路或網路段位址可包含IP位址前三、六或九個數，網路或網路段上的裝置是以結點位址來確認，而結點位址是由網路或網路段位址中未使用之剩餘的數所組成。

來源及目的地服務位址包含在一UDP標頭裡的16位元數，所知的如"埠位址(ports)"或"座位址(sockets)"，用來指示封包到一個預定程序，也就是在傳送或接收裝置中的動作。使用於此中，"埠"或"埠位址"一詞係參照一儲存在UDP標頭的服務位址，儘管在理論上有許多埠的位址是16位元數，藉著協定，許多的埠位址已被保留給已制定的程序。因此，例如埠80是保留給超文件的通訊協定(HyperText Transfer Protocol，簡稱HTTP)，而埠20及21是保留給檔案傳輸協定(File Transfer Protocol，簡稱FTP)，透過使用埠位址，到達一運作一個以上程序的區域機置裝置的資料將被指示到預設的程序。一運作在區域主機的程序並不是保留的程序之一，區域主機可以從一群未被預訂的埠位址號碼中選出任何一個埠位址號碼來確認「來源」程序，回傳封包則參考"目的"檔內的位址號碼而被指示到前述程序上。。

在近十年裡網際網路使用的爆發性成長及未來的預計

五、發明說明（4）

成長，全域唯一的IP位址已經成為一個稀有的資源，此外，許多企業維護私有區域網路有極少甚至沒有必要為每一個在區域網路中的電腦或裝置設置唯一全域IP位址，許多此類企業在各種情況下會寧可保持他們電腦IP位址的機密，而不是為每一部區域裝置設置全域唯一的IP位址而浪費少數全球資源，許多私有區域網路利用區域IP位址於區域網路的裝置上，為了提供網際網路上的連結，此類區域網路將利用一全域唯一性位址被使用在以閘道(Gateway)分隔區域網路及網際網路的網際網路上。

透過使用網路位址轉換技術(Network Address Translation，簡稱NAT)，閘道裝置將區域網路由網際網路分離能夠提供類似防火牆(Firewall)的防備措施，同時使具有區域IP位址的機置能夠透過閘道唯一全域位址以進入網際網路。一個在區域網路上的裝置可有一個靜態區域IP位址或一個開機動態指定的區域IP位址，前述閘道以區域IP位址提供一個轉換表給在區域網路上的每一個裝置。一個UDP封包被分別地從區域機置傳送並針對網際網路指定到將擁有此區域IP位址及被確認在IP及UDP標頭來源檔之埠位址，前述閘道將接收來自區域機置的封包，並將代替此封包外部全域唯一IP位址及一個新的埠位址(從一群未使用、未預訂的埠位址中取得)成為IP及UDP標頭的來源檔，其次將更新週期重覆檢查(Cyclical Redundancy Check，簡稱CRC)並更改任何必須的更新以確保資料完整，接著將傳送出封包到網際網路上，如同程序的部份，

五、發明說明 (5)

閘道將更新其內部轉換表以交叉參考前述區域機置之IP位址與機置原來傳達的來源埠位址，以及被指定至網際網域封包之新的來源埠位址以及目的地IP位址，在接收到網際網路的回傳之後，閘道將辨識本身擁有在封包標頭內的IP位址，並將檢查進來的封包目的地埠位址，如果在其內部轉換表中發現前述目的地位址，則閘道將取代此交叉參考區域機置之IP位址及原始埠位址以成為封包之目的地檔，並將更新CRC及任何其它必須的參數，接著發送封包到將被區域機置接收並被指示適當程序的區域網路。在此一實施例中，一些在區域網路上的電腦只擁有區域IP位址能夠透過一種全域唯一IP位址傳訊於整個網際網路。

雖然NAT閘道提供防火牆安全防禦以防止區域網路從網際網路直接存取，但不提供安全防禦防止於網際網路上傳輸時的攔截或區域網路預定封包的修改，並且無法保證起源於區域網路挑戰之"可靠性"，因此，藉由IPSec提供的安全防禦對於區域網路與網際網路連繫時必需維護安全性來說是必須的。

IPSec的一般實施例是提供安全性於由至少一個主要運算網站或一個以上之遠端區域網路組成之虛擬企業網路，主機與遠端區域網路連結於網際網路，使用高速媒介於網站間傳輸以取代可觀且較昂貴的私有專線。然而使用網際網路為一傳輸媒介的缺點是網際網路固有地危險以及提供極小或沒有固有的保護以防止窺視、偵查、"惡作劇"或者到最後遭駭客偷竊、修改或訊息轉換，因此，在要求

五、發明說明 (6)

安全資料傳輸時有廣泛的安全措施需要，IPSec通訊協定實施安全措施確保資料的正確及資料完全。

IPSec通訊協定群組實施安全措施於多層開放性系統連結(Open Systems Interconnection，簡稱OSI)網路參考模組之網路層上，此群組包含一些獨立的通訊協定用於與其它通訊協定互相連結以確保UDP資料封承載資訊於網際網路之安全性，IPSec子系統的基本結構解釋於Security Architecture for the Internet Protocol之附錄2401，作者S. Kent及R. Atkinson(1998年11月)。確認標頭(Authentication Header，簡稱AH)通訊協定確保資料完整性、來源確認以及納入反重覆措施以阻斷拒絕服務攻擊。概括安全性承載(Encapsulation Security Payload，簡稱ESP)通訊協定係提供與AH類似的保護，但額外增加了承載加密的特性，AH及ESP標頭皆含有安全性參數索引(Security Parameters Index，簡稱SPI)檔，SPI是一個32位元使用於確認資料封之安全性結合的假隨機值。更進一步通訊協定之相關資訊可參照IP Authentication Header之附錄1826，作者R. Atkinson (1995年8月)及IP Encapsulating Security Payload(ESP)，作者S. Kent及R. Atkinson (1998年11月)。網際網路安全關聯與密鑰管理協議/密鑰確認協議(ISAKMP/Oakley，Internet Security Association and Key Management Protocol)一般被稱為網際網路密鑰交換(Internet Key Exchange，簡稱IKE)為一種交握協定

五、發明說明 (7)

(Handshaking)，用以建立介於兩個主機之間安全協議之參數，並提供密鑰交換及其它用於執行安全的協議及允許加密資料傳輸之安全資訊，ISAKMP/Oakley通訊協定(此後簡稱為ISAKMP)包含未加密資訊之初始交換，用以提供可從鑑定建立初始資料之機置與資料加密產生，這些程序說明可參考The Internet Key Exchange之附錄2409，作者D. Harkins及D. Carrel(1998年11月)。一旦安全性參數足夠建立已交換之主機之間的安全協定時，則所有之後的傳輸將被加密並依照協議的通訊協定充分地鑑定，此時，ISAKMP通訊協定終止，其後的定址是基於每一部機置的IP位址和那段期間機置的SPI。前述SPI對於每一個機置在一個期間來說是唯一的，私有區域網路的閘道裝置將維護一個內部表SPI-in值，用以交叉參考前述區域機置的IP位址，並且"SPI-out"是交叉參考在網際網路上與區域機置通訊的機置的IP位址。針對每個SPI的機置是於ISAKMP傳送期間資訊交換計算而來，並承載於被附加至UDP封包的AH或ESP標頭，因為IPSec通訊協定可被套用在各式各樣的環境以提供安全防禦或一個可能包含AH及ESP報標頭兩者的單獨資料封或可能將一些標頭資訊加密。

每一個前述的安全通訊協定藉由置換封包上新的標頭資訊來修改，在封包內部修改特定檔案以符合正在使用之通訊協定，並且在某些情況下對承載及所有或部份其他封包標頭加密。因此，根據IPSec，當一個UDP資料封經過一個"安全的"傳輸區域到一個不可信賴的網路時，其通常由

五、發明說明 (8)

一個IP標頭、AH或ESP標頭(或兩者)以及一個壓縮承載所組成，標頭資訊將包含一個目的地位址、一個SPI以及充份的安全協議(Security Associations，簡稱SAs)資訊以確認資料封到達此目的地並能夠鑑定目的地主機。承載的封裝確保被包含在承載裡的資訊拒絕不需要的竊聽者及駭客的要求。資料封最初的目的地主機可能是一個路由器、閘道或介於區域網路及網際網路間的防火牆。依據達成介於區域網路及網際網路邊界上的裝置，為了分析進一步的位址資訊，資料封可能會整個或部份被打開、檢查或解密並且被安排到一個在區域網路上的區域IP位址。

在IPSec的使用的ISAKMP交握協定中，需要兩台主機間使用一個特殊程序埠位址(埠位址500)用於最初的訊息交換以預先制定一個介於兩主機間的安全協議，基於此原因，埠位址500已經被指定為與ISAKMP通訊協定專用。透過協定，電腦嘗試藉著利用ISAKMP協定議定安全通訊參數，必須完全的透過每一部電腦的埠位址500通訊，也就是說，從任何一部電腦來的ISAKMP訊息必須確認埠位址500和來源及目的地埠位址位址兩者一樣，如果任何一部電腦接收一個埠位址500沒有規定為來源及目的地的封包，則此封包將被丟棄。

雖然此協定提供保證兩主機是互相通訊，但當某一個主機是位於區域網路使用區域IP位址及NAT閘道時，此協定就變得無法運作。例如，主機A，在一個遠端區域網路上擁有一個區域IP位址並以一個NAT閘道保護，欲與位於

五、發明說明 (9)

一個主要伺服電腦網站主機B上建立一個安全協議，主機A則藉由傳送一個未加密的UDP資料封到主機B來建立通訊協定，以"目的地"作為主機B的IP位址，並以目的地埠位址位址為"埠位址500"，然而，當前述資料封到達NAT閘道與遠端區域網路連結到網際網路時，此閘道將轉譯此目的地埠位址位址成為一個專屬的埠位址號碼，位於主機B的資料封抵達後，ISAKMP通訊協定將無法被辨識且主機B將不做反應，電腦間的安全協議制定則失敗，基於前述困難之處，此協定已經被相信ISAKMP協定無法被用於利用遠端區域網路上每一台電腦使用區域而非全域IP位址之NAT閘道建立VPN閘道。

因此，本發明之主要目的係提供一閘道裝置，其允許以網際網路為傳輸媒介，使用ISAKMP通訊協定鑑定及密鑰交換於擁有非全域IP位址之電腦及主機之間。

本發明之另一目的係提供一閘道裝置，其允許位於私有區域網路上之任何電腦使用區域IP位址，經由網際網路使用ISAKMP協定建立或接收訊息。

本發之再一目的係提供一種使用ISAKMP協定建立安全通訊於利用虛擬私有網路於網際網路上兩個或多個區域網站的方法。

以上及其它本發明之目的將透過以下詳細說明揭露。

[發明概述]

本發明係於遠端區域網路上使用區域IP位址的電腦，透過NAT閘道進入外部網路，利用ISAKMP協定交換密鑰及

五、發明說明 (10)

制定SAs並依據IPSec提供安全協議。基於非ISAKMP運輸，閘道裝置以標準執行位址轉換，然而，每當於區域網路上的器機裝置產生一個ISAKMP通訊協定的訊息時，閘道裝置會鑑定資料封所包含埠位址500的埠位址位址，當遇到此類的資料封時，前述閘道裝置會轉換來源IP位址，但不轉換來源埠位址位址並將來源埠位址位址留給埠位址500，且依埠位址500指定之來源及目的地埠位址位址傳送封包至網際網路，同樣的閘道裝置會更新本身"繫結"埠位址500之內部表為區域IP位址及有關目的地機置的外部IP位址的繫結預定時間區間，如果於預定的時間區間內有效的回應不被接收，則於埠位址500與區域IP位址間的"繫結"會被釋放，此特徵是必須確認埠位址500不是無限期暫用的，如同，例如，一個ISAKMP通訊協定已經開始傳輸到一個不正確的目的地IP位址的情形，在此情況下，閘道裝置將永遠無法接收到有效的回應；如果經過一段時間之後閘道裝置沒有接收到有效的回應，而沒有計時裝置去釋放埠位址500，則埠位址會持續繫結到區域IP位址直到閘道裝置被重新設定，基於多數情況，在一個兩秒鐘的期間內應該有足夠的時間長度去維持埠位址500與區域IP位址間的繫結同時等待有效回應。

在埠位址500與區域IP位址繫結的時間內，前述閘道裝置將在等待有效回報時持續正常的處理沒有埠位址500位址之資料封，一個有效的回應將會是一個擁有與埠位址500關連的外部IP位址相同的來源IP位址的資料封，且會

五、發明說明 (11)

同時擁有兩個與埠位址500位址相同的來源及目的地位址，在等待有效回應的同時，閘道裝置會忽略其它從外部網路而來擁有埠位址500來源及目的地位址的UDP資料封，而非本身的來源IP位址。同樣的，當埠位址500繫結到一個區域IP位址時，從擁有來源及目的地埠位址500的埠位址位址而來的資料封將於埠位址500來源埠位址位址中接受"合法"位址轉換，在傳送到外部網路前轉換為一個任意的未使用的埠位址位址。因為這樣的資料封不同時擁有埠位址500的來源及目的地埠位址位址而不是有效的ISAKMP資料封，在到達本身IP目的地時將不被理會，如果埠位址500繫結到一個區域IP位址的期間不需藉著由閘道裝置所接收的合法資料封終止，則此繫結將會被釋放，同時埠位址500對於下個擁有埠位址500來源及目的地埠位址位址的資料封將會成為可使用的。

當埠位址500是被繫結的，在接收一個有效回應的擁有埠位址500來源及目的地埠位址位址及正確來源IP位址資料封之後，閘道裝置會藉由替代區域機置的IP位址成為資料封標頭的目的地IP位址領域的IP位址處理資料封，接著傳遞資料封經過區域網路到達區域機置，當資料封離開閘道裝置時，閘道裝置將會釋放區域IP位址及埠位址500間的繫結，並且恢復正常的的資料封處理。

假設一個擁有本身的來源IP位址及埠位址500的埠位址位址的回應不是從外部網部接收而來，經過一短暫預定的時間後閘道裝置將會停止，如果閘道裝置的停止時間在

五、發明說明 (12)

接收到有效回應之前，而ISAKMP訊息交換不能完成，則必須重新設定。

一旦ISAKMP通訊協定完成，且一個加密安全的期間是進行中，前述閘道裝置將執行參考ESP進出資料封標頭中的SPI完成區域位址轉換，此閘道裝置將同時會確認每一個封包型態(ESP封包的型態50)對被透過閘道傳遞的資料是正確的。有時，一個通過VPN的安全的期間會被中斷或新的期間開始，閘道裝置的第一指示將是於IP位址中被識別的型態50資料封的接收，但SPI與目的地的關連不在其本身內部表中出現。當此情形發生時，閘道裝置會使用新的SPI發送資料封到達目的地IP位址，同時設定目的地新的SPI值(SPI-in或SPI-out，視傳送方向而定)到其內部表中，並將來源SPI值設定為零，接受一個傳送回應後，閘道裝置將會以新的SPI目的地IP位址取代SPI領域表中的零值。

由於本發明之閘道裝置沒有訊息加解密，只簡單的傳遞承載(可能加密或不加密)通過傳輸區域網路或網際網路到達接收機置，而不要求強烈的處理功能性，因此能夠使用在考慮設定、維護的費用、簡易的私人區域網路上。

[標號說明]

10 --- 區域網路

15 --- 電腦

20 --- 網路位址轉換閘道

30 --- 電腦網站

五、發明說明 (13)

35 --- 防水牆或閘道

40 --- 伺服器

50 --- 網際網路

100 --- 資料封程序系統

110 --- 計時器

120 --- 啟始計時器之訊號

130 --- 停止計時器之訊號

140 --- 計時器終止時釋放埠之訊號

[圖式之詳細說明]

請參考圖一所示，其為虛擬私人網路(VPN)圖，顯示私人區域網路10與於網際網路50上之電腦網站30連結，區域網路10使用區域IP位址，並透過本發明之網路位址轉換閘道20與網際網路連結，電腦網站30可能是企業、公司或任何一個由跨國公司、教育機關、或任何其它經常由遠端位置進出的網站所使用的私人區域網路，此類的網站通常具有防火牆或閘道35做為加密或其它安全應用，此類閘道有能力可以開啟封包、解密或存取其內容及顯示位址轉換、路徑、解壓縮及資料運用功能。同時此類裝置利用封包開啟、解密及資料運用能夠支援ISAKMP及其它IPSec通訊協定，總的來說，以主機建立VPN於遠端區域網路網站需求有效地利用，太昂貴也太強大了。

位於主機內的伺服器40執行VPN伺服軟體，遠端網站的每一部電腦15執行適當的VPN用戶軟體實施IPSec安全協定於每一部電腦上。

五、發明說明 (14)

位於區域網路10上的電腦15透過閘道裝置利用傳送一個IP資料封到電腦網站30上之伺服器40與網際網路裝置通訊。

資料封依照圖二及圖三之決策流程圖程序由閘道20接收，僅管流程圖圖二及圖三顯示程序步驟及步驟順序，但功能執行的次序不是必須的，有些步驟可能被以除了流程圖中次序外之次序實施，仍不影響其最終結果。例如，圖二及圖三顯示資料封從閘道裝置接收後的第一步驟是判別資料封型態，而最後步驟是必需於透過閘道裝置傳輸資料封前顯示IP位址轉換，而然，某些具體實施能夠更換位址轉換步驟為較早的程序並不影響程序實施結果。由於轉換IP位址的順序對所有程序來說不是必要的，因此，判定何時該實行轉換是一工程選擇問題。

如圖二所示，從區域網路接收資料封後，閘道裝置藉由檢查IP標頭中的"下一個標頭"欄位判定往來的資料封型態，檢查資料封是否為加密的及資料封是否曾經被加密。50(ESP)的資料封型態表示資料封是加密的，且埠位址位址資訊不一定是有效的。

繼續參考圖二之決策樹，假設資料封是加密的，則閘道裝置將檢查資料封的SPI是否出現在閘道內部表之SPI-out欄中，此代表欄位於圖五a至圖五c中顯示。假設資料封的SPI在內部表的SPI-out欄中找到，閘道裝置將修改資料封的來源IP位址成為閘道外部IP位址，並傳送此資料封到外部網路上之外部裝置。

五、發明說明 (15)

假設資料封是加密的，而SPI卻沒有顯示於閘道內部表中，則依據圖二之決策流程圖，閘道裝置會假定資料封初始設定為新的期間，在這種情況下，閘道裝置將會設定內部表的SPI-in為零，並從資料封設定SPI-out為新的SPI，內部表的改變可見於圖五a及圖五b中，一個沒有於圖五a閘道內部表的SPI-out顯示的一個新的 SPI 值"14662"於圖五b中已經登入SPI-out欄中，且SPI-in也已被設定為"0"，此已加密的資料封繼來源IP位址從區域裝置IP位址轉換閘道裝置外部IP位址後，區域裝置接著會被傳送到外部閘道裝置。以上步驟說明於圖五b及圖五c。

接著參考決策圖二，假設資料封是未加密的，則閘道裝置接著會檢查資料封的目的地埠位址位址，假設埠位址位址是除了埠位址500以外的任一位址，則閘道裝置將會登入來源埠位址位址至其內部表中，交叉參考閘道與區域來源IP位址後，接著會替代一個任意的、未使用的埠位址位址到IP標頭得的來源埠位址位址欄，相同的，閘道裝置會登入一個新的埠位址位址至其內部表中，並再次參考區域來源IP位址。此程序是用於沒有埠位址500位址的未加密資料封，稱為區域網路資料封發明「合法位址轉換」。此轉換說明於圖六第2、3列，此資料封接著會被發送到網際網路目的地IP位址安排的路徑。

圖二中，在一個傳送進來的資料封來源及目的地埠位址位址為埠位址500時，閘道裝置必須下一次檢查其內部表是否埠位址500已經繫結到一個IP位址上，假設埠位址

五、發明說明 (16)

500是空的，則閘道裝置會"繫結"埠位址500到資料封的區域來源IP位址，建立埠位址與外部目的地埠位址位址間的連結，並傳送訊號去開始內部計時器，同時閘道裝置於來源IP位欄中以取代閘道外部IP位址為區域IP址處理但不轉換來源埠位址位址。透過暫緩來源埠位址位址的"合法"轉換，閘道裝置能夠確認目標裝置資料封為ISAKMP資料封。以上步驟見圖六第5列及第6列。

圖二中，假設一個擁有埠位址500的來源及目的地埠位址資料封從區域網路傳送進來，但埠位址500已經繫結到其它區域IP位址，則閘道裝置無法繫結此資訊埠位址500及處理，在此情況下，閘道裝置將合法化的處理資料封，假設為非ISAKMP資料封，也就是說，閘道裝置會轉換資料封的來源埠位址位址成為一任意數並轉換來源IP位址為閘道的外部IP位址，接著閘道裝置會傳送此資料封至網際網路中，將被目標拒絕因其無法確認ISAKMP資料封。以上情形說明於圖七第15、16列。

圖三，描述閘道裝置處理從網際網路接收資料封的步驟流程圖。在接收一個資料封時，閘道裝置首先會檢查其型態，同時，若此資料封是加密的，會再SPI是否出現在內部表中，如果SPI可辨識，則目的地IP位址會被轉換成為區域裝置的IP位址，且資料封會被網際網路傳送至區域裝置上；假若SPI不可辨識，則閘道裝置會檢查其SPI-in欄是否符合資料封的來源IP位址"0"，假設SPI-in為"0"，則閘道裝置會假定資料封是新期間的第一次回應並以資料

五、發明說明 (17)

封的SPI置換"0"於SPI-in欄中。接著閘道裝置會轉換目的地IP位址為區域裝置的區域IP位址，並傳送資料封至區域網路中。以上情形描述於圖五b及圖五c。於圖五b，區域機器裝置L-1的SPI設定為"0"，依據從網際網路接收的資料封閘道接收擁有一個3288的SPI，閘道裝置將無法找到SPI於SPI-in欄中，接著閘道裝置會在下一次檢查SPI-in欄中是否擁有0值，在判定區域機器裝置的SPI-in為0後，閘道裝置會以資料封"3288"的SPI置換0，並傳送資料封至區域網路中。以上說明於圖五c。

圖三中，假設從網際網路傳來的資料封是未加密的，閘道裝置會檢查其是否擁有埠位址位址500，假若沒有，則資料封會接受外部網路資料封的"合法"位址轉換，意即區域網路裝置的區域埠位址位址及區域IP位址將被替代成為資料封的目的地欄，且資料封會被傳送到區域網路上。此網際網路資料封的"合法"位址轉換顯示於圖六第3、4列。

再次參考圖三，假設資料封不具有埠位址位址500，則閘道裝置必須檢查埠位址500是否繫結到區域IP位址及是否與資料封的外部來源IP位址連結，假若是，則資料封是合法的，並於目的地IP位址被從外部閘道轉換為區域裝置IP位址後傳送到區域網路上，傳送資料封到區域網路後，閘道裝置會釋放埠位址500。此情形圖式說明於圖六第7、8列。

假設，圖三中埠位址500是繫結到一個區域IP位址，

五、發明說明 (18)

並且除了與一個在資料封來源IP位址中找到的外部IP位址聯結外，資料封是不合法的且將無法被閘道進一步的處理。此情形見於圖七第25至31列。於第25、26列上，區域裝置L-1傳送一個ISAKMP資料封到預定目標T-1，此時，埠位址500是繫結到一個區域裝置L-1的IP位址，並且與預定目標T-1的IP位址連結；然而，如同圖七第27列所示，計時器時間停止於閘道從T-1接收的回應之前，且埠位址500是被釋放的；第28、29列，區域裝置L-3傳送一個ISAKMP資料封到預定目標T-3，繫結埠位址500到L-3的IP位址並與T-3的IP位址建立連結，當埠位址500是繫結時，從T-1接收回應，然而，因為埠位址500是繫結的且與T-3的IP位址連結，於是從T-1來的回應會被丟棄。見圖七第30、31列。

圖五a至圖五c係描述網際網路區域電腦與預定目標目加密通訊的IP位址及SPI數閘道內部表維護。"L-1"、"L-2"、"L-x"及"T-1"到"T-3"欄被包含以便參考但不出現於閘道內部表中，圖五中，"SPI-out"欄具有每一個預定目標裝置與位於區域網路上一特定電腦間安全期間的SPI，而SPI-in欄提供將被區域電腦視為合法的資料封預定識別的相對的SPI。圖五a為起始時間表，為八部電腦與三個預定目標T-1～T-3於加密期間表資料生命週期。由事實顯示每一區域裝置表示一個SPI-in與其IP位址連結，即便於此表中只有三個預定目標，仍可記錄每一個預定目標使用不同的SPI-out做為與每一個裝置間的通訊。此方法

五、發明說明（19）

中，預定目標可得加密資料封的產生來源。

圖五b與圖五A採用相同的區域及預定目標電腦，但圖五b於L-1及T-1之間的期間SPI-out為一新的SPI，描述電腦間的一個新的期間。閘道裝置第一個描述為一正在產生的新期間，為其接收的區域網路加密資料封"14662"不在此表內；閘道裝置傳送資料封至網際網路中，同樣的不更改此資料封內部表，置換新的SPI到SPI-out欄中與資料封的來源及目的地IP位址連結；並填入0至SPI-in欄作為一標示，表示預定的新SPI-in。圖五c顯示一個新的SPI－"3288"，包含於從T-1接收來的資料封中，此SPI曾被登入至閘道裝置的SPI-in欄中，而於此期間，L-1及T-1間的進一步通訊將使用此SPI確認其訊息。

圖六描述曲型的資料封透過本發明之閘道系統利用一個區域網路上的單獨電腦與遠端網際網路上之預定目標通訊之流程。圖的每一列代表任一個區域網路與閘道裝置或網際網路與閘道裝置的資料封資訊，連續的列代表資料從它端登入閘道裝置及離開閘道至它端，閘道裝置具有一個IP位址，此IP位址可能為一區IP位址與區域網路接口，或一個全域IP位址與網際網路接口；圖六的每一行描述使用ESP協定閘道端資料往返、資料型態、資料封來源IP位址及埠位址位址、資料封目的地IP位址及埠位址位址以及加密資料封型態50的資料封安全參數索引（SPI）。

圖六第一列表示一個UDP資料封到達閘道區域介面，及擁有一個與區域電腦L-1相同的來源IP位址，及網際網

五、發明說明 (20)

路預定目標的目的地IP位址，T-1。基於閱讀方便，圖四提供一個交叉參考區域目的地L-1至L-3及預定目標之目的地T-1至T-3的IP位址表。L-1的來源埠位址位址是埠位址6404，而預定目標之目的地埠位址是埠位址80，由於資料封是未加密的，且沒有顯示埠位址500，其接受"任一個"埠位址合法轉換，埠位址10425被替代到來源埠位址位址欄，而閘道之外部IP位址被資料封的來源IP位址替代，既使前述來源埠位址位址轉換是"任一個"，但通常是由未被預定及由閘道維持目前沒有使用的埠位址位址序列中取出下一個。

如圖六第二列所示，當資料封離開閘道裝置時，閘道位址轉換功能已經取代閘道之外部IP位址成為來源IP位址的資料封標頭，且已經授予來源埠位址一個任一的數，第3、4列係顯示從預定目標回應資料封，於第3列中，一個從預定目標而來的UDP資料封顯示目的地IP位址作為閘道裝置外部IP位址，而目的地位址被閘道裝置指定為任一個埠位址位址，由於資料封是未加密的且不具有埠位址500，資料封經過目的地埠位址位址及IP位址的正常轉換而傳送到區域網路上；在第4列中，閘道裝置已經替代了區域電腦的區域IP位址及標頭傳送資料封到區域網路之前的目的地欄中埠位址位址。

於圖六第5列中，區域電腦以欲達到的目標開始實施ISAKMP通訊協定，資料封型態以ISAKMP顯示，而來源及目的地埠位址位址皆為埠位址500，當閘道裝置確定目的地

五、發明說明 (21)

埠位址位址為埠位址500時，閘道裝置會檢查埠位址500目前是否繫結到任何IP位址，因其未繫結到任何IP位址，閘道裝置傳送資料封時，僅轉換來源IP位址欄顯示閘道裝置的外部IP位址，但不改變來源埠位址位址。

於圖六第5～16列中顯示六個標準ISAKMP"交握協定"(Handshaking)資料封交換必需制定SAs充份的支持加密及鑑定的資料封，然而有些ISAKMP型式使用較少的交換，此主要的型式描述於圖六中，繼SAs制定後，區域電腦及預定目標開始使用ESP通訊協定加密資料封通訊，此時，資料封效力透過於資料封標頭的SPI欄內SPI號碼的使用來維持，每一個主機識別一個資料封"定址(addressed)"到其SPI，其能於安全期間內隨著必需確認未完成的安全性被主機的相互協議修改，當一個加密的資料封透過閘道裝置傳送，如圖六第17及18列，即使資料封的來源IP位址被轉換為閘道裝置的外部IP位址，來源或目的地SPI也不會被閘道裝置修改。

因此，當一個加密的資料封被閘道裝置接收時，將會被以資料封的型態50(ESP)表示，繼接觸到此資料封型態後，閘道裝置將檢查資料封的SPI是否被記錄在其內部表中，假若此SPI存在於內部表中，則閘道裝置將適當的轉換資料封的來源或目的地IP位址，並且依據其傳送指示傳送此資料封到區域網路或網際網路上；然而，假若從區域網路來的資料封的SPI沒有存在於閘道內部表中，而來源及目的地能夠辨識IP位址，則閘道裝置會認為一個新的期

五、發明說明 (22)

間已經開始，於此例中，閘道裝置將會傳送資料封到外部網路留下一個未更動的新SPI，僅記錄新的SPI到內部表的SPI-out欄中且置換" 0"到SPI-in欄中。於第25、26列上，可看到一個代表一個新期間的新SPI出現，此情況與圖五b相同，於SPI-in欄中的" 0"與新的SPI-out "14662"一致，而於27、28列上，從外部網路而來的回應封包顯示一個舊的SPI "9802"已經被新的SPI "3288"置換。

圖七與圖六類似，除了說明在區域網路上經由本發資料封閘道在三台電腦之間的通道，被指定的L-1、L-2、L3以及網際網路上三個預定目標具有全域IP位址T-1、T-2及T-3。圖四中，為便於參考，給予一個包含這些裝置的IP位址表格，如圖七所示，一個傳輸指定"L-1 out"表示一個從區域電腦L-1到閘道裝置的傳輸；"T-1 in"表示一個從閘道裝置到預定目標"T-1"的傳輸；"T1-out"表示一個從預定目標T-1到閘道裝置的傳輸；同時"L-1 in"表示一個從閘道裝置到電腦L-1的傳輸。

如圖七第1～8列所示，電腦L-1及L-2引導與預定目標T-1及T-2的 "in the clear"通訊，於第9列上，L-1與T-1開始一個ISAKMP期間，第9～14列表示在ISAKMP通訊協定期間L-1及T-1間前三個訊息的交換，於15列上，電腦L-3與T-3開始一個ISAKMP-1訊息交換，然而，此時埠位址500是繫結到L-1且與T-1的IP位址連結，並等待一個從T-1回應的ISAKMP-4，在此情況下，從L-3而來的資料封無法繫結埠位址500且其來源埠位址將會被轉換，如此，L-3無法

五、發明說明 (23)

完成第15列開始的傳輸。

之後，於17～18列上，T-1的回應於閘道裝置收到並傳送到L-1，且埠位址500立即成為閒置的。因此，當L-3於19列中重新嘗試其ISAKMP-1傳輸時，此傳輸將會成功。

於圖七第19～20列上，L-3的ISAKMP-1傳輸繫結埠位址500到L-3之IP位址，因此，當L-1於21-22列上嘗試其ISAKMP-5傳輸時，埠位址500不是閒置的，且閘道裝置僅從埠位址500轉換目的地埠位址位址到一個"任意的"埠位址號碼(於本情況中為"9063")，並傳送資料封到網際網路，在此，預定目標T-1將不視為一個ISAKMP資料封；然而，繼L-1釋放埠位址500之後，於第23、24列，L-1的下一次接著試圖傳送其ISAKMP-5傳輸成功的被T-1接收，但由於T-1的回應緩慢，且於27列中埠位址500被從其繫結到的L-1釋放，於是於28、29列上會立即被L-3攫取做為ISAKMP-3傳輸；因此，當T－1的ISAKMP-6回應抵達閘道裝置時，如30、31列所示，埠位址500會被阻止且此資料封會被忽視，之後，沒有接收回應到其ISAKMP-5訊息的L-1，於35、35列會重新傳送且於36、37列從T-1接收回應。下述其ISAKMP交握協定，L-1及T-1可在38-39列及42-43列使用ESP通訊協定能夠安全的通訊。

圖七38-57列說明閘道裝置於無數區域電腦及預定目標間各種資料封包的處理，顯示於40-41列的UDP資料封、42-43列及52-53列之ESP資料封以及44-45列之ISAKMP資料封；同時，圖七顯示每一個裝置的不同IP位址，實際上，

五、發明說明 (24)

也可能發生一些程序執行在同一個裝置上，以閘道裝置取代唯一的來源埠位址以及SPI的使用以區分加密傳輸，確認從多重程序執行於一單機而來的資料封不會被指錯裝置位址。

圖八描述於資料封程序系統100及計時器110間的訊號轉換與初始值。依據程序的發生要求一個埠位址位址繫結到一個IP位址，訊號120將被傳送到計時器開始計時，繼相對的期間終止，計時器將會傳送一訊號140表示時間已經終止，在程序中已經被繫結的任何埠位址將會被釋放。在期間內，假設一個預期的資料封已經到達，且先前繫結的埠位址已經被釋放，一個還原訊號130將被傳送到計時器指示計時器重新設定等待下一個訊號啟始計時器。顯然地，可知在此技術中有許多計時線路，而於圖八中的實施例結構只是多種可能的實施例中的一個。

在詳細說明本發明的較佳實施例之後，熟悉該項技術人士可清楚的瞭解，並在不脫離下述申請專利範圍與精神下可進行各種變化與改變，而且本發明亦不受限於說明書之實施例的實施方式。例如，雖然較佳實施例藉由參考埠位址500描述，此埠位址已經為使用ISAKMP通訊協定專門地保留了，但本發明可使用相同方法處理其它埠位址位址預定的資料封，其它埠位址能夠於將來被指定給其它程序或通訊協定，尤其許多網路遊戲需要使用特殊埠位址於無法承受合法埠位址轉換的區域及外部機置；再者，儘管本發明已經描述於私人區域網路及網際網路間的通訊方面，

五、發明說明（25）

但其明顯的描述本發明之閘道裝置能夠被使用在任何於兩個網路間的介面且將具有如先前描述之相同的功能性。

圖式簡單說明

圖一係描述遠端區域網路使用區域IP位址經由外部網路(可能為網際網路)與主要運算網站連結的虛擬私人網路。前述區域網路係與外部網路透過NAT閘道連結。

圖二係描述本發明之閘道裝置使用決策之流程圖，用以處理從傳輸區域網路至網際網路所接收的UDP資料封。

圖三係描述本發明之閘道裝置使用步驟決策流程圖，用以處理從網際網路傳遞至區域網路裝置上所接收的UDP資料封。

圖四係提供用來參考圖五、六及七。圖四為一表，包含區域網路(L-1至L3)上區域機置的IP位址、閘道裝置的內部及外部IP及位址於外部網路上外部裝置("targets" T1至T3)的IP位址。

圖五a至圖五c為從閘道內部表交叉參考區域網路(L-1, L-2, …, L-x)上之區域IP位址機置及外部裝置(T-1~T-3)的外部IP位址及使用SPI s鑑定資料封加密的表示檔。SPI-out表示一個加密資料封的SPI離開閘道裝置至網際網路上的裝置，同時SPI-in表示加密資料封的SPI預定的區域網路上之區域機置，a、b、c每個表記錄標頭來源值、目的地值及於不同時間點的SPI值。以一個區域機置加上一個目標機置數值的改變表示一個新時段的開始。

圖六係顯示資料封標頭於單一區域機置與外部網路單機的交換表示檔。標頭值透過本發明之閘道裝置處理做修改。

圖七係顯示透過本發明之閘道裝置處理資料封標頭於

圖式簡單說明

區域網路上的三個區域機置(L-1~L-3)以及外部網路上之三個目標裝置(T-1~T-3)間的交換。

圖六係顯示資料封標頭於單一區域機置與外部網路單機的交換表示檔。標頭值透過本發明之閘道裝置處理做修改。

圖七係顯示透過本發明之閘道裝置處理資料封標頭於區域網路上的三個區域機置(L-1~L-3)以及外部網路上之三個目標裝置(T-1~T-3)間的交換。

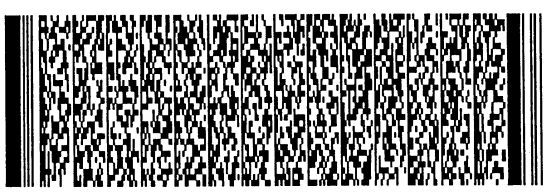
圖八為資料封處理功能及計時器間的信號傳訊圖。

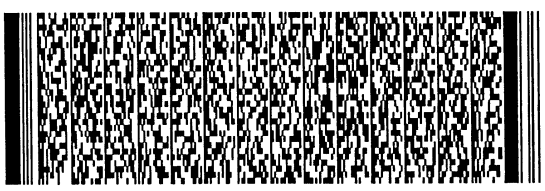
四、中文發明摘要 （發明之名稱：使用區域網際網路通訊協定位址及不可移轉之位址埠於區域網路的網路位址轉換途徑）

一種網路位址轉換閘道裝置，提供IP資料封從區域網路使用區域IP位址移動到一外部網路的一般網路轉換，而當位址被預定為一特定協定時暫緩來源服務位址(埠)轉換，例如ISAKMP交握協定為IPSec通訊協定模型的一部份，ISAKMP交換需要來源及預定目標電腦兩者使用相同的服務位址(埠)，藉由提供一不轉換來源服務位址的網路介面，使得閘道裝置達到安全的開始及維護，加密傳輸使用IPSec通訊協定於區域網路使用區域IP位址及網際網路上伺服器之間。

英文發明摘要 （發明之名稱：NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA ENTWORKS USING LOCAL IP ADDRESSES AND NON-TRANDLATABLE PORT ADDRESSES）

A network address translation gateway provides normal network translation for IP datagrams traveling from a local area network using local IP addresses to an external network, but suspends source service address (port) translation when the port is reserved for a specific protocol, such as the ISAKMP "handshaking" protocol that is part of the IPSec protocol model. ISAKMP exchanges require both source and target computers to use the same service address (port). By providing a network





四、中文發明摘要　（發明之名稱：使用區域網際網路通訊協定位址及不可移轉之位址埠於區域網路的網路位址轉換途徑）

英文發明摘要　（發明之名稱：NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA ENTWORKS USING LOCAL IP ADDRESSES AND NON-TRANDLATABLE PORT ADDRESSES）

interface that does not translate the source service address (port), this gateway enables the initiation and maintenance of secure, encrypted transmissions using IPSec protocol between a local ares network using local IP addresses and servers on the internet.

六、申請專利範圍

1. 一種連結區域網路至外部網路的網路位址轉換閘道，前述區域網路使用區域IP位址，前述閘道係具有一能夠被前述區域網路的裝置看到之區域IP位址及能夠被前述外部網路的裝置看到之外部IP位址，此閘道包含：

複數個內部表，係關於前述區域網路的區域裝置之區域IP位址、前述外部網路的外部裝置之外部IP位址、SPI-In值、SPI-Out值、來源埠位址、目的地埠位址、預定埠位址及維護預定埠位址之目錄的結合；

用於執行從前述區域網路傳遞資料封到前述外部網路及從前述外部網路傳遞資料封到前述區域網路之合法位址轉換的裝置；

用於從前述區域網路的區域裝置遞送一資料封到前述外部網路的外部裝置的裝置，係藉由從欲遞送到前述外部網路的外部裝置之前述區域網路的區域裝置接收資料封，並決定前述資料封是否加密，假設前述資料封是加密的，則決定前述資料封的SPI是否記錄於前述內部表中之I-Out欄中，假若前述SPI是記錄在前述SPI-Out欄中，則更改前述資料封的來源IP位址為前述閘道之外部IP位址，且傳遞前述資料封到預定安排的前述外部網路並遞送到前述外部裝置；

假設前述SPI沒有記錄於前述內部表中之前述SPI-Out欄中，則設定對應前述區域裝置的區域IP位址的SPI-In欄為0，並設定前述SPI-Out欄為前述SPI，更改前述資料封之來源IP位址為前述閘道之前述外部IP位

六、申請專利範圍

址，且傳遞前述資料封到預定安排的前述外部網路並遞送到前述外部裝置；

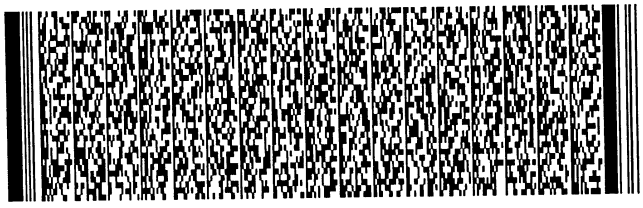
假設前述資料封不是加密的，則決定前述資料封之目的地埠位址是否被包含於前述預定埠位址目錄中，假若目的地埠位址不是被包含於前述預定埠位址位址目錄中，則執行前述資料封的合法位址轉換並傳遞前述資料封到前預定安排的外部網路，且遞送到前述外部裝置；

假設前述目的地埠位址是包含於前述預定埠位址目錄中，則決定前述目的地埠位址是否繫結到前述區域裝置之前述區域IP位址，且假若前述目的地埠位址是繫結到前述區域IP位址，則執行前述資料封的合法位址轉換，並傳遞前述資料封到預定安排的前述外部網路，且遞送到前述之外部裝置；

假設前述資料封不是繫結到前述區域裝置之前述區域IP位址，則更改前述資料封之前述區域IP位址為前述閘道之前述外部IP位址、繫結前述目的地埠位址到前述區域裝置之區域IP位址以及在前述目的地埠位址與前述外部裝置之外部IP位址間建立關聯，並傳遞前述資料封到預定安排的前述外部網路且遞送到前述外部裝置；

用於從前述外部裝置遞送一資料封到前述區域裝置的裝置，係藉由從欲遞送到前述區域網路的區域裝置之前述外部網路的外部裝置接收資料封，

決定前述資料封是否加密，且假若前述資料封是加密的，則決定該資料封的SPI是否記錄於前述內部表之



六、申請專利範圍

SPI-In欄中，而假若前述SPI是記錄於前述SPI-In欄中，則更改前述資料封之目的地IP位址為前述區域裝置之前述區域IP位址，並傳遞前述資料封到預定安排的前述外部網路且遞送到前述外部裝置；

假設前述SPI沒有記錄於前述內部表之前述SPI-In欄中，則決定對應到前述外部裝置之前述IP位址之前述SPI-In欄是否為0，假若前述SPI-In欄不為0，則丟棄前述資料封；

假設前述SPI-In欄為0，則設定前述SPI-In欄為前述SPI，更改前述資料封之目的地IP位址為前述區域裝置之區域IP位址，並傳遞前述資料封到用以傳送到前述區域裝置的前述區域網路；

假設前述資料封不是加密的，則決定前述資料封之目的地埠位址是否被包含於前述預定埠位址目錄，而假若前述目的地埠位址沒有被包含於前述預定埠位址目錄，則執行前述資料封合法位址轉換並傳遞前述資料封到用以傳送到前述區域裝置的前述區域網路；

假設前述目的地埠位址是被包含於前述預定埠位址目錄，則決定前述目的地埠位址是否繫結到前述區域裝置之區域IP位址，而假若前述目的地埠位址沒有繫結到前述區域IP位址，則丟棄前述資料封；

假設前述目的地埠位址是繫結到前述區域IP位址，則更改前述資料封之前述目的地IP位址為前述區域裝置之區域IP位址，不從前述區域IP位域繫結到前述目的地

六、申請專利範圍

埠位址，並傳送前述資料封到用以傳送到前述區域裝置的前述區域網路。

2. 如申請專利範圍第1項所述之網路位址轉換閘道，進一步包含一計時器，其中，在接收一埠位址已經繫結到一IP位址之訊號後，前述計時器將會開始計時一預定時間長度，並在前述預定時間長度終止，將會送出一訊號引發前述埠位址成為未從前述IP位址繫結，並且在接收一訊號指示前述埠位址於前述預定時間長度終止以前已成為未從前述IP位址繫結，前述計時器將會停止計時並重新設定。

3. 如申請專利範圍第1項所述之網路位址轉換閘道，前述外部網路即為網際網路；

4. 如申請專利範圍第3項所述之網路位址轉換閘道裝置，前述區域網路即為虛擬私人網路；

5. 一種處理IP資料封方法，該IP資料封從區域網路的區域裝置到外部網路的外部裝置，該區域裝置透過網路轉換閘道使用區域IP位址，其步驟包含：

維護複數個表格，係關於前述區域網路上區域裝置的區域IP位址、前述外部網路上外部裝置的外部IP位址、前述區域裝置之埠位址、前述外部裝置之埠位址、SPI-in值、SPI-out值、預定埠位址及一預定埠位址目錄；

從前述區域網路接收一資料封；

決定前述資料封是否加密，假若前述資料封是加密

六、申請專利範圍

的，則決定於前述資料封中之SPI是否記錄於前述複數個內部表之一的SPI-out欄中，假若前述SPI是記錄於前述內部表之SPI-out欄中，則更改來源IP位址為前述閘道之外部IP位址，並且傳遞前述資料封到預定安排之前述外部網路且遞送到前述外部裝置；

假設前述SPI沒有記錄於前述內部表之前述SPI-out欄中，則設定對應前述外部裝置之IP位址的前述SPI-out欄為前述SPI，並設定前述內部表之SPI-in欄為0，更改前述來源IP位址為前述閘道之前述外部IP位址，且傳遞前述資料封到預定安排之前述外部網路並遞送到前述外部裝置；

假設前述資料封不是加密的，則決定前述資料封之目的地埠位址是否被包含於前述預定埠位址表中，假若前述目的地埠位址沒有被包含於前述預定埠位址表中，則執行前述資料封合法位址轉換，並傳遞前述資料封到預定安排之前述外部網路且遞送到前述外部裝置；

假設前述目的地埠位址是被包含於前述預定埠位址表中，則決定前述目的地埠位址是否繫結到一IP位址，假若前述目的地埠位址是繫結到一IP位址，則執行前述資料封合法位址轉換，並傳遞前述資料封到預定安排之前述外部網路且遞送到前述外部裝置；

假設前述目的地埠位址不是繫結到一IP位址，則更改前述來源IP位址為前述外部裝置之前述IP位址、繫結前述目的地埠位址到前述區域裝置之區域IP位址以及於

六、申請專利範圍

前述目的地埠位址及前述外部裝置之前述外部IP位址間建立關聯，並傳遞前述資料封到預定安排之前述外部網路且遞送到前述外部裝置。

6. 一種處理IP資料封方法，該IP資料封從外部網路的外部裝置透過一網路轉換閘道到使用區域IP位址之區域網路上的區域裝置，其步驟包含：

維護複數個表格，係關於前述區域網路上區域裝置的區域IP位址、前述外部網路上外部裝置之外部IP位址、前述區域裝置之埠位址、前述外部裝置之埠位址、SPI-in值、SPI-out值、預定埠位址以及一預定埠位址目錄；

接收從前述外部網路而來的資料封；

決定前述資料封是否加密，假若資料封是加密的，則決定前述資料封內的SPI是否記錄於前述複數個內部表格之一的SPI-in欄中，而假若前述SPI是記錄於前述內部表格之前述SPI-in欄中，則更改目的地IP位址為前述區域裝置之內部IP位址，並傳遞前述資料封到預定安排之前述區域網路且遞送到前述區域裝置；

假設前述SPI沒有記錄於前述內部表之前述SPI-in欄中，則決定對應前述外部裝置之IP位址的前述SPI-in欄是否為0，而假若前述SPI-in欄不為0，則丟棄前述資料封；

假設前述SPI-in欄為0，則更改前述SPI-in欄為前述SPI、更改前述目的地IP位址為前述區域裝置之前述

六、申請專利範圍

區域IP位址，並傳遞前述資料封到預定安排之前述區域網路且遞送到前述區域裝置；

假設前述資料封不是加密的，則決定前述資料封的目的地埠位址是否被包含於前述預定埠位址目錄中，假若前述目的地埠位址不被包含於前述預定埠位址目錄中，則執行合法位址轉換並傳遞前述資料封到預定安排之前述區域網路，且遞送到前述區域裝置；

假設前述目的地埠位址是被包含於前述預定埠位址目錄中，則決定前述目的地埠位址是否繫結到前述區域IP位址，假若前述目的位址不是繫結到前述區域IP位址，則丟棄前述資料封；

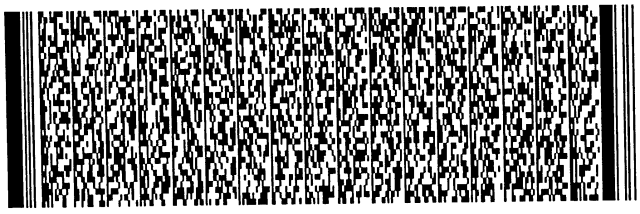
假設前述目的地埠位址是繫結到前述區域IP位址，則更改前述目的地IP位址為前述區域裝置之前述區域IP位址，不從前述區域IP位址繫結前述目的地埠位址，並傳遞前述資料封到預定安排之前述區域網路且遞送到前述區域裝置；

7. 如申請專利範圍第5項所述之處理IP資料封方法，進一步包含當前述目的地埠位址繫結到前述區域裝置之前述區域IP位址時啟始一計時器之步驟；

當前述目的地埠位址已被釋放時重新設定前述計時器；

當前述計時器運作時及前述計時器已經啟始而預定時間長度終止時，傳送一訊號。

8. 如申請專利範圍第6項所述之處理IP資料封方法，進一



六、申請專利範圍

步包含當前述目的地埠位址繫結到前述區域裝置之前述區域IP位址時啟始計時器的步驟；

當前述目的地埠位址已被釋收時重新設定前述計時器；

當前述計時器運作時及前述計時器已經啟始而預定時間長度終止時，傳送一訊號。

9. 如申請專利範圍第5項所述之處理IP資料封方法，其中前述之外部網路即為網際網路。

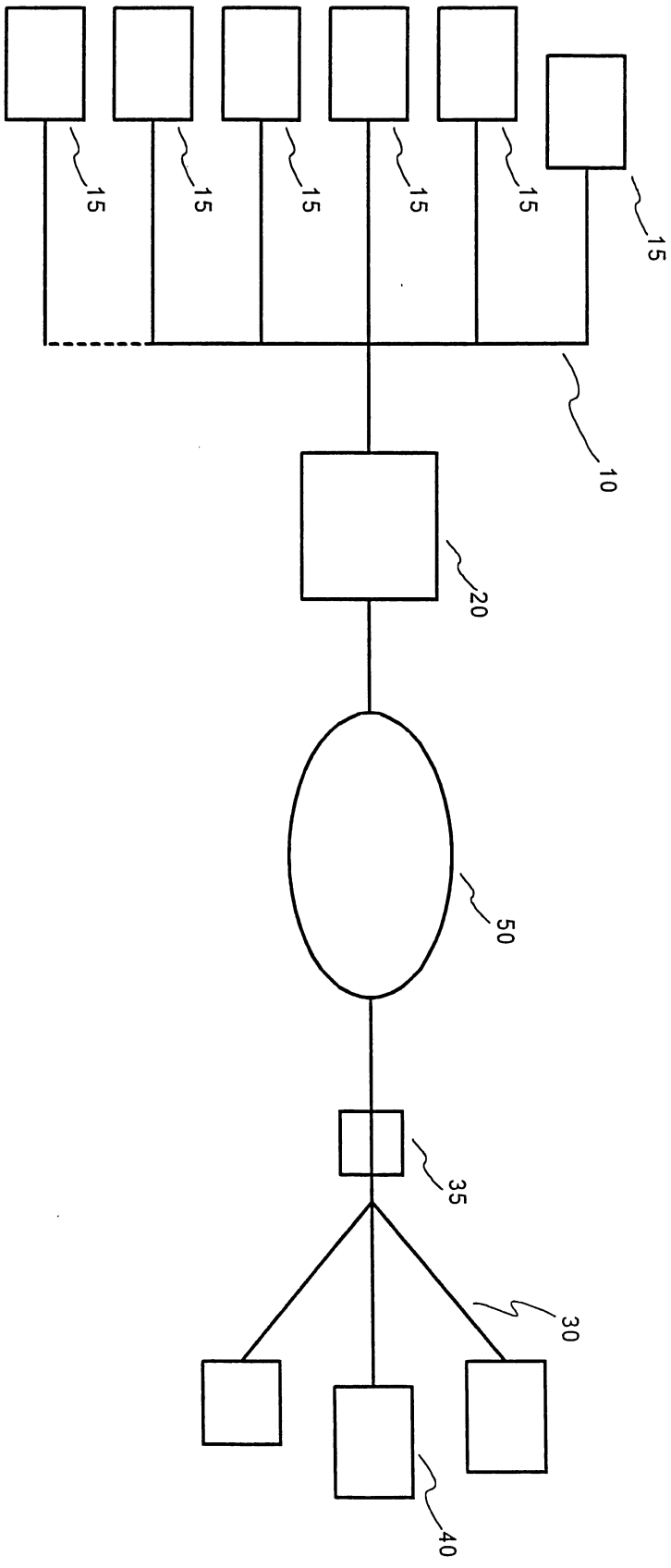
10. 如申請專利範圍第6項所述之處理IP資料封方法，其中前述之外部網路即為網際網路。

11. 如申請專利範圍第5項所述之一種處理IP資料封方法，其中前述之區域網路即為一虛擬私人網路。

12. 如申請專利範圍第6項所述之一種處理IP資料封方法，其中前述之區域網路即為一虛擬私人網路。

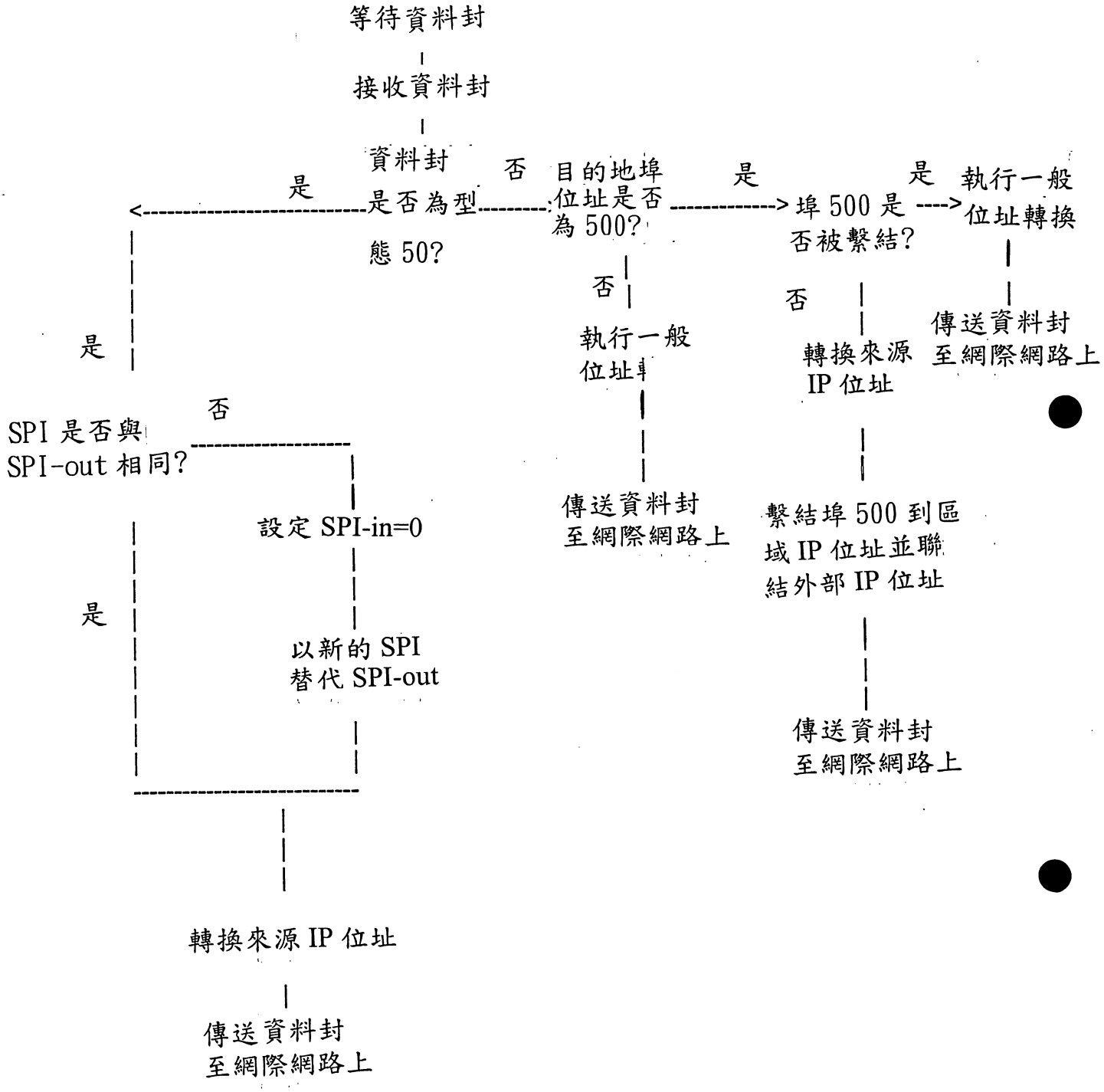
494301

891>4867



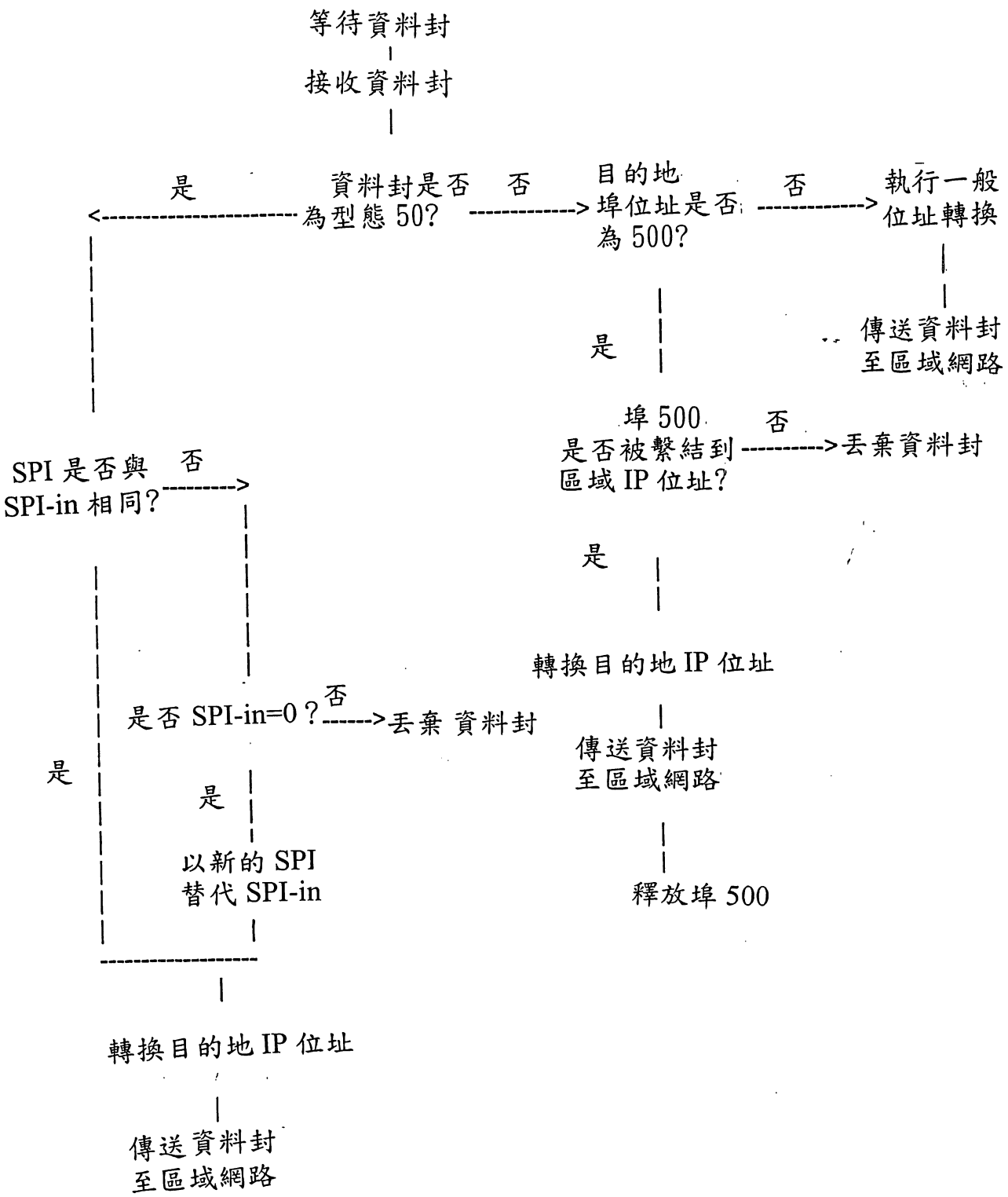
圖一

區域網路資料封決策樹



圖二

網際網路資料封決策樹



圖三

IP 位址

	區域電腦	內部閘道	外部閘道	預定目標	
L-1	192.168.0.2	102.168.0.1	142.140.3.6	204.71.202.160	T-1
L-2	192.168.0.4	102.168.0.1	142.140.3.6	207.46.131.137	T-2
L-3	192.168.0.3	102.168.0.1	142.140.3.6	207.158.227.235	T-3

圖四

SPI 表—八部區域電腦與三部主機通訊

	預定目標	區域 IP		SPI-out	SPI-in
T-1	204.71.202.160	192.168.0.2	L-1	4859	9802
		192.168.0.5	L-x	52856	7000
		192.168.0.10	L-x	8565	8523
T-2	207.46.131.137	192.168.0.4	L-2	1353	6234
		192.168.0.7	L-x	2562	10125
		192.168.0.10	L-x	25763	12106
T-3	207.158.227.235	192.168.0.3	L-3	38935	7753
		192.168.0.8	L-x	9093	32828

圖五 a

新期間—新 SPI-out—SPI-in 設定為 0

	預定目標	區域 IP		SPI-Out	SPI-In
T-1	204.71.202.160	192.168.0.2	L-1	14662	0
		192.168.0.5	L-x	52856	7000
		192.168.0.10	L-x	8565	8523
T-2	207.46.131.137	192.168.0.4	L-2	1353	4562
		192.168.0.7	L-x	2562	10125
		192.168.0.10	L-x	25763	12106
T-3	207.158.227.235	192.168.0.3	L-3	8773	20889
		192.168.0.8	L-x	9093	32828

圖五 b

封包接收回應－接收新 SPI-in

	預定目標	區域 IP		SPI-OU	SPI-IN
T-1	207.200.0.2	192.168.0.2	L-1	14662	3288
		192.168.0.5	L-x	52856	7000
		192.168.0.10	L-x	8565	8523
T-2	206.23.5.120	192.168.0.4	L-2	1353	6234
		192.168.0.7	L-x	43966	17937
		192.168.0.10	L-x	25763	12106
T-3	207.198.75.3	192.168.0.3	L-3	8773	20889
		192.168.0.8	L-x	9093	32828

圖五 C

通過閘道的連續封包　　單一區域裝置－單一預定目標							
路徑	資料封型態	來源位址 IP	埠	目的地位址 IP	埠	SPI	列
LAN - Gate	UDP	192.168.0.2	6404	204.71.202.160	80		1
Gate - Net	UDP	142.140.3.6	10425	204.71.202.160	80		2
Net - Gate	UDP	204.71.202.160	80	142.140.3.6	10425		3
Gate - LAN	UDP	204.71.202.160	80	192.168.0.2	6404		4
LAN - Gate	ISAKMP-1	192.168.0.2	500	204.71.202.160	500		5
Gate - Net	ISAKMP-1	142.140.3.6	500	204.71.202.160	500		6
Net - Gate	ISAKMP-2	204.71.202.160	500	142.140.3.6	500		7
Gate - LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500		8
LAN - Gate	ISAKMP-3	192.168.0.2	500	204.71.202.160	500		9
Gate - Net	ISAKMP-3	142.140.3.6	500	204.71.202.160	500		10
Net - Gate	ISAKMP-4	204.71.202.160	500	142.140.3.6	500		11
Gate - LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500		12
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		13
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		14
Net - Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		15
Gate - LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500		16
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859	17
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859	18
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802	19
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	20
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859	21
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859	22
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802	23
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	24
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		14662	25
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		14662	26
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		3288	27
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		3288	28
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		14662	29
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		14662	30
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		3288	31
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		3288	32

圖六

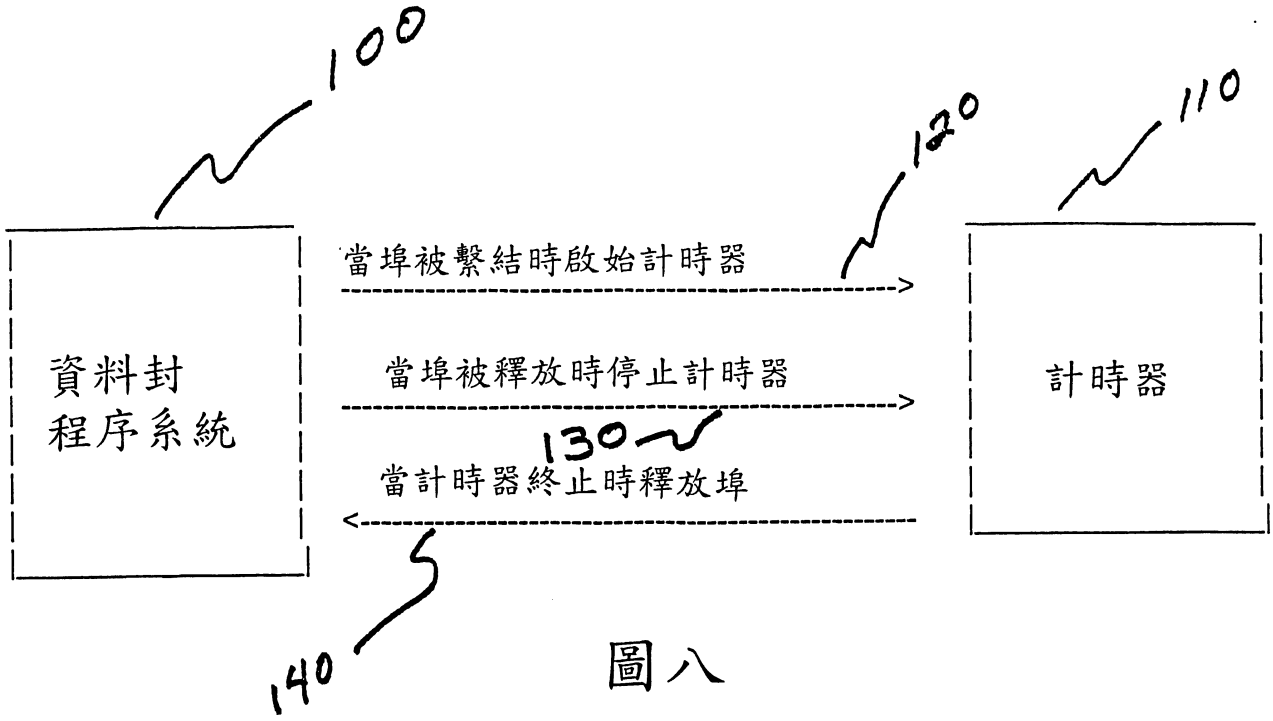
通過閘道的連續封包　　多個區域裝置－多個預定目標

路徑	封包型態	來源位址 IP	伺服器	目的地位址 IP	伺服器	SPI	目前執行	列
LAN - Gate	UDP	192.168.0.2	6404	204.71.202.160	80		L-1 Out	1
Gate - Net	UDP	142.140.3.6	10425	204.71.202.160	80		T-1 In	2
LAN - Gate	UDP	192.168.0.4	4562	207.46.131.137	1353		L-2 Out	3
Gate - Net	UDP	142.140.3.6	37525	207.46.131.137	1353		T-2 In	4
Net - Gate	UDP	204.71.202.160	80	142.140.3.6	10425		T-1 Out	5
Gate - LAN	UDP	204.71.202.160	80	192.168.0.2	6404		L-1 In	6
Net - Gate	UDP	207.46.131.137	1353	142.140.3.6	37525		T-2 Out	7
Gate - LAN	UDP	207.46.131.137	1353	192.168.0.4	4562		L-2 In	8
LAN - Gate	ISAKMP-1	192.168.0.2	500	204.71.202.160	500		L-1 Out – Port 500 bound to 192.168.0.	9
Gate - Net	ISAKMP-1	142.140.3.6	500	204.71.202.160	500		T-1 In – Associated with 204.71.202.160	10
Net - Gate	ISAKMP-2	204.71.202.160	500	142.140.3.6	500		T-1 Out	11
Gate - LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500		L-1 In – Port 500 released	12
LAN - Gate	ISAKMP-3	192.168.0.2	500	204.71.202.160	500		L-1 Out – Port 500 bound to 192.168.0.	13
Gate - Net	ISAKMP-3	142.140.3.6	500	204.71.202.160	500		T-1 In – Associated with 204.71.202.160	14
LAN - Gate	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L-3 Out	15
Gate - Net	ISAKMP-1	142.140.3.6	500	207.158.227.235	8773		T-3 In - Port 500 not available	16
Net - Gate	ISAKMP-4	204.71.202.160	500	142.140.3.6	500		T-1 Out	17
Gate - LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500		L-1 In – Port 500 released	18
LAN - Gate	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L-3 Out	19
Gate - Net	ISAKMP-1	142.140.3.6	500	207.158.227.235	500		T-3 In - Port 500 bound to 192.168.0.3	20
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out – Port 500 not available	21
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	9063		T-1 In – Source port address translated	22
Net - Gate	ISAKMP-2	207.158.227.235	500	142.140.3.6	500		T-3 Out	23
Gate - LAN	ISAKMP-2	207.158.227.235	500	192.168.0.3	500		L-3 In – Port 500 released	24
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out – Port 500 bound to 192.168.0.	25
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 In – Associated with 204.71.202.160	26
							Time-out for T-1 Out--Port 500 released	27
LAN - Gate	ISAKMP-3	192.168.0.3	500	207.158.227.235	500		L-3 Out	28
Gate - Net	ISAKMP-3	142.140.6.3	500	207.158.227.235	500		T-3 In - Port 500 bound to 192.168.0.3	29
Net - Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 Out – Port 500 blocked	30
							T-1 Out – packet ignored	31
Net - Gate	ISAKMP-4	207.158.227.235	500	142.140.3.6	500		T-3 Out	32
Gate - LAN	ISAKMP-4	207.158.227.235	500	192.168.0.3	500		L-3 In – Port 500 released	33
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out – Port 500 bound to 192.168.0.	34
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 In – Associated with 204.71.202.160	35
Net - Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 Out	36
Gate - LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500		L-1 In – Port 500 released	37

圖七(第一頁)

LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859	L-1 Out	38
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859	T-1 In	39
LAN - Gate	UDP	192.168.0.4	4562	207.46.131.137	1353		L-2 Out	40
Gate - Net	UDP	142.140.3.6	37525	207.46.131.137	1353		T-2 In	41
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802	T-1 Out	42
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	L-1 In	43
LAN - Gate	ISAKMP-5	192.168.0.3	500	207.158.227.235	500		L-3 Out - Port 500 bound to 192.168.0.3	44
Gate - Net	ISAKMP-5	142.140.6.3	500	207.158.227.235	500		T-3 In - Associated with 207.158.227.23	45
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859	L-1 Out	46
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859	T-1 In	47
Net - Gate	ISAKMP-6	207.158.227.235	500	142.140.3.6	500		T-3 Out	48
Gate - LAN	ISAKMP-6	207.158.227.235	500	192.168.0.3	500		L-3 In – Port 500 released	49
Net - Gate	UDP	207.46.131.137	1353	142.140.3.6	37525		T-2 Out	50
Gate - LAN	UDP	207.46.131.137	1353	192.168.0.4	4562		L-2 In	51
LAN - Gate	ESP (50)	192.168.0.3		207.158.227.235		38935	L-3 Out	52
Gate - Net	ESP (50)	142.140.6.3		207.158.227.235		38935	T-3 In	53
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802	T-1 Out	54
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	L-1 In	55
Net - Gate	ESP (50)	207.158.227.235		142.140.3.6		7753	T-3 Out	56
Gate - LAN	ESP (50)	207.158.227.235		192.168.0.3		7753	L-3 In	57

圖七(第二頁)


100
120
110
資料封
程序系統
當埠被繫結時啟始計時器
當埠被釋放時停止計時器
130
當計時器終止時釋放埠
計時器
140

圖八