

VPN

本 NUS-MS3000 採 VPN 方式建立安全與私密的網路通訊服務，結合遠端用戶認證辨識系統，以整合企業各個遠地網路與全球外勤人員遠地個人電腦，提供公司企業與遠端使用者一個安全便利的網路加密方式，讓企業在網際網路上傳遞資料時，得到最佳的效能及保密效果，更節省管理者管理太多鑰匙的麻煩。

【IPSec Autokey】：系統管理員可於此單元以加密功能建立連線兩端以固定標準方式交換網路加密鑰匙碼，並設定 IPSec Lifetime（加密鑰匙更新週期），啟動 NUS-MS3000 系統自動隨機選取更新無法被判讀入侵的加密鑰匙碼。

【CA 證書】：系統管理員可於此單元匯入【IPSec Autokey】在使用【認證方法】為 RSA-SIG 時，所需之 CA Server 證書。

【本地證書】：系統管理員可於此單元設定並產生 Private Key 以及 CSR（Certificate Signing Request）。且可匯入【IPSec Autokey】在使用【認證方法】為 RSA-SIG 時，所需之 CSR（Certificate Signing Request）交由 CA Server 簽署後取回的證書。

【PPTP 伺服器】：系統管理員可於此單元建立 VPN-PPTP 伺服器的相關功能設定。

【PPTP 用戶端】：系統管理員可於此單元建立 VPN-PPTP 用戶端的相關功能設定。

【VPN Trunk】：系統管理員可於此單元建立 VPN 負載平衡和備援(要配合 GRE /IPSec 功能來運作)的相關功能設定。



如何運用網路驗證

建立虛擬私有網路驗證 Virtual Private Network (VPN)，需先將 IPSec Autokey、PPTP 伺服器或 PPTP 用戶端的連線設定套用到 Trunk 功能中，並將要彼此連線溝通的 VPN Trunk 條例套用至設有相關管制規則的【管制條例】中，即可為連線兩端建立安全保密的網路通訊。

【VPN】專有名詞解釋：

RSA 說明如下：

- 為非對稱性密碼系統，使用者擁有兩把金鑰，一個為秘密金鑰，使用者須秘密收藏，為連線解密時用，另一個為公開金鑰，將任何欲傳送訊息者皆可自認證中心取得，並使用此金鑰將訊息加密傳送給接收者。

Preshared Key 說明如下：

- 當 VPN 雙方進行連線時用來進行 IPSec 驗證用的專用的 Key.

ISAKMP 說明如下：

- 「IP Security Association Key Management Protocol」(ISAKMP) 就是提供一種方法供兩台電腦建立安全性關聯 (SA)。SA(Security Association) 對兩台電腦之間進行連線編碼，指定使用哪些演算法和什麼樣的金鑰長度或實際加密金鑰。事實上 SA 不止一個連線方式：從兩台電腦 ISAKMP SA 作為起點，必須指定使用何種加密演算法 (DES、triple DES、40 位元 DES 或根本不用)、使用何種認證。

Main mode 說明如下：

- 在 VPN 第一階段的 IKE 開始連線時，會提供兩種模式選擇，其中的一種模式就是 Main mode，會對資料交換的雙方先進行認證，Main mode 會提供六個訊息在雙方之間進行傳遞來達到認證的需求，確保與自己交流資料是對方本人，而不是偽造的。

Aggressive mode 說明如下：

- 在 VPN 第一階段的 IKE 開始連線時，另一種認證模式就是 Aggressive mode，會對資料交換的雙方先進行認證，Aggressive mode 則僅會提供三個訊息在雙方之間進行傳遞來達到認證的需求，確保與自己交流資料是對方本人，而不是偽造的。

AH (Authentication Header) 說明如下：

- 提供 VPN 連線時的認證及選擇性的認證檢測。

ESP 說明如下：

- (Encapsulated Security Payload) 提供 VPN 連線時的認證及認證檢測。並對傳送中的資料提供了機密和保護。

DES 說明如下：

- 資料加密標準 (Data Encryption Standard) 是一種 NIST 標準安全加密金鑰方法，使用的加密金鑰為 56 位元。

3DES 說明如下：

- 提供比 DES 更加安全的三重資料加密標準 (Triple Data Encryption Standard, 3DES) 安全加密金鑰方法，使用的加密金鑰為 168 位元。

AES 說明如下：

- 為高階加密模式其標準比 DES 的加密標準更加嚴謹，DES 加密金鑰長度為 56 位元，AES 加密金鑰長度則高達 128 位元、192 位元、以及 256 位元。

NULL 演算法 說明如下：

- 是一種快速又便利的連線模式來取代確保其機密性或負責身份驗證而不進行加密的動作。NULL 演算法不提供機密性也沒有提供其他任何安全服務，僅僅是一條快速方便去替換在使用 ESP 加密時的選項。

SHA1 安全雜湊演算法 (Secure Hash Algorithm, SHA) 說明如下：

- 是用於產生訊息摘要或雜湊的演算法。原有的 SHA 演算法已被改良式的 SHA1 演算法取代。可以計算出 160 位元的演算。

MD5 雜湊演算法 說明如下：

- 一種單向字串雜湊演算，其演算方式是將你給予任何長度字串，使用 MD5 雜湊演算法，可以計算出一個長度為 128 位元的演算。

GRE 通用路由協定封裝 說明如下：

- GRE 只提供了資料包的封裝，它沒有防止網路偵聽和攻擊的加密功能。所以在實際環境中它常和 IPsec 一起使用，由 IPsec 為用戶資料的加密，給用戶提供更好的安全服務。

CA 證書 說明如下：

- 即 Self-Signed CA，也就是 CA 之 Certificate 由自己所認證，而非經由其他 CA 來認證。它沒有所謂的上層 CA，通常是 CA 鏈中最頂層的 CA，因此又稱為 Root CA。



本地證書 說明如下：

- 即 Signed CA，也就是 CA 之 Certificate 由其它 CA 所認證；認證它的 CA 為 Signed CA 的上層 CA 或 Parent CA，而 Signed CA 則為 Sub CA 或 Child CA。

【IPSec Autokey】視窗表格內圖示與名詞名稱定義：

i 說明如下：

- 以圖示顯示 VPN 連線建立的狀況。

圖例	--		
代表涵義	條例未被套用	斷線	連線

名稱 說明如下：

- 定義 IPSec AutoKey 名稱。此名稱必須是唯一且不可重複。

WAN 說明如下：

- 本地端網路介面位址。

閘道 IP 位址 說明如下：

- 目的端網路介面位址。

IPSec 演算法 說明如下：

- 顯示目前 VPN 連線的資料加密模式。

變更 說明如下：

- 變更 IPSec VPN 中各項設定值。點選【修改】，可修改自動加密之各項參數，點選【刪除】，可刪除該項設定。(如圖 11-1)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
<input type="button" value="新增"/>					

圖 11-1 IPSec Autokey 視窗表格

【CA 證書】視窗表格內圖示與名詞名稱定義：

名稱 說明如下：

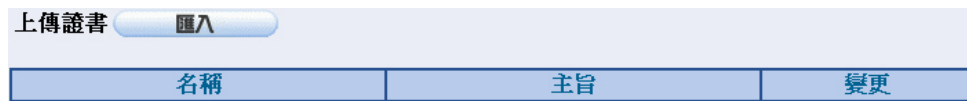
- 為 CA Server 證書的名稱。

主旨 說明如下：

- 為 CA Server 的設定資訊。

變更 說明如下：

- 點選【檢視】，可顯示證書詳細資料，點選【下載】，可下載已匯入至 NUS-MS3000 的證書，點選【刪除】，可刪除已匯入至 NUS-MS3000 的證書。(如圖 11-2)



The screenshot shows a software interface for managing CA certificates. At the top, there is a header bar with the text '上傳證書' (Upload Certificate) on the left and a button labeled '匯入' (Import) in the center. Below the header is a table with three columns: '名稱' (Name), '主旨' (Purpose), and '變更' (Change). The table is currently empty.

名稱	主旨	變更
----	----	----

圖 11-2 CA 證書視窗表格

【本地證書】視窗表格內圖示與名詞名稱定義：

L 說明如下：

- 可分為兩種情形：
 - ◆ 空白：代表匯入經由 CA Server 簽署之非本機設定 CSR (Certificate Signing Request) 所取回之證書。即【IPSec Autokey】在使用【認證方法】為 RSA-SIG 時的遠端 PEM。
 - ◆ V：代表在未匯入證書時，本地自行設定之 CSR (Certificate Signing Request)，和已匯入經由 CA Server 簽署之本地自行設定之 CSR (Certificate Signing Request) 所取回之證書。即【IPSec Autokey】在使用【認證方法】為 RSA-SIG 時的本地 PEM。

名稱 說明如下：

- 為本地自行設定之 CSR (Certificate Signing Request) 和匯入經由 CA Server 簽署之證書名稱。

主旨 說明如下：

- 為本地自行設定之 CSR (Certificate Signing Request) 和匯入經由 CA Server 簽署之證書設定資訊。

變更 說明如下：

- 點選【檢視】，可顯示證書詳細資料，點選【下載】，在未匯入證書時，僅可下載自行設定之 CSR (Certificate Signing Request)；在匯入證書後，僅可下載已匯入至 NUS-MS3000 的證書，點選【刪除】，可刪除自行設定之 CSR (Certificate Signing Request) 或已匯入至 NUS-MS3000 的證書。(如圖 11-3)



圖 11-3 本地證書視窗表格

【PPTP 伺服器】視窗表格內圖示與名詞名稱定義：

PPTP 伺服器 說明如下：



- 可設定開啓或關閉。

用戶端 IP 範圍 說明如下：

- 可設定 PPTP 用戶端連入分配的網路位址範圍。

i 說明如下：

- 以圖示顯示 VPN 連線建立的狀況。

圖例	--		
代表涵義	條例未被套用	斷線	連線

使用者名稱 說明如下：

- PPTP 用戶端連入時所使用的名稱。

用戶端 IP 位址 說明如下：

- PPTP 用戶端連入 PPTP 伺服器時，所使用的用戶端網路位址。

連線歷時 說明如下：

- 顯示目前 PPTP 用戶端與 PPTP 伺服器連線時間。

設定 說明如下：

- 變更 PPTP VPN Server 中各項設定值。點選【修改】，可修改 PPTP 伺服器之各項參數；點選【刪除】，可刪除該項設定。(如圖 11-4)

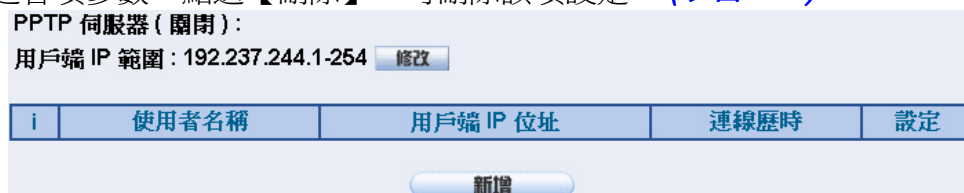




圖 11-4 PPTP 伺服器視窗表格

【PPTP 用戶端】視窗表格內圖示與名詞名稱定義：

i 說明如下：

- 以圖示顯示 VPN 連線建立的狀況。

圖例	--		
代表涵義	條例未被套用	斷線	連線

使用者名稱 說明如下：

- PPTP 用戶端連入 PPTP 伺服器時所使用的名稱。

伺服器位址 說明如下：

- PPTP 用戶端連入 PPTP 伺服器網路位址。

加密認證 說明如下：

- 顯示目前 PPTP 用戶端與 PPTP 伺服器的連線傳輸，是否開啓加密認證機制。

連線歷時 說明如下：

- 顯示目前 PPTP 用戶端與 PPTP 伺服器連線時間。

設定 說明如下：

- 變更 PPTP VPN Client 中各項設定值。點選【修改】，可修改 PPTP 用戶端之各項參數；點選【刪除】，可刪除該項設定。(如圖 11-5)

PPTP 用戶端：



i	使用者名稱	伺服器位址	加密認證	連線歷時	設定
<input type="button" value="新增"/>					

圖 11-5 PPTP 用戶端視窗表格

【VPN Trunk】視窗表格內圖示與名詞名稱定義：

i 說明如下：

- 以圖示顯示 VPN Trunk 連線建立的狀況。

圖例	--		
代表涵義	條例未被啓動	斷線	連線

名稱 說明如下：

- 定義 VPN Trunk 名稱。此名稱必須是唯一且不可重複。

來源子網路 說明如下：

- 來源端子網路位址。

目的端子網路 說明如下：

- 目的端子網路位址。

通道 說明如下：

- 顯示 VPN Trunk 所包含的虛擬私有網路（VPN）驗證通道（IPSec、PPTP Server、PPTP Client）。

變更 說明如下：

- 變更 VPN Trunk 中各項設定值。點選【修改】，可修改自動加密之各項參數；點選【刪除】，可刪除該項設定；點選【暫停】，可停止運作該項設定；點選【啓動】，可使該項設定開啓運作。（如圖 11-6）

i	名稱	來源子網路	目的端子網路	通道	變更
					

圖 11-6 VPN Trunk 視窗表格

我們在此範例設定中，總共架設了 6 種 VPN 環境。

編碼	適用範圍	範例環境	頁碼
範例 1	IPSec Autokey	使用兩台 NUS-MS3000 建立的 IPSec VPN 連線，存取特定網段的資源。	200
範例 2	IPSec Autokey	使用一台 NUS-MS3000 與 Windows 2000 設定 IPSec VPN 連線的方法。	217
範例 3	IPSec Autokey	使用兩台 NUS-MS3000 設定 IPSec VPN 連線的方法。 (連線使用 Aggressive mode) (資料使用 IPSec 演算 3DES 加密.MD5 認證)	276
範例 4	IPSec Autokey	使用兩台 NUS-MS3000 設定 IPSec VPN 的 OutBound Load Balance 連線方法。 (使用 RSA-SIG 認證方法) (使用 ISAKMP 演算法 3DES 加密.MD5 認證) (資料使用 IPSec 演算 3DES 加密.MD5 認證) (使用 GRE 封包封裝)	293
範例 5	PPTP	使用兩台 NUS-MS3000 設定 PPTP VPN 的 OutBound Load Balance 連線方法。	332
範例 6	PPTP	使用一台 NUS-MS3000 與 Windows 2000 設定 PPTP VPN 連線的方法。	348

使用兩台 NUS-MS3000 建立的 IPSec VPN 連線，存取特定網段的資源

先前作業

甲公司 WAN IP 為 61.11.11.11
LAN IP 為 192.168.10.X
乙公司 WAN IP 為 211.22.22.22
LAN IP 為 192.168.20.X
Multiple Subnet 為 192.168.85.X

本範例以兩台 NUS-MS3000 作為平台操作。假設甲公司 192.168.10.100 要向乙公司 192.168.85.100 做【虛擬私有網路】連線並下載其分享檔案。

甲公司的預設閘道為 NUS-MS3000 的 LAN IP 192.168.10.1，以下為其設定步驟：

步驟1. 進入甲公司 NUS-MS3000 預設位址 192.168.10.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖11-7)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
<input type="button" value="新增"/>					

圖 11-7 IPSec Autokey 視窗

步驟2. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_A，並選擇甲公司用來建立 VPN 連線的【外部網路介面】位址 WAN1。 (如圖 11-8)

需填項目	
名稱	VPN_A
外部網路介面	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-8 IPSec VPN 連線名稱和使用的外網路介面設定表單

步驟3. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線乙公司的遠端 IP 位址。 (如圖 11-9)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	211.22.22.22
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-9 IPSec 到目的位址設定表單

步驟4. 於【認證方法】表單中，選擇 Preshare，並填入連線時的【加密金鑰】(加密金鑰最高可輸入 100 位元)。 (如圖 11-10)

認證方法	Preshare
本地PEM	Null
遠端PEM	Null
加密金鑰	123456789

圖 11-10 IPSec 認證方法設定表單

- 步驟5. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 MD5 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 1 來進行連線。(如圖 11-11)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	MD5
群組	GROUP 1

圖 11-11 IPSec 加密或認證設定表單

- 步驟6. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:
 【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-12)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-12 IPSec 演算法設定表單

步驟7. 【進階加密】(NO-PFS/ GROUP 1,2,5) 選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒，【使用模式】選擇 Main mode。(如圖 11-13)

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒
使用模式	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

圖 11-13 IPSec 進階加密設定表單

步驟8. 完成 IPSec Autokey 設定。(如圖 11-14)

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-14 IPSec Autokey 設定完成畫面

步驟9. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-15)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（乙公司）內部網路位址 192.168.85.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 VPN_A 之 IPSec VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-16)

新增Trunk	
名稱	IPSec_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.10.0 / 255.255.255.0
到目的位址	<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩
	192.168.85.0 / 255.255.255.0
	<input type="radio"/> 遠端用戶端
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> VPN_A </div> <div style="text-align: center;"> <input type="button" value="刪除"/> <input type="button" value="新增"/> </div> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> VPN_A </div> </div>
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-15 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	IPSec_VPN_Tr..	192.168.10.0	192.168.85.0	VPN_A	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-16 完成新增 VPN Trunk 設定畫面

步驟10. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-17)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-18)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-17 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-18 完成 VPN Trunk 內部至外部管制條例的設定

步驟11. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-19)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-20)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-19 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-20 完成 VPN Trunk 外部至內部管制條例的設定

乙公司的預設開道為 NUS-MS3000 的 LAN IP 192.168.20.1，以下為其設定步驟：

步驟1. 於【系統管理】組態的【Multiple Subnet】功能中，新增下列設定：
(如圖 11-21)

外部網路介面位址 / 連線模式	內部網路介面位址 / 子網路遮罩	變更
外部網路 1 : 211.22.22.22 / NAT 外部網路 2 : 不能使用 外部網路 3 : 不能使用 外部網路 4 : 不能使用	192.168.85.1 / 255.255.255.0	<input type="button" value="修改"/> <input type="button" value="刪除"/>
<input type="button" value="新增"/>		

圖 11-21 Multiple Subnet WebUI 設定畫面

步驟2. 進入乙公司 NUS-MS3000 預設位址 192.168.20.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-22)

i	名稱	WAN	開道 IP 位址	IPSec演算法	變更
<input type="button" value="新增"/>					

圖 11-22 IPSec Autokey 視窗

步驟3. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_B，並選擇乙公司用來建立 VPN 連線的【外部網路介面】位址 WAN1。 (如圖 11-23)

需填項目	
名稱	VPN_B
外部網路介面	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-23 IPSec VPN 連線名稱和使用的網路介面設定表單

步驟4. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線甲公司的遠端 IP 位址。 (如圖 11-24)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	61.11.11.11
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-24 IPSec 到目的位址設定表單

步驟5. 於【認證方法】表單中，選擇 Preshare，並填入連線時的【加密金鑰】(加密金鑰最高可輸入 100 字元)。 (如圖 11-25)

認證方法	Preshare
本地PEM	Null
遠端PEM	Null
加密金鑰	123456789

圖 11-25 IPSec 認證方法設定表單

- 步驟6. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 MD5 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 1 來進行連線。(如圖 11-26)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	MD5
群組	GROUP 1

圖 11-26 IPSec 加密或認證設定表單

- 步驟7. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:
 【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-27)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-27 IPSec 演算法設定表單

步驟8. 【進階加密】(NO-PFS/ GROUP 1,2,5) 選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒，【使用模式】選擇 Main mode。(如圖 11-28)

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒
使用模式	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

圖 11-28 IPSec 進階加密設定表單

步驟9. 完成 IPSec Autokey 設定。(如圖 11-29)

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-29 IPSec Autokey 設定完成畫面

步驟10. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖11-30)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（乙公司）內部網路位址 192.168.85.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 VPN_B 之 IPSec VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖11-31)

新增Trunk	
名稱	IPSec_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.85.0 / 255.255.255.0
到目的位址	<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩
	192.168.10.0 / 255.255.255.0
	<input type="radio"/> 遠端用戶端
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> VPN_B </div> <div style="text-align: center;"> <input type="button" value="刪除"/> <input type="button" value="新增"/> </div> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> VPN_B </div> </div>
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-30 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	IPSec_VPN_Tr..	192.168.85.0	192.168.10.0	VPN_B	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-31 完成新增 VPN Trunk 設定畫面

步驟11. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-32)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-33)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-32 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-33 完成 VPN Trunk 內部至外部管制條例的設定

步驟12. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-34)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-35)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-34 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-35 完成 VPN Trunk 外部至內部管制條例的設定

步驟13. 完成 IPSec VPN 連線 (如圖 11-36)

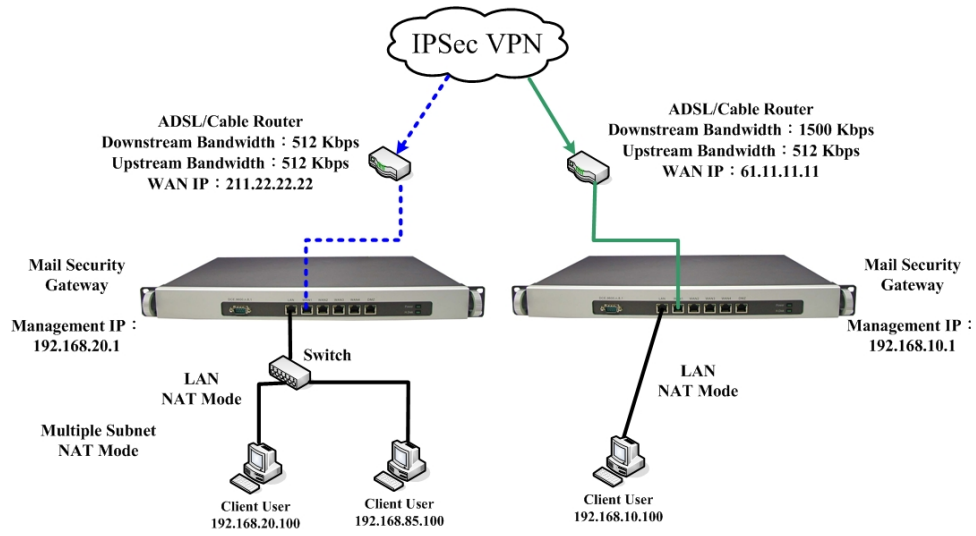


圖 11-36 IPSec VPN 連線之架設環境

使用一台 NUS-MS3000 與 Windows 2000 設定 IPSec VPN 連線的方法

先前作業

甲公司 使用 NUS-MS3000

WAN IP 為 61.11.11.11

LAN IP 為 192.168.10.X

乙公司 使用 Windows2000 之單一 PC

WAN IP 為 211.22.22.22

本範例以一台 NUS-MS3000 及 Windows 2000 VPN-IPsec 作為平台操作。假設乙公司 211.22.22.22 要向甲公司 192.168.10.100 做【虛擬私有網路】連線並下載其分享檔案。

甲公司的預設閘道為 NUS-MS3000 的 LAN IP 192.168.10.1，以下為其設定步驟：

- 步驟1. 進入甲公司 NUS-MS3000 預設位址 192.168.10.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-37)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
<input type="button" value="新增"/>					

圖 11-37 IPSec Autokey 視窗

步驟1. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_A，並選擇甲公司用來建立 VPN 連線的【外部網路介面】位址 WAN1。 (如圖11-38)

需填項目	
名稱	VPN_A
外部網路介面	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-38 IPSec VPN 連線名稱和使用的外網路介面設定表單

步驟2. 於【到目的位址】表單中，選擇遠端閘道或用戶端 - 動態 IP。 (如圖11-39)

到目的位址	
<input type="radio"/> 遠端閘道 -- 固定 IP	<input type="text"/>
<input checked="" type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-39 IPSec 到目的位址設定表單

步驟3. 於【認證方法】表單中，選擇 Preshare，並填入連線時的【加密金鑰】(加密金鑰最高可輸入 100 位元)。 (如圖11-40)

認證方法	Preshare
本地PEM	Null
遠端PEM	Null
加密金鑰	123456789

圖 11-40 IPSec 認證方法設定表單

- 步驟4. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 MD5 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 2 來進行連線。(如圖 11-41)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	MD5
群組	GROUP 2

圖 11-41 IPSec 加密或認證設定表單

- 步驟5. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通：
 【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-42)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-42 IPSec 演算法設定表單

步驟6. 【進階加密】(NO-PFS/ GROUP 1,2,5) 選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒，【使用模式】選擇 Main mode。(如圖 11-43)

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒
使用模式	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

圖 11-43 IPSec 進階加密設定表單

步驟7. 完成 IPSec Autokey 設定。(如圖 11-44)

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_A	WAN1	動態 IP	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-44 IPSec Autokey 設定完成畫面

步驟8. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-45)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【到目的位址】選擇遠端用戶端。
- 【通道】選擇並【新增】名稱爲 VPN_A 之 IPSec VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-46)

新增Trunk	
名稱	IPSec_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.10.0 / 255.255.255.0
到目的位址	
<input type="radio"/> 到目的位址 子網路 / 遮罩	
<input checked="" type="radio"/> 遠端用戶端	
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> VPN_A </div> <div style="text-align: center;"> <input type="button" value="刪除"/> <input type="button" value="新增"/> </div> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> VPN_A </div> </div>
保持連線IP :	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-45 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	IPSec_VPN_Tr..	192.168.10.0	遠端用戶端	VPN_A	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>
<input type="button" value="新增"/>					

圖 11-46 完成新增 VPN Trunk 設定畫面

步驟9. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-47)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-48)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-47 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-48 完成 VPN Trunk 內部至外部管制條例的設定

步驟10. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-49)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-50)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-49 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-50 完成 VPN Trunk 外部至內部管制條例的設定

乙公司的 PC 使用實體 IP (211.22.22.22) ，以下為其設定步驟：

步驟1. 進入 Windows 2000 點選【開始】，選擇【執行】功能。(如圖11-51)

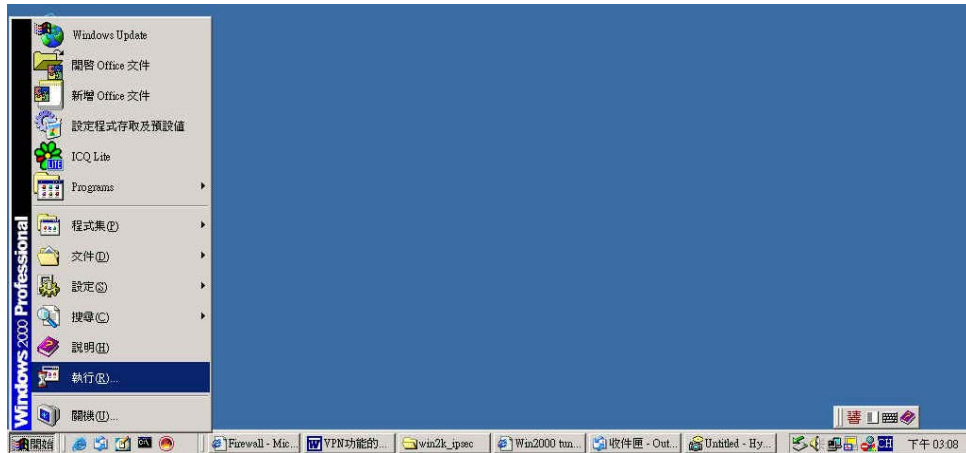


圖 11-51 開始 Windows 2000 IPsec VPN 設定

步驟2. 在【執行】視窗內的【開啓】欄位內輸入指令 mmc。(如圖 11-52)

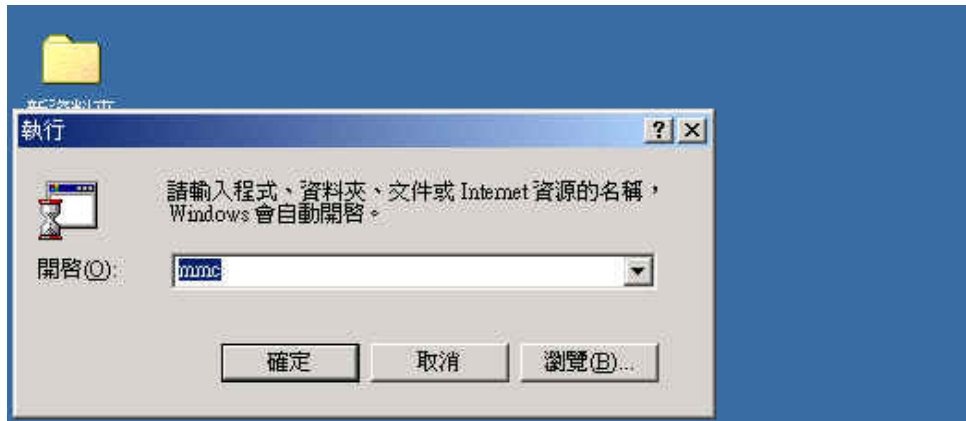


圖 11-52 啟動 Windows 2000 IPsec VPN 設定

步驟3. 進入【主控台 1】視窗時，點選【主控台(C)】選項，並選擇【新增/移除嵌入式管理單元】功能。(如圖 11-53)

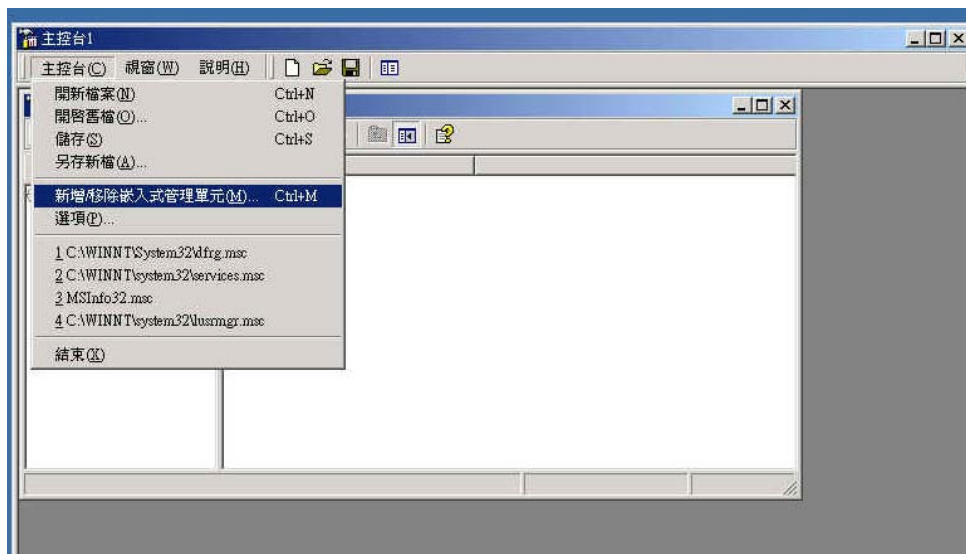


圖 11-53 新增/移除嵌入式管理單元

步驟4. 於【新增/移除嵌入式管理單元】視窗中，按下【新增】鈕，並在【新增獨立嵌入式管理單元】視窗中，新增【IP 安全性原則管理】單元。
(如圖 11-54)

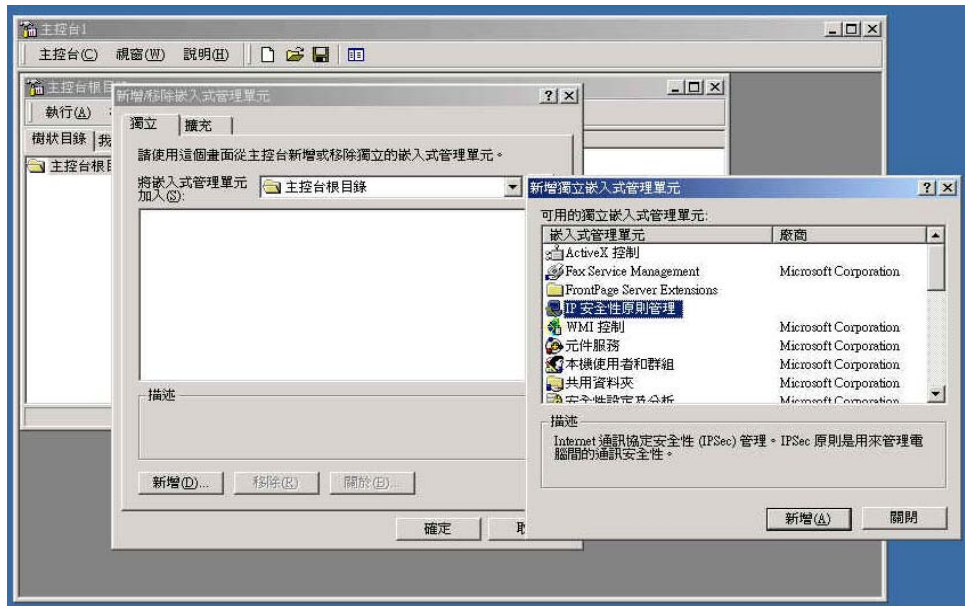


圖 11-54 新增 IP 安全性原則管理

步驟5. 選擇【本機電腦(L)】，並按下【完成】鈕。(如圖11-55)

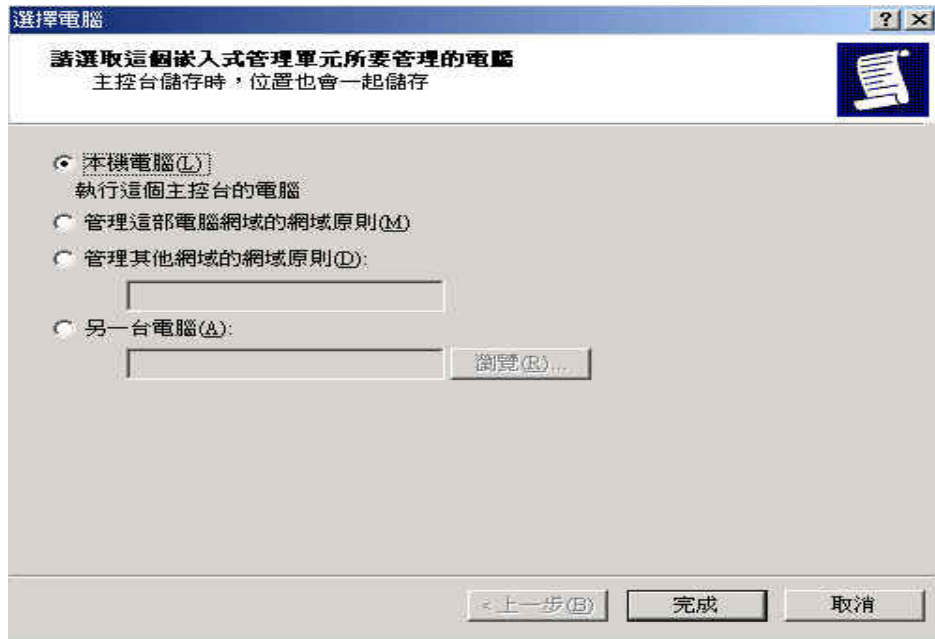


圖 11-55 選擇新增 IP 安全性原則管理之類型

步驟6. 完成新增的動作。(如圖 11-56)

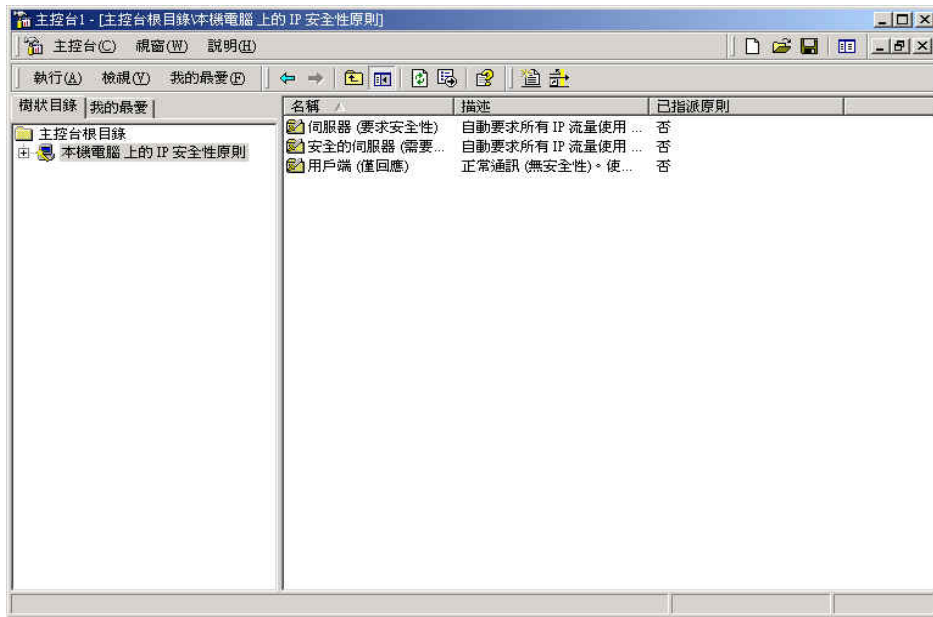


圖 11-56 完成新增 IP 安全性原則管理

步驟7. 在【本機電腦上的 IP 安全性原則】選項上按下滑鼠右鍵，並選擇【建立 IP 安全性原則(C)】選項。(如圖 11-57)

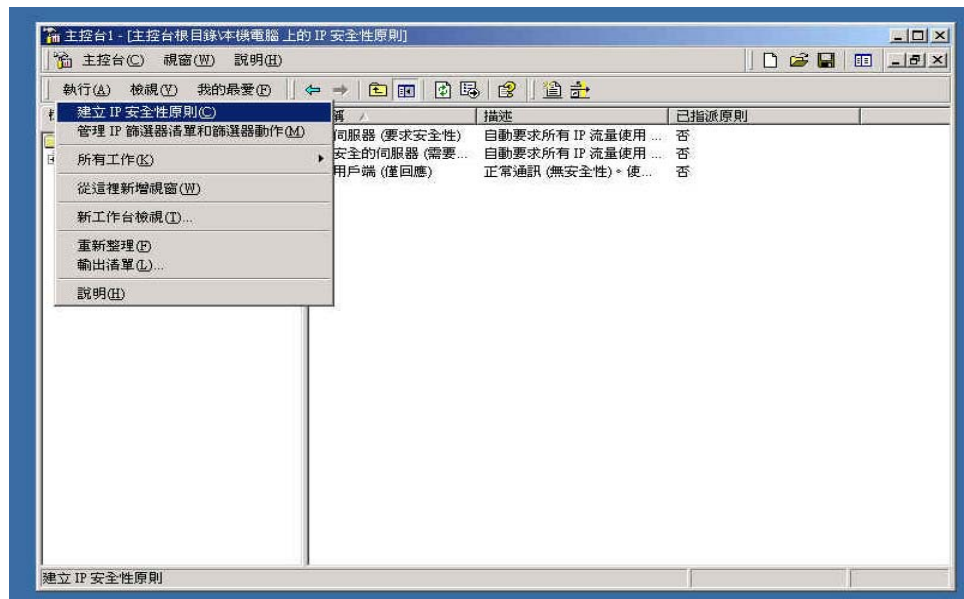


圖 11-57 建立 IP 安全性原則

步驟8. 點選【下一步】。(如圖 11-58)

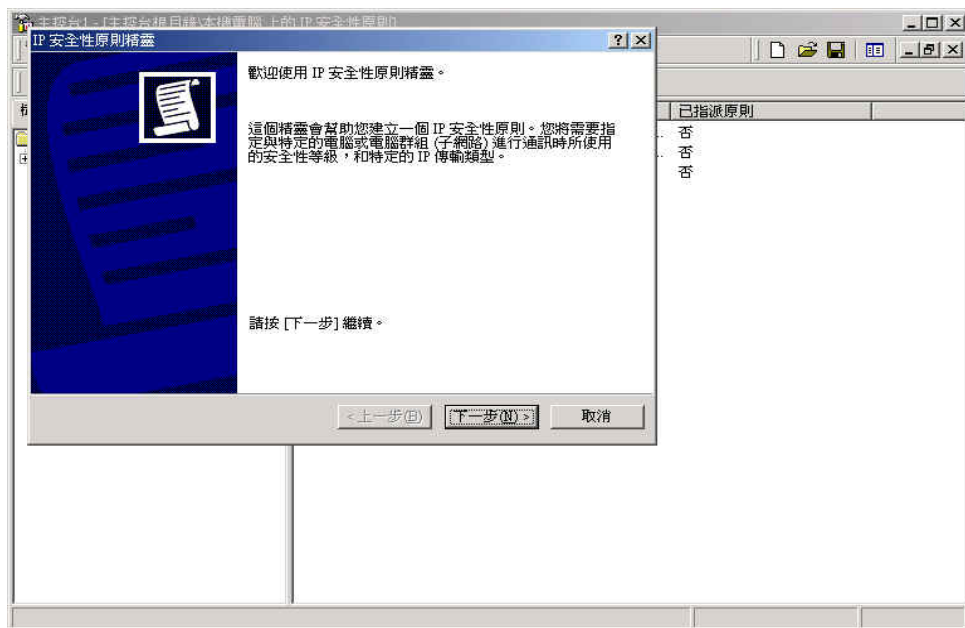


圖 11-58 開啟 IP 安全性原則精靈

步驟9. 填入 VPN 連線所使用的【名稱】及【描述】，並按【下一步】鈕。
(如圖 11-59)



圖 11-59 設定 VPN 連線名稱和描述

步驟10. 請取消使用【啟動預設的回應規則】，並按【下一步】鈕。(如圖11-60)

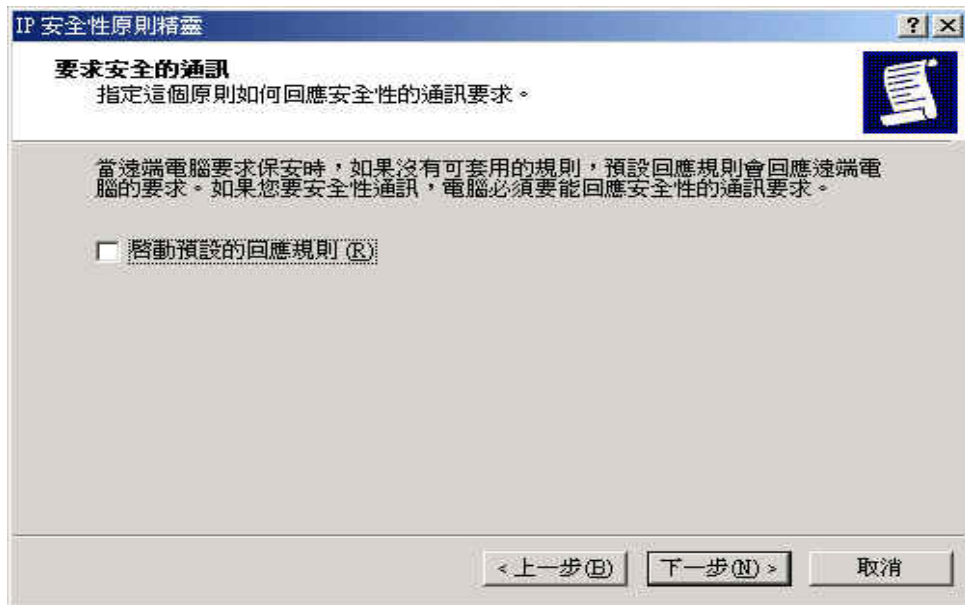


圖 11-60 取消啟動預設的回應規則

步驟11. 於【IP 安全性原則精靈】視窗中，選擇【編輯內容】選項，並按下【完成】鈕。(如圖 11-61)

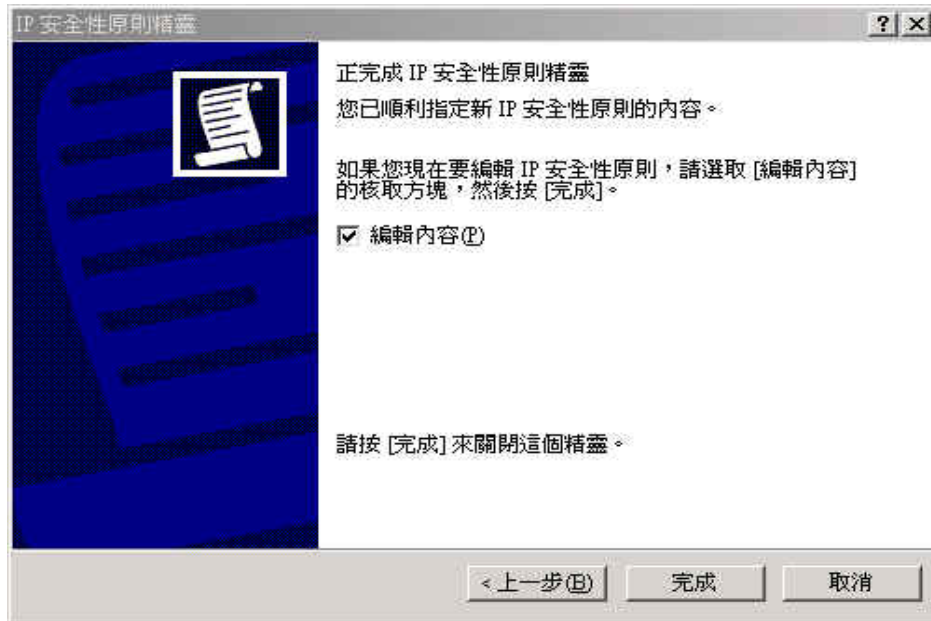


圖 11-61 完成 IP 安全性原則精靈設定

步驟12. 於【VPN_B 內容】視窗中，請勿勾選【使用新增精靈】功能，並按下【新增】鈕。(如圖11-62)

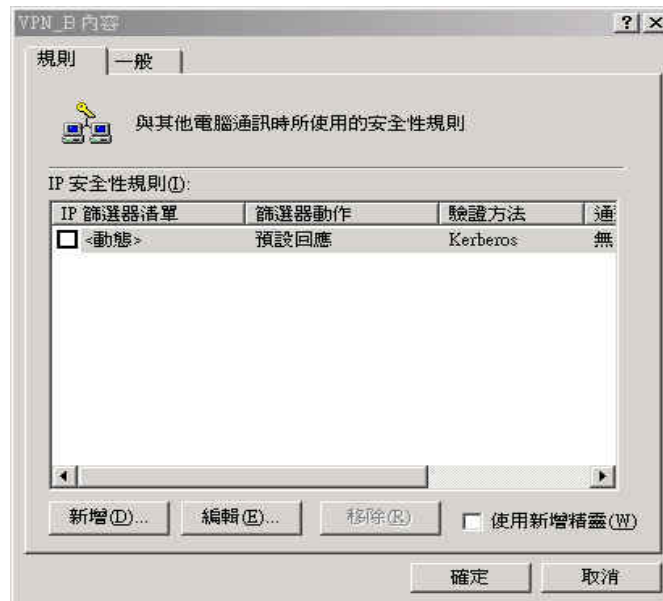


圖 11-62 VPN_B 內容視窗

步驟13. 於【新增規則內容】視窗中，按下【新增】鈕。(如圖11-63)

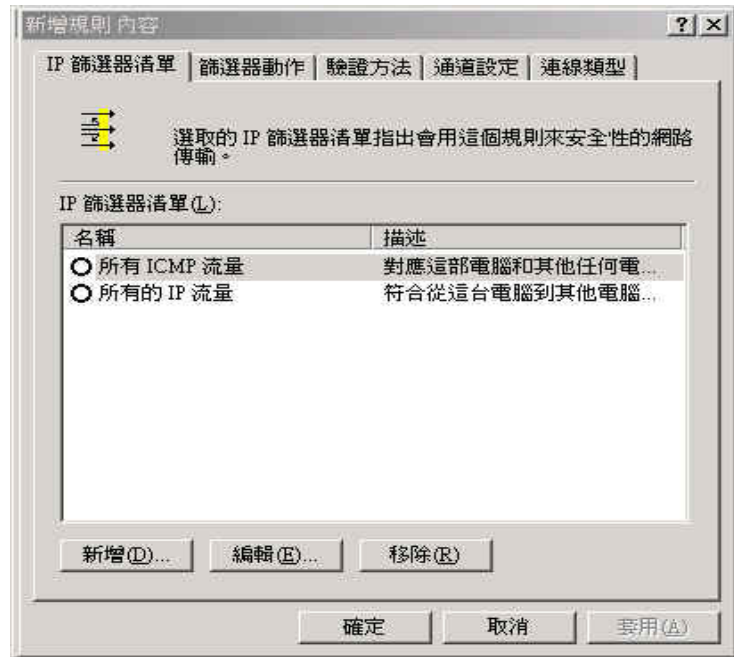


圖 11-63 新增 IP 篩選器清單

步驟14. 在【IP 篩選器清單】視窗中，請勿勾選【使用新增精靈】功能，更改【名稱】為 VPN_B WAN TO LAN，並按下【新增】鈕。(如圖 11-64)

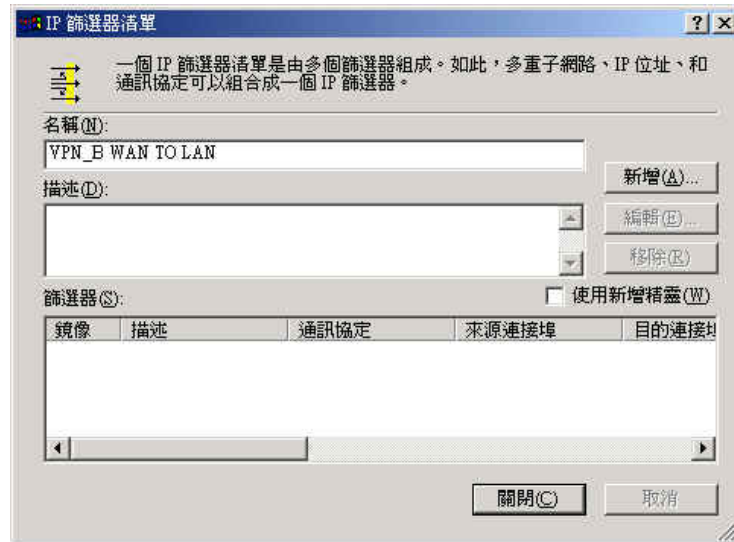


圖 11-64 IP 篩選清單視窗

步驟15. 於【篩選器內容】視窗中，請於【來源位址】的下拉式選單中點選【特定 IP 位址】，並輸入乙公司的外部網路 IP 211.22.22.22 子網路遮罩 255.255.255.255，請於【目的地位址】的下拉式選單中點選【特定 IP 子網路】，並輸入甲公司的內部網路 192.168.10.0 子網路遮罩 255.255.255.0，請勿勾選【已鏡像處理。也對應完全相反的來源及目的地位的封包】功能。(如圖 11-65)

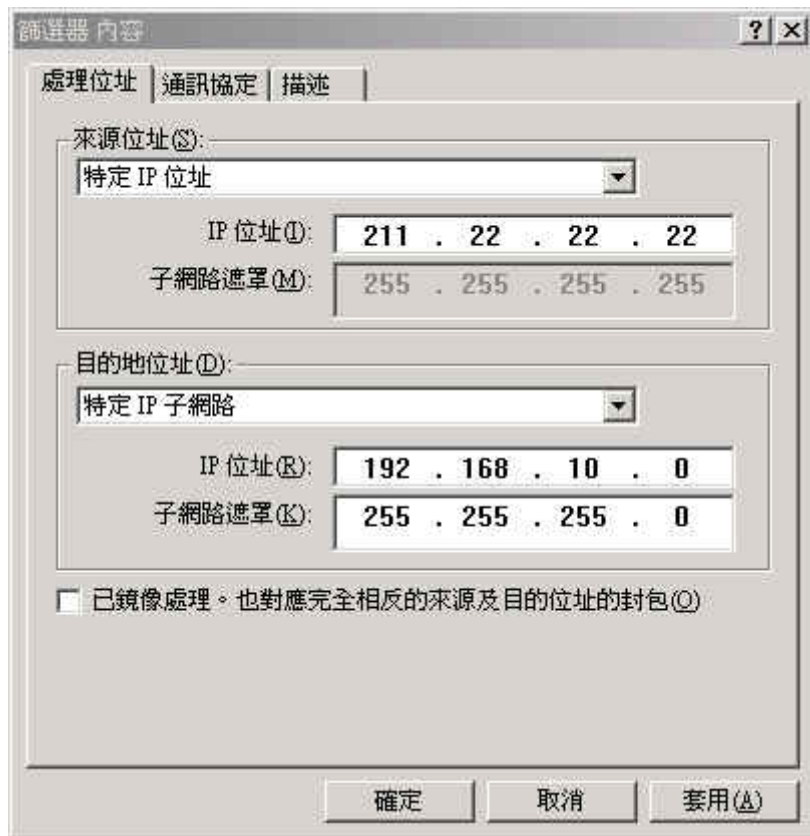


圖 11-65 篩選器內容視窗

步驟16. 完成設定，並關閉【IP 篩選器清單】視窗。(如圖11-66)



圖 11-66 完成 IP 篩選器設定

步驟17. 於【新增規則內容】的【篩選器動作】視窗中，選擇【需要安全性】功能，並按下【編輯】鈕。(如圖11-67)

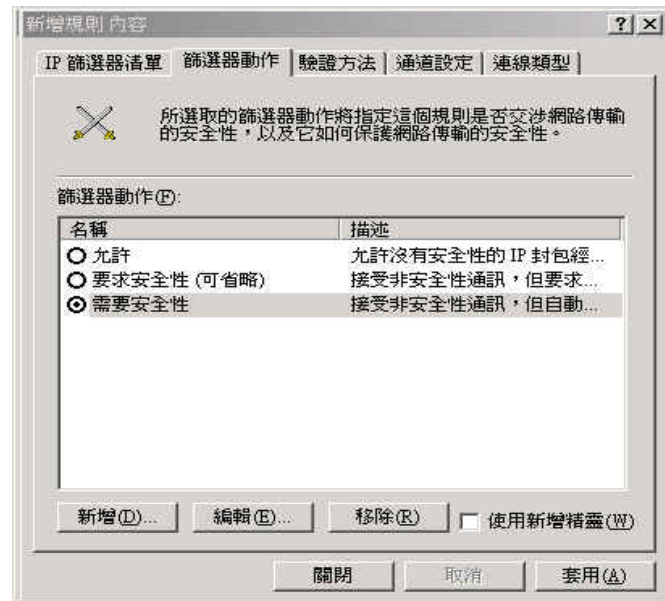


圖 11-67 篩選器動作設定

步驟18. 於【需要安全性內容】視窗中，勾選【工作階段辨識碼完整轉寄密碼】功能。(如圖11-68)

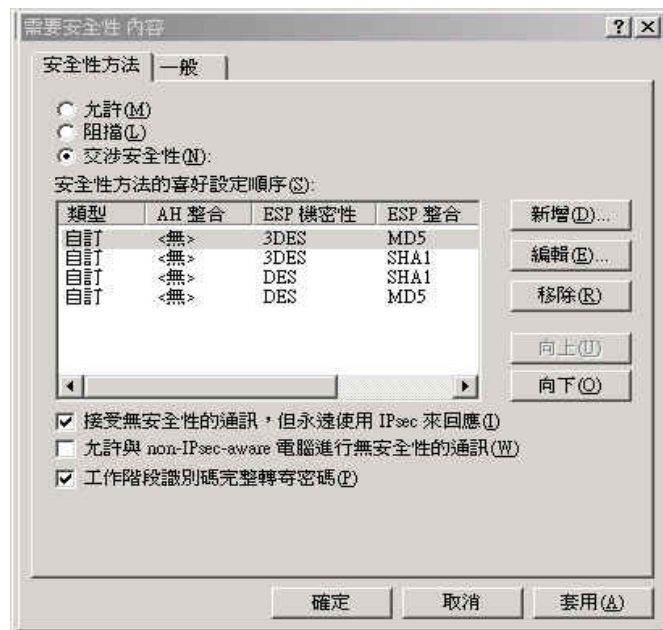


圖 11-68 選取工作階段辨識碼完整轉寄密碼

步驟19. 請選擇 自定 / 無 / 3DES / MD5 安全性方法，並按下【編輯】鈕。(如圖 11-69)

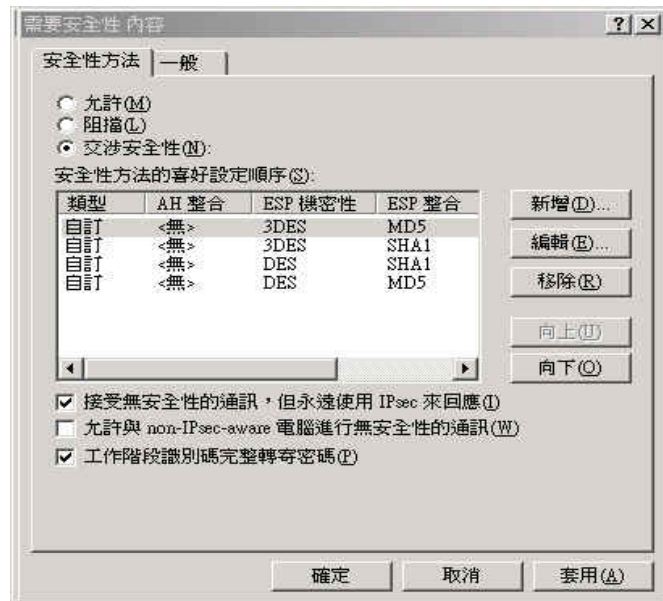


圖 11-69 編輯安全性方法

步驟20. 點選【自訂(提供給專業使用者)】選項，並按下【設定】鈕。(如圖 11-70)

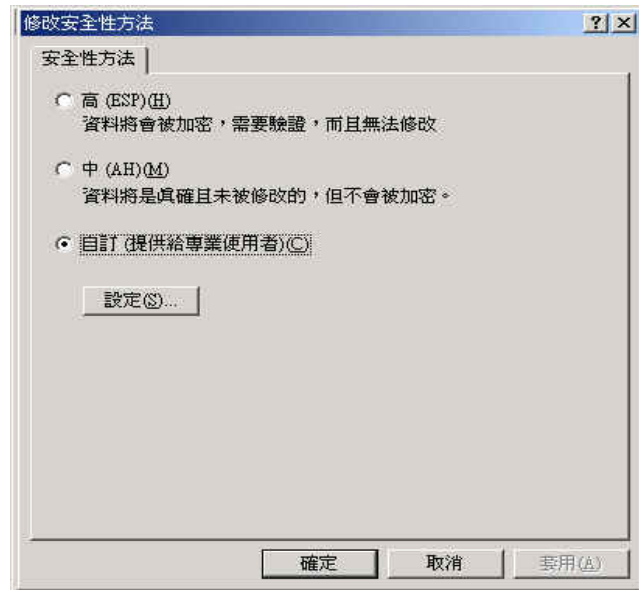


圖 11-70 自訂安全性方法

步驟21. 請勾取【資料完整性及加密(ESP)】，分別選擇【整合演算法】為 MD5 和【加密演算法】為 3DES，勾選【產生新金鑰間隔】，並輸入 28800 秒。然後按 3 次【確定】回到【新增規則內容】視窗。(如圖 11-71)

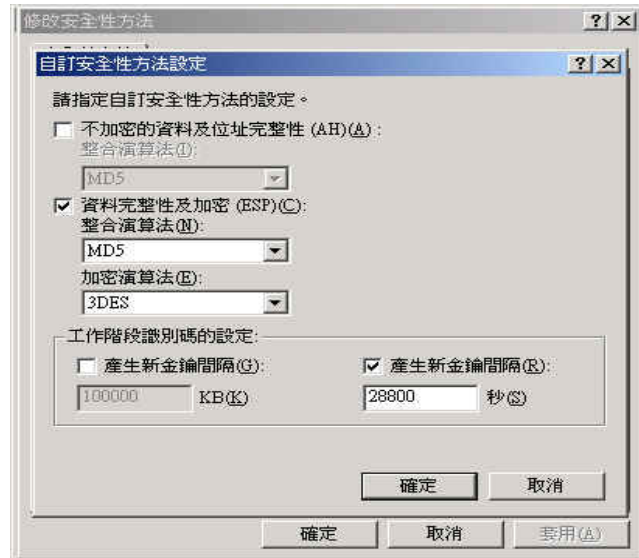


圖 11-71 設定自訂安全性方法

步驟22. 於【新增規則內容】的【連線類型】視窗中，選擇【所有網路連線】。(如圖 11-72)

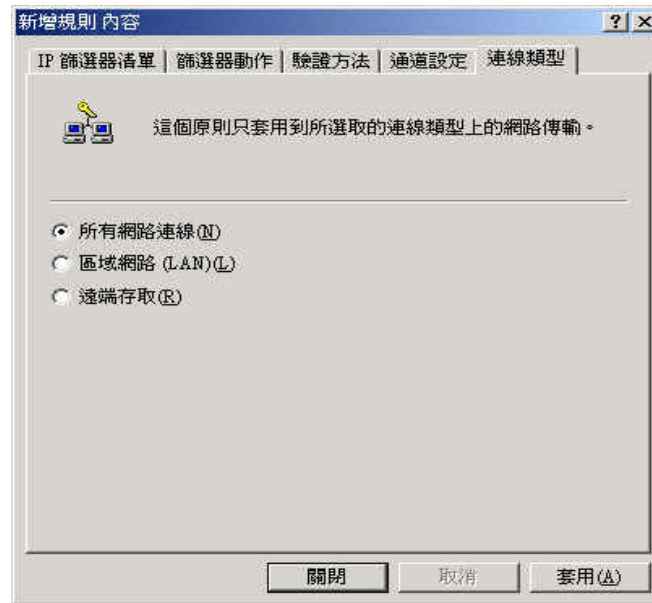


圖 11-72 連線類型設定

- 步驟23. 於【新增規則內容】的【通道設定】視窗中，選擇【由這個 IP 位址來指定通道的結束點】，並輸入甲公司 WAN 的 IP 位址 61.11.11.11。
(如圖 11-73)



圖 11-73 通道設定視窗

步驟24. 於【新增規則內容】的【驗證方法】視窗中，按下【編輯】鈕。(如圖 11-74)

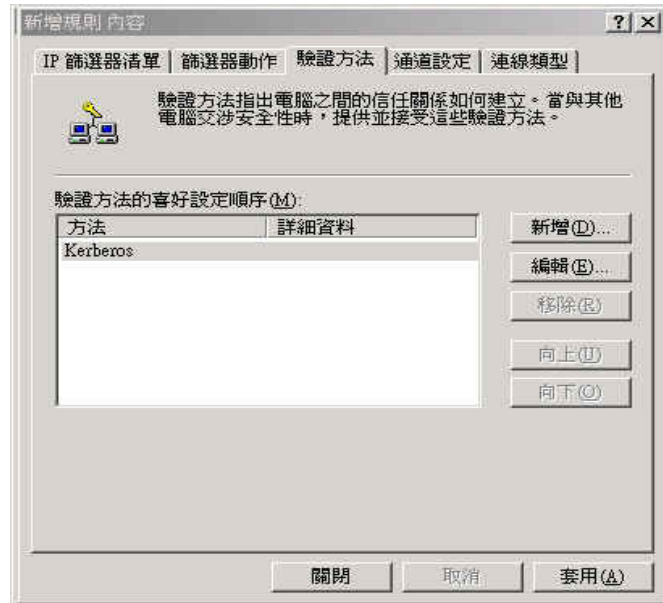


圖 11-74 驗證方法設定視窗

步驟25. 點選【使用這個字串來保護金鑰間的交換】選項，並輸入雙方所要連線的金鑰 123456789。(如圖11-75)

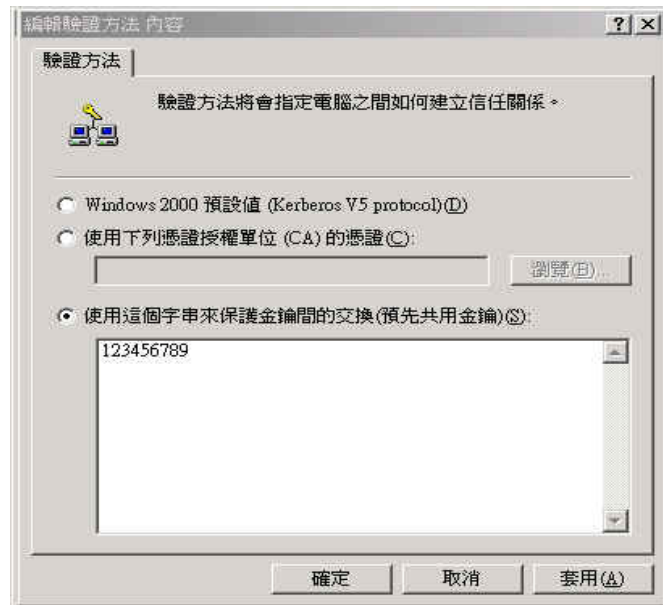


圖 11-75 設定 VPN 連線金鑰

步驟26. 【套用】設定，並關閉設定視窗。(如圖11-76)

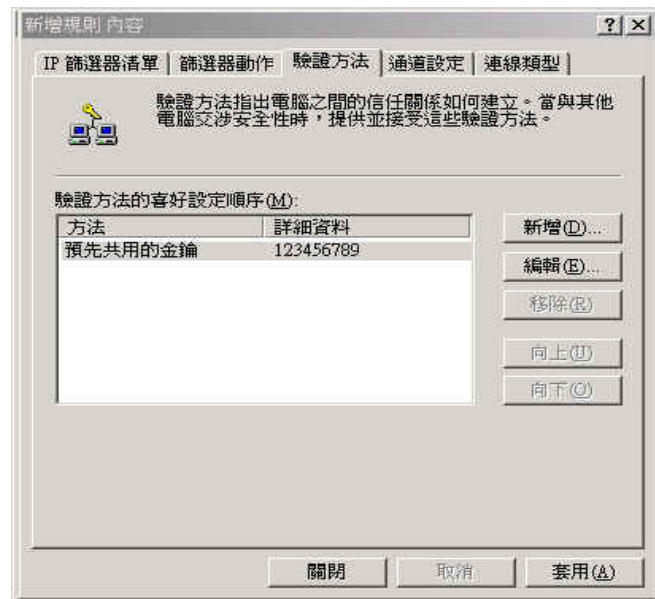


圖 11-76 完成驗證方法設定

步驟27. 完成 VPN_B WAN TO LAN 規則所有設定。(如圖 11-77)

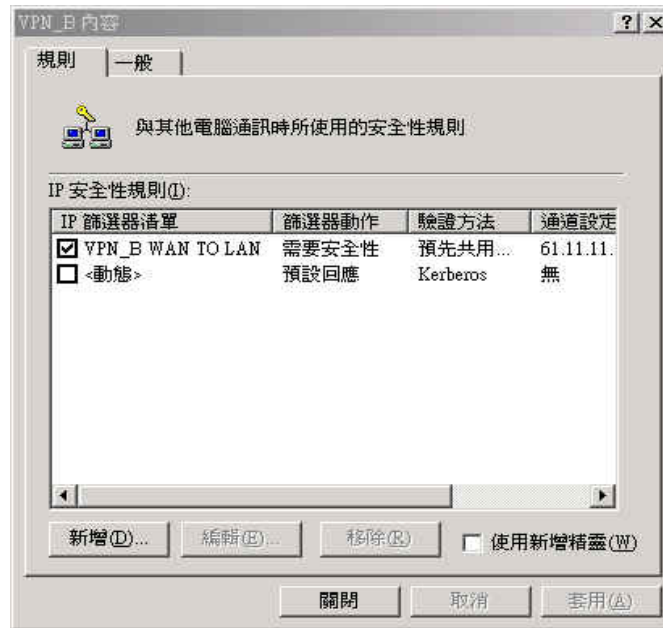


圖 11-77 完成 VPN_B WAN TO LAN 規則設定

步驟28. 請再次進入【VPN_B 內容】視窗，請勿勾選【使用新增精靈】功能，並按下【新增】鈕，以新增第二條 IP 安全性規則。(如圖 11-78)

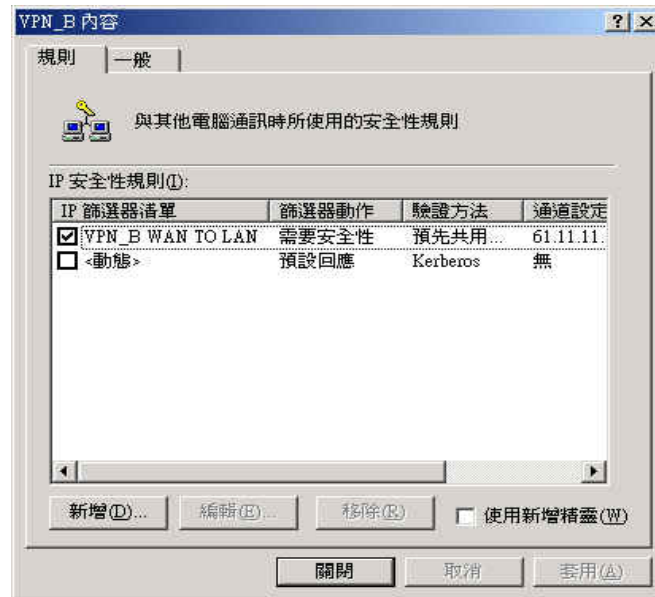


圖 11-78 VPN_B 內容視窗

步驟29. 於【新增規則內容】視窗中，按下【新增】鈕。(如圖11-79)

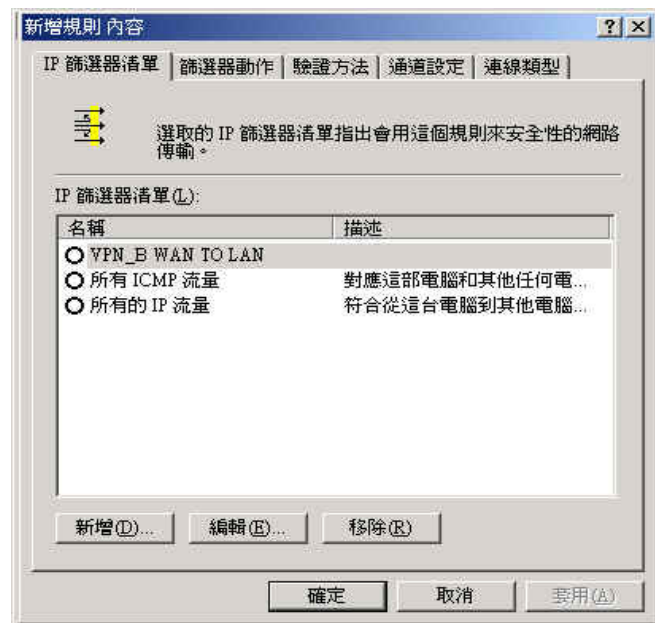


圖 11-79 新增規則內容視窗

步驟30. 於【IP 篩選器清單】視窗中，請勿勾選【使用新增精靈】功能，更改【名稱】為 VPN_B LAN TO WAN，並按下【新增】鈕。(如圖 11-80)

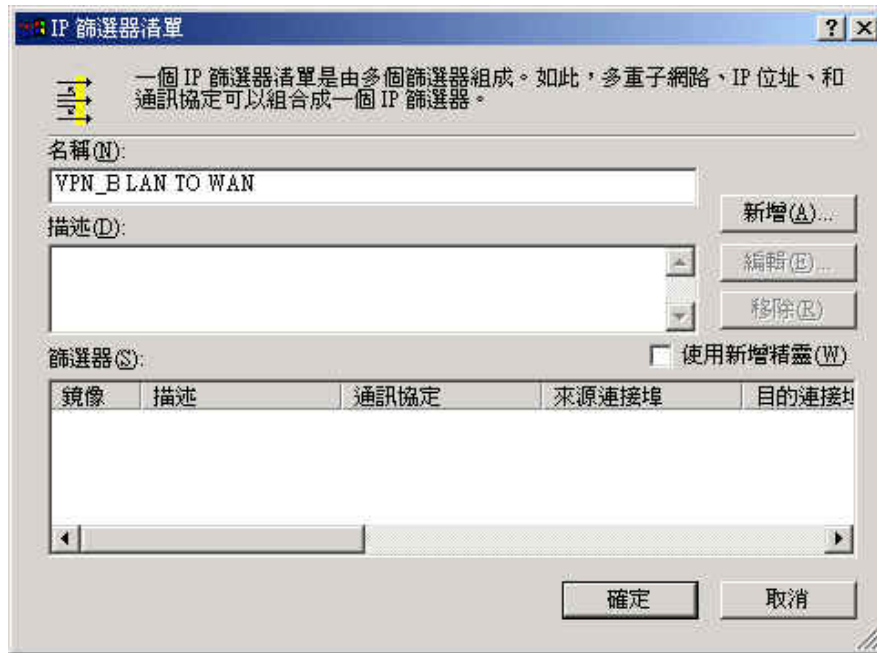


圖 11-80 IP 篩選清單視窗

步驟31. 於【篩選器內容】視窗中，請於【來源位址】的下拉式選單中點選【特定 IP 子網路】，並輸入甲公司的內部網路 192.168.10.0 子網路遮罩 255.255.255.0，請於【目的地位址】的下拉式選單中點選【特定 IP 位址】，並輸入乙公司的外部網路 IP 211.22.22.22 子網路遮罩 255.255.255.255，請勿勾選【已鏡像處理。也對應完全相反的來源及目的地位的封包】功能。(如圖 11-81)

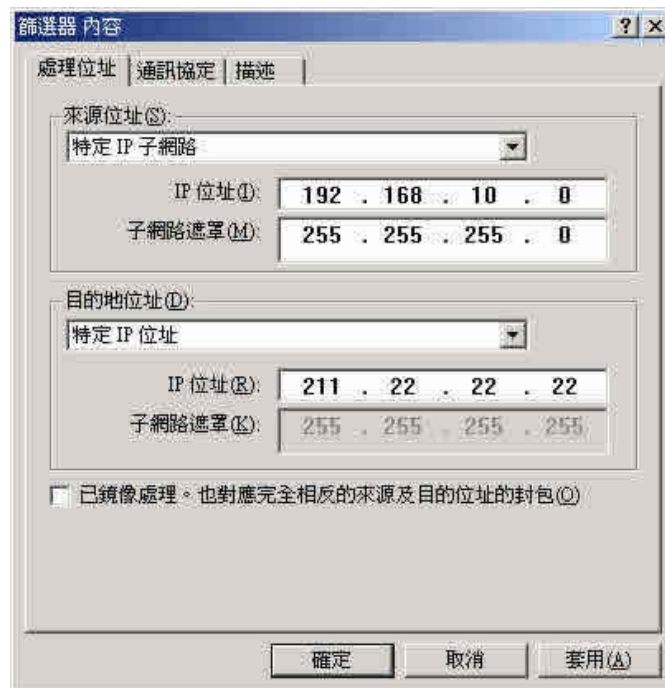


圖 11-81 篩選內容視窗

步驟32. 完成設定，並關閉【IP 篩選器清單】。(如圖11-82)

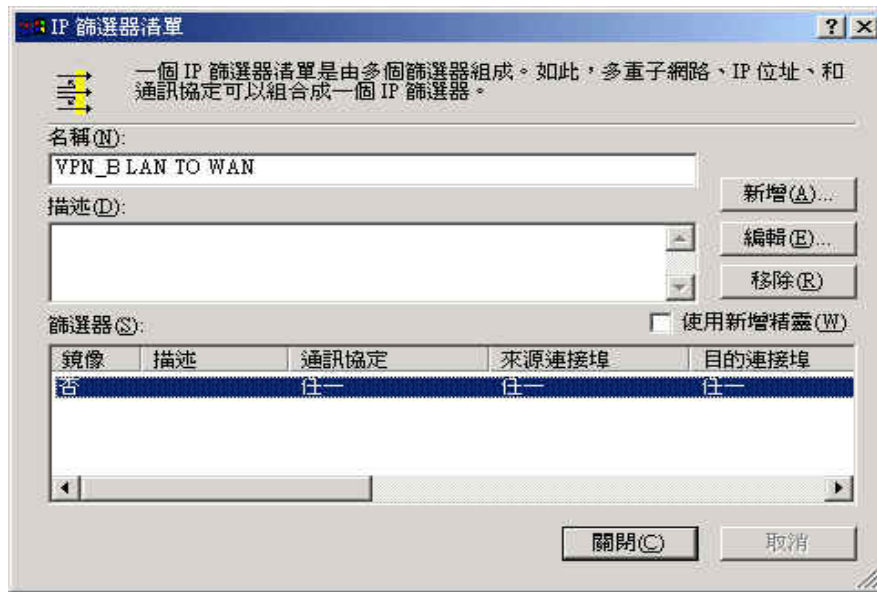


圖 11-82 完成 IP 篩選器清單設定

步驟33. 於【新增規則內容】的【篩選器動作】視窗中，選擇【需要安全性】功能，並按下【編輯】鈕。(如圖 11-83)

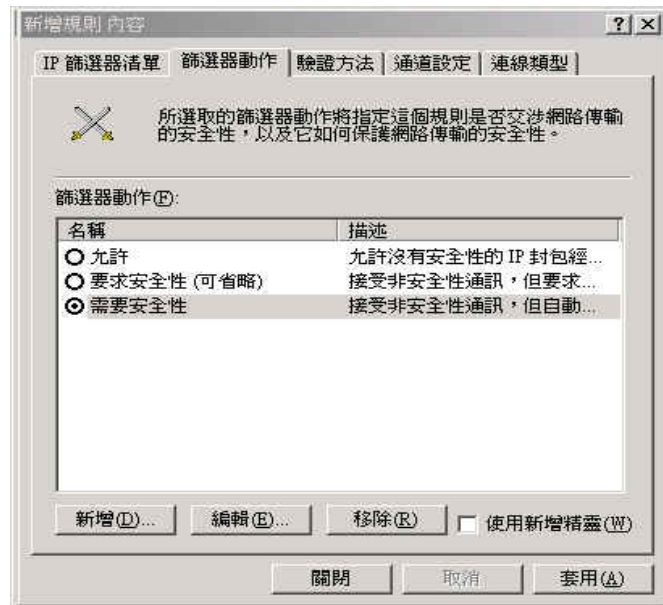


圖 11-83 篩選器動作視窗

步驟34. 於【需要安全性內容】視窗中，勾選【工作階段辨識碼完整轉寄密碼】功能。(如圖 11-84)

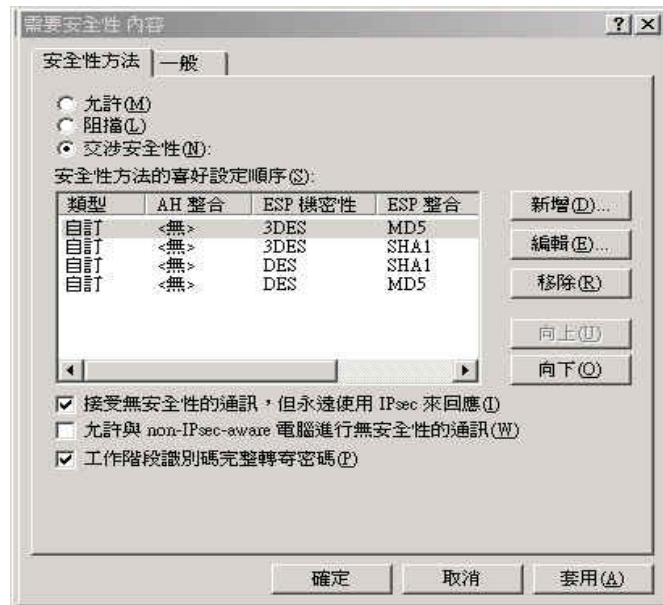


圖 11-84 選擇工作階段辨識碼完整轉寄密碼功能

步驟35. 請選擇 自定 / 無 / 3DES / MD5 安全性方法，並按下【編輯】鈕。(如
圖 11-85)

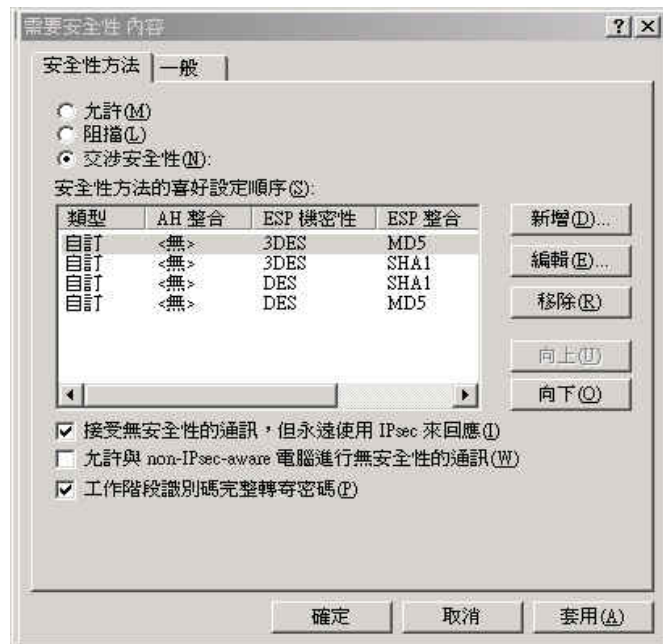


圖 11-85 設定安全性方法

步驟36. 點選【自訂(提供給專業使用者)】選項，並按下【設定】鈕。(如圖 11-86)

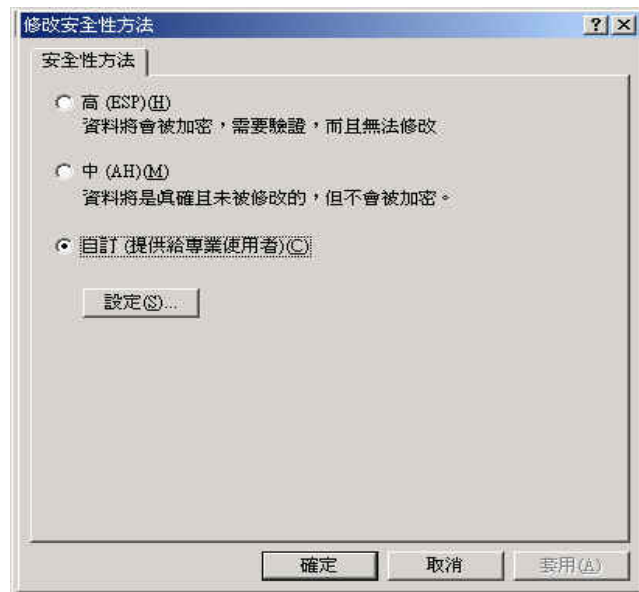


圖 11-86 自訂安全性方法

步驟37. 請勾取【資料完整性及加密(ESP)】，分別選擇【整合演算法】為 MD5 和【加密演算法】為 3DES，勾選【產生新金鑰間隔】，並輸入 28800 秒。然後按 3 次【確定】回到【新增規則內容】視窗。(如圖 11-87)

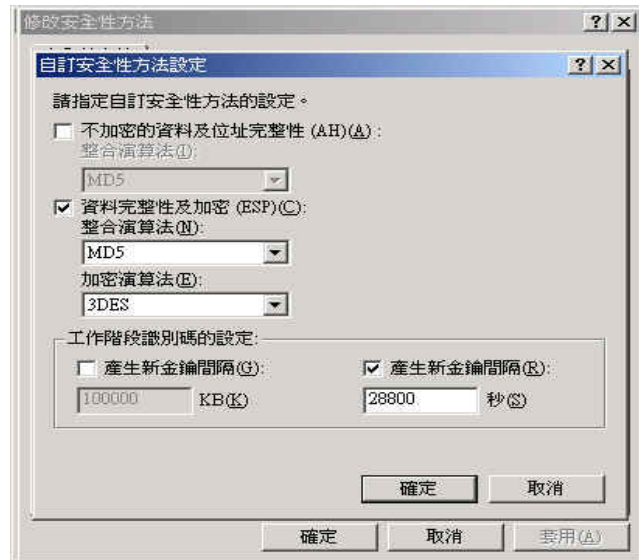


圖 11-87 完成自訂安全性方法設定

步驟38. 於【新增規則內容】的【連線類型】視窗中，選擇【所有網路連線】。(如圖 11-88)

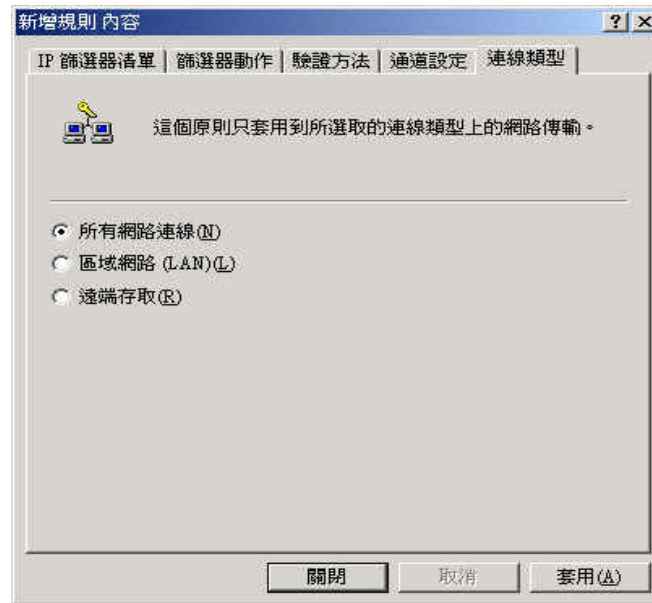


圖 11-88 設定連線類型

步驟39. 於【新增規則內容】的【通道設定】視窗中，選擇【由這個 IP 位址來指定通道的結束點】，並輸入乙公司 WAN 的 IP 位址 211.22.22.22。
(如圖 11-89)

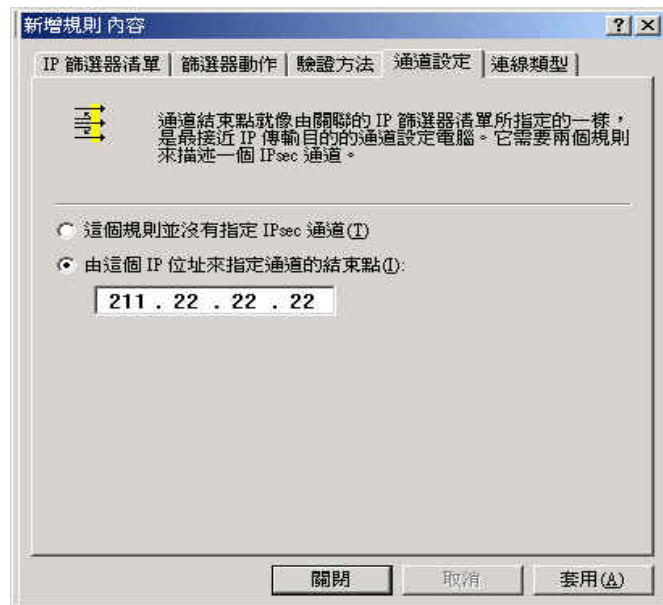


圖 11-89 通道設定視窗

步驟40. 於【新增規則內容】的【驗證方法】視窗中，按下【編輯】鈕。(如圖 11-90)

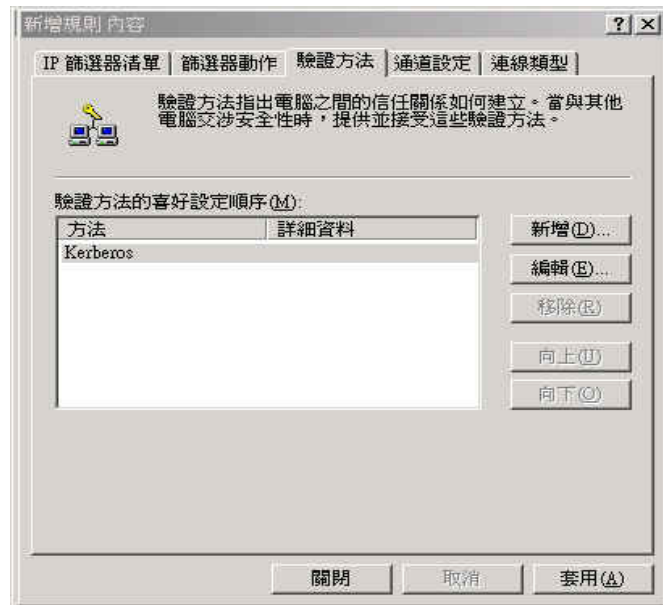


圖 11-90 驗證方法視窗

步驟41. 點選【使用這個字串來保護金鑰間的交換】選項，並輸入雙方所要連線的金鑰 123456789。(如圖11-91)

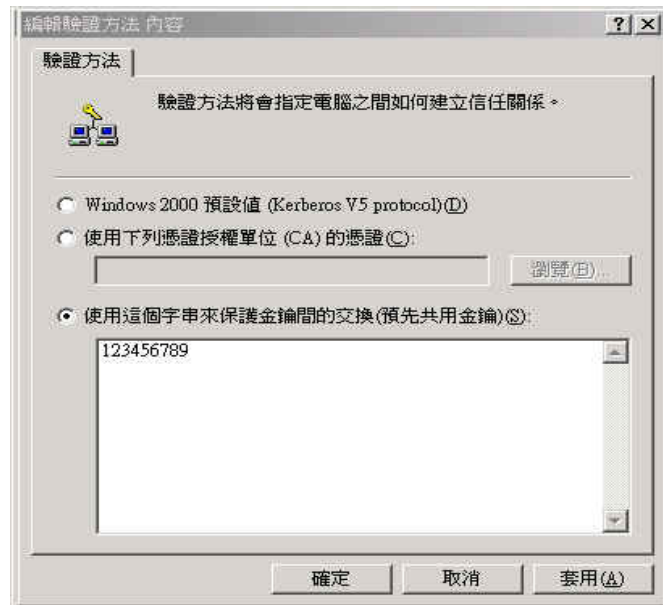


圖 11-91 設定 VPN 連線金鑰

步驟42. 【套用】設定，並關閉設定視窗。(如圖 11-92)

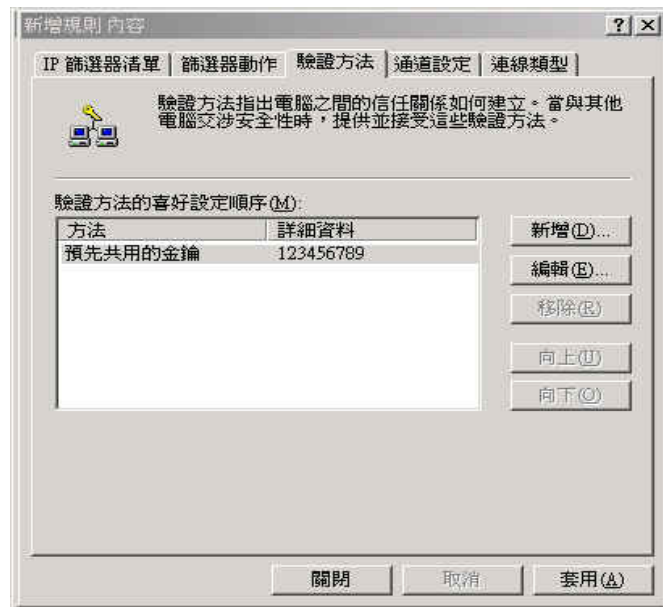


圖 11-92 完成新規則設定

步驟43. 完成 VPN_B LAN TO WAN 規則所有設定。(如圖 11-93)

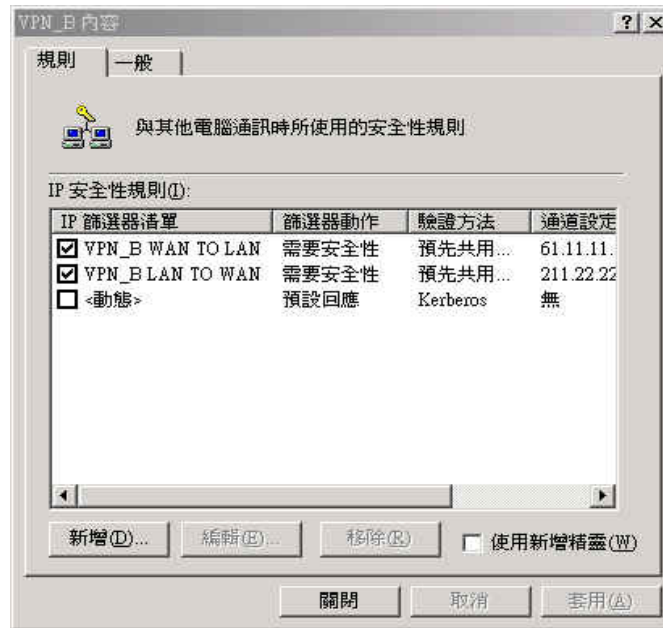


圖 11-93 完成 VPN_B LAN TO WAN 規則設定

步驟44. 於【VPN_B 內容】的【一般】視窗中，按下【進階】鈕。(如圖11-94)



圖 11-94 VPN_B 內容之一般內容視窗

步驟45. 於勾選【主要金鑰完整轉寄密碼】後，按下【方法】鈕。(如圖11-95)



圖 11-95 金鑰交換設定視窗

步驟46. 請選擇將 IKE / 3DES / MD5 / 中(2)安全性方法移至最上方，並按下【確定】鈕。(如圖 11-96)

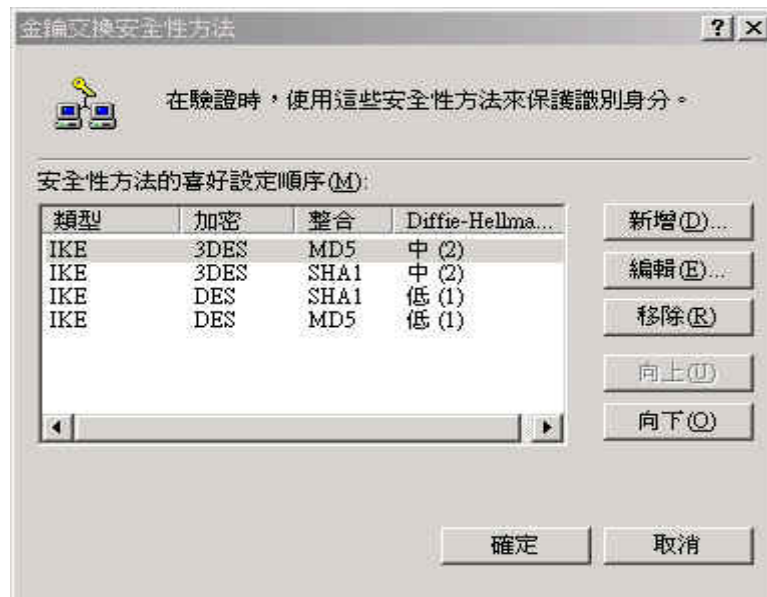


圖 11-96 調整安全性方法順序

步驟47. 完成乙公司 Windows 2000 VPN 所有設定。(如圖11-97)

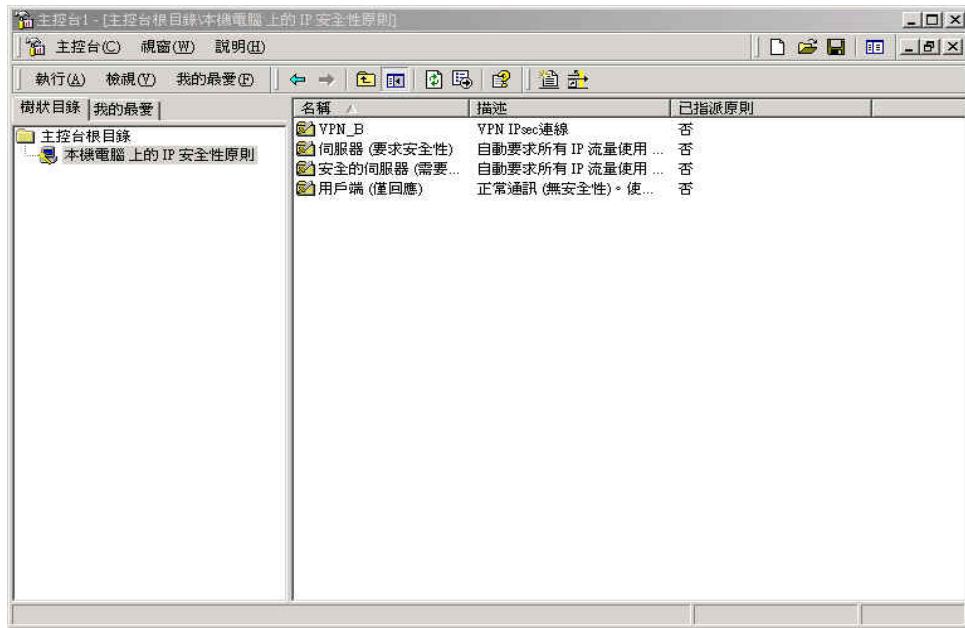


圖 11-97 完成 Windows 2000 IPsec VPN 設定

步驟48. 請在 VPN_B 上點選滑鼠右鍵，選擇將 VPN_B 指派啟動。(如圖11-98)

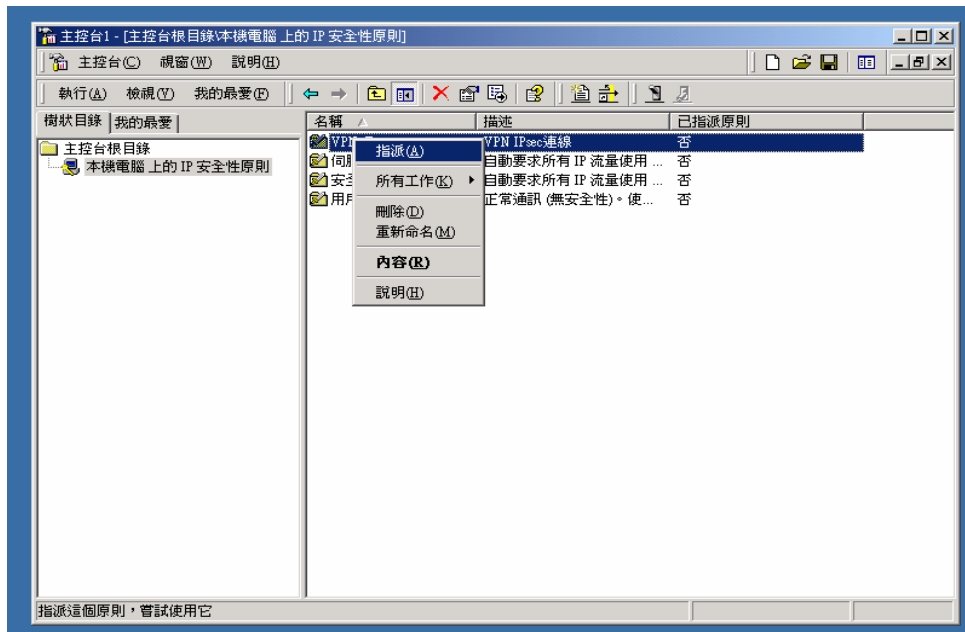


圖 11-98 啟動 VPN_B 安全性規則

步驟49. 我們需要重新啓動 IPsec 服務，請由【開始】選單，選擇【設定】選項，再選擇進入【控制台】。(如圖 11-99)

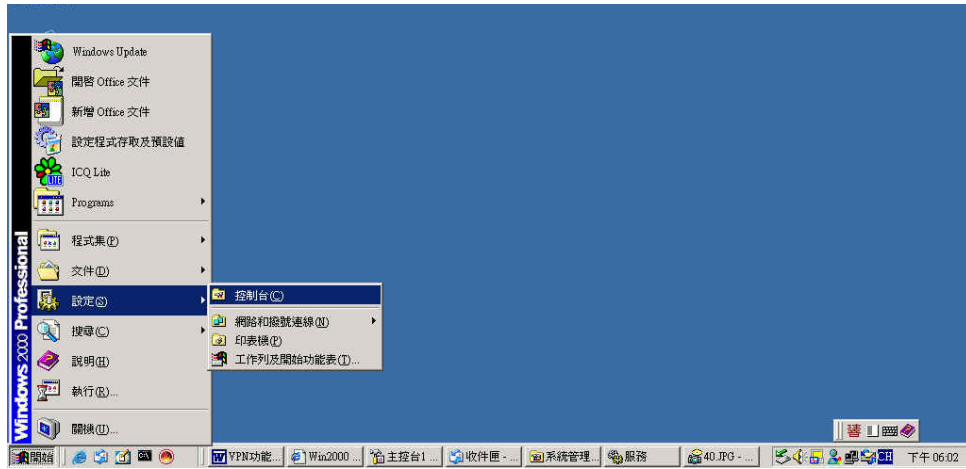


圖 11-99 進入控制台

步驟50. 於【控制台】視窗中，請選擇進入【系統管理工具】。(如圖11-100)

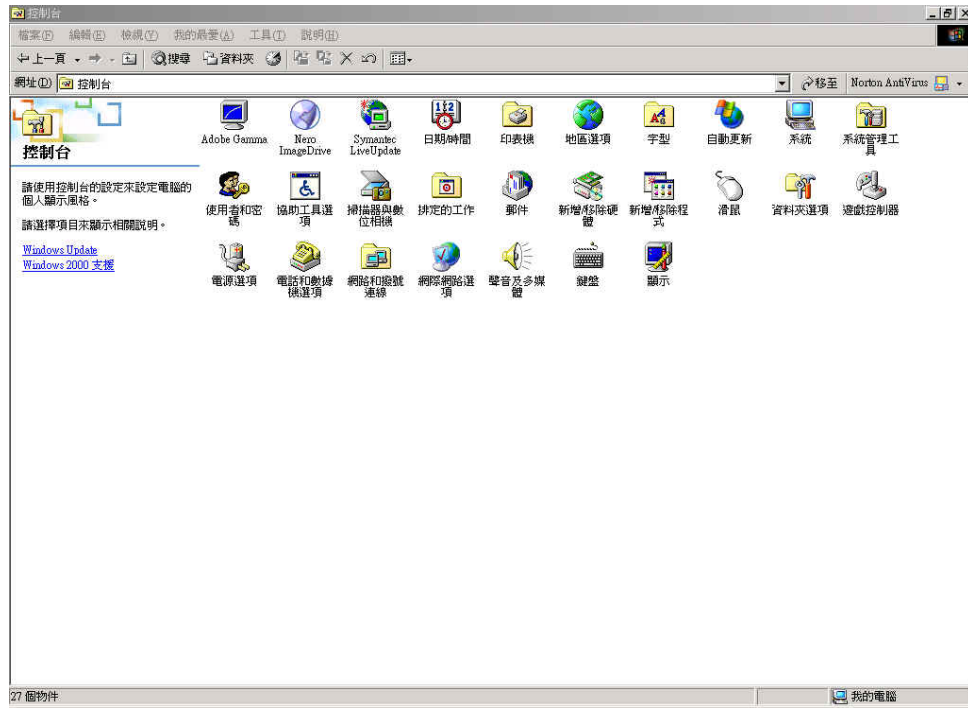


圖 11-100 進入系統管理工具

步驟51. 於【系統管理工具】視窗中，請選擇進入【服務】選項。(如圖11-101)

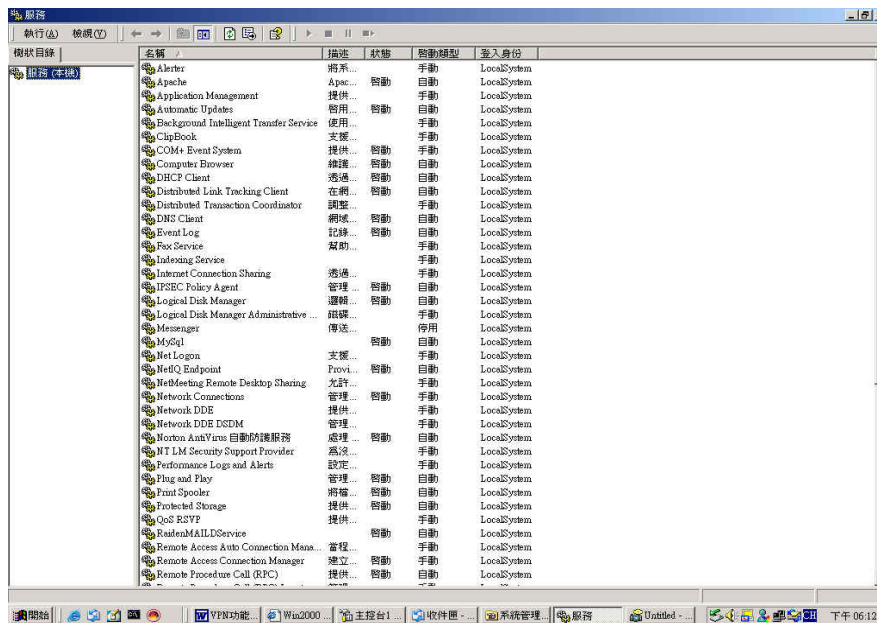


圖 11-101 進入服務選項

步驟52. 於【服務】視窗中，請重新啟動【IPsec Policy Agent】服務。(如圖 11-102)

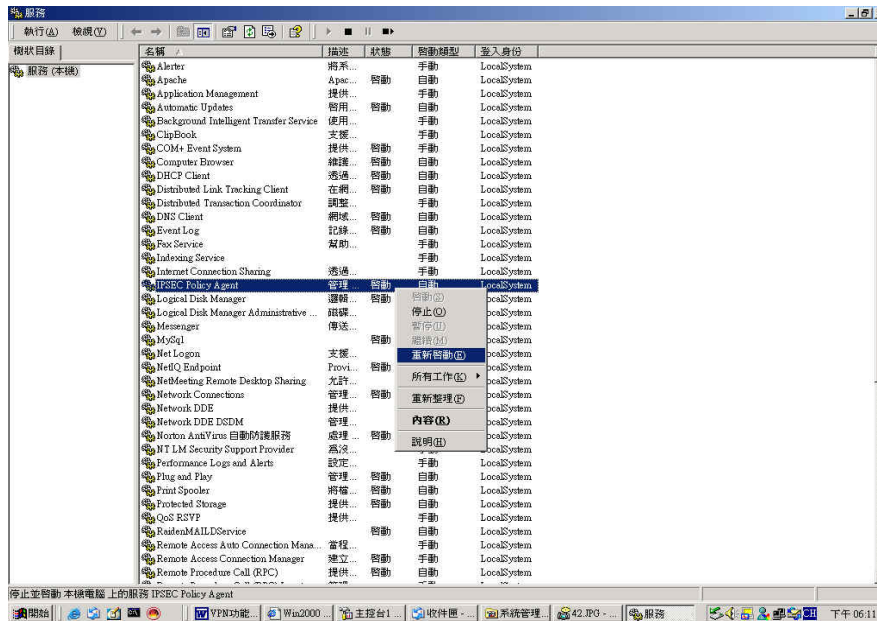


圖 11-102 重新啟動 IPsec Policy Agent

步驟53. 完成所有設定。(如圖11-103)

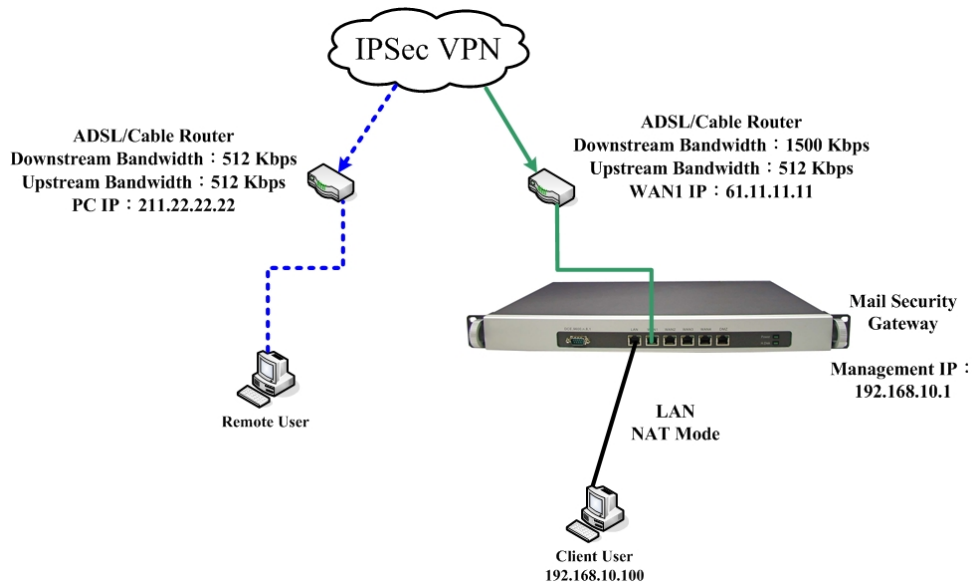


圖 11-103 NUS-MS3000 和 Windows 2000 建立 IPSec VPN 連線之架設環境

使用兩台 NUS-MS3000 設定 IPSec VPN 連線的方法

(連線使用 **Aggressive mode** 演算法)

先前作業

甲公司 WAN IP 為 61.11.11.11
LAN IP 為 192.168.10.X
乙公司 WAN IP 為 211.22.22.22
LAN IP 為 192.168.20.X

本範例以兩台 NUS-MS3000 作為平台操作。假設甲公司 **192.168.10.100** 要向乙公司 **192.168.20.100** 做【虛擬私有網路】連線並下載其分享檔案。(連線使用 **Aggressive mode** 演算法)

甲公司的預設閘道為 NUS-MS3000 的 LAN IP 192.168.10.1，以下為其設定步驟：

- 步驟1. 進入甲公司 NUS-MS3000 預設位址 192.168.10.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-104)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
<input type="button" value="新增"/>					

圖 11-104 IPSec Autokey 視窗

步驟2. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_A，並選擇甲公司用來建立 VPN 連線的【外部網路介面】位址 WAN1。 (如圖 11-105)

需填項目	
名稱	VPN_A
外部網路介面	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-105 IPSec VPN 連線名稱和使用的網路介面設定表單

步驟3. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線乙公司的遠端 IP 位址。 (如圖 11-106)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	211.22.22.22
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-106 IPSec 到目的位址設定表單

步驟4. 於【認證方法】表單中，選擇 Preshare，並填入連線時的【加密金鑰】(加密金鑰最高可輸入 100 位元)。 (如圖 11-107)

認證方法	Preshare
本地PEM	Null
遠端PEM	Null
加密金鑰	123456789

圖 11-107 IPSec 認證方法設定表單

- 步驟5. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 SHA1 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 2 來進行連線。(如圖 11-108)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	SHA1
群組	GROUP 2

圖 11-108 IPSec 加密或認證設定表單

- 步驟6. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:
 【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-109)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-109 IPSec 演算法設定表單

步驟7. 【進階加密】(NO-PFS/ GROUP 1,2,5) 選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒。(如圖 11-110)

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒

圖 11-110 IPSec 進階加密設定表單

步驟8. 【使用模式】選擇 Aggressive mode 演算法(請參閱名詞解說)。本地 / 遠端 ID 可選擇不輸入。本地 / 遠端 ID 如要輸入的話雙方需輸入不相同的 IP 位址，例如：11.11.11.11、22.22.22.22。如要輸入數字或字母來提供驗證前端需加 @，例如：@123a、@abcd1。(如圖 11-111)

使用模式	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
本地ID	11.11.11.11
遠端ID	@abc123

圖 11-111 IPSec Aggressive mode 設定表單

步驟9. 完成 IPSec Autokey 設定。(如圖 11-112)

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-112 IPSec Autokey 設定完成畫面

步驟10. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖11-113)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（乙公司）內部網路位址 192.168.20.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 VPN_A 之 IPSec VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖11-114)

新增Trunk	
名稱	IPSec_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.10.0 / 255.255.255.0
到目的位址	<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩
	192.168.20.0 / 255.255.255.0
	<input type="radio"/> 遠端用戶端
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> VPN_A </div> <div style="text-align: center;"> <input type="button" value="刪除"/> <input type="button" value="新增"/> </div> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> VPN_A </div> </div>
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-113 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的子網路	通道	變更
	IPSec_VPN_Tr..	192.168.10.0	192.168.20.0	VPN_A	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-114 完成新增 VPN Trunk 設定畫面

步驟11. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-115)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-116)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-115 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-116 完成 VPN Trunk 內部至外部管制條例的設定

步驟12. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-117)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-118)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-117 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-118 完成 VPN Trunk 外部至內部管制條例的設定

乙公司的預設閘道為 NUS-MS3000 的 LAN IP 192.168.20.1，以下為其設定步驟：

- 步驟1. 進入乙公司 NUS-MS3000 預設位址 192.168.20.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-119)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
新增					

圖 11-119 IPSec Autokey 視窗

- 步驟2. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_B，並選擇乙公司用來建立 VPN 連線的【外部網路介面】位址 WAN1。(如圖 11-120)

需填項目	
名稱	VPN_B
外部網路介面	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-120 IPSec VPN 連線名稱和使用的外網路介面設定表單

步驟3. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線甲公司的遠端 IP 位址。(如圖 11-121)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	61.11.11.11
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-121 IPSec 到目的位址設定表單

步驟4. 於【認證方法】表單中，選擇 Preshare，並填入連線時的【加密金鑰】(加密金鑰最高可輸入 100 位元)。(如圖 11-122)

認證方法	Preshare
本地PEM	Null
遠端PEM	Null
加密金鑰	123456789

圖 11-122 IPSec 認證方法設定表單

步驟5. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 SHA1 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 2 來進行連線。(如圖 11-123)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	SHA1
群組	GROUP 2

圖 11-123 IPSec 加密或認證設定表單

步驟6. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:

【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-124)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-124 IPSec 演算法設定表單

步驟7. 【進階加密】(NO-PFS/ GROUP 1,2,5) 選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒。(如圖 11-125)

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒

圖 11-125 IPSec 進階加密設定表單

步驟8. 【使用模式】選擇 Aggressive mode 演算法(請參閱名詞解說)。本地 / 遠端 ID 可選擇不輸入。本地 / 遠端 ID 如要輸入的話雙方需輸入不相同的 IP 位址，例如：11.11.11.11、22.22.22.22。如要輸入數字或字母來提供驗證前端需加 @，例如：@123a、@abcd1。(如圖 11-126)

使用模式	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
本地ID	@abc123
遠端ID	11.11.11.11

圖 11-126 IPSec Aggressive mode 設定表單

步驟9. 完成 IPSec Autokey 設定。(如圖 11-127)

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-127 IPSec Autokey 設定完成畫面

步驟10. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-128)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（乙公司）內部網路位址 192.168.20.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 VPN_B 之 IPSec VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-129)

新增Trunk	
名稱	IPSec_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.20.0 / 255.255.255.0
到目的位址	<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩
	192.168.10.0 / 255.255.255.0
	<input type="radio"/> 遠端用戶端
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> VPN_B </div> <div style="text-align: center;"> <input type="button" value="刪除"/> <input type="button" value="新增"/> </div> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> VPN_B </div> </div>
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-128 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	IPSec_VPN_Tr..	192.168.20.0	192.168.10.0	VPN_B	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-129 完成新增 VPN Trunk 設定畫面

步驟11. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-130)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-131)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-130 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-131 完成 VPN Trunk 內部至外部管制條例的設定

步驟12. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-132)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-133)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-132 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-133 完成 VPN Trunk 外部至內部管制條例的設定

步驟13. 完成 IPsec VPN Aggressive mode 連線 (如圖 11-134)

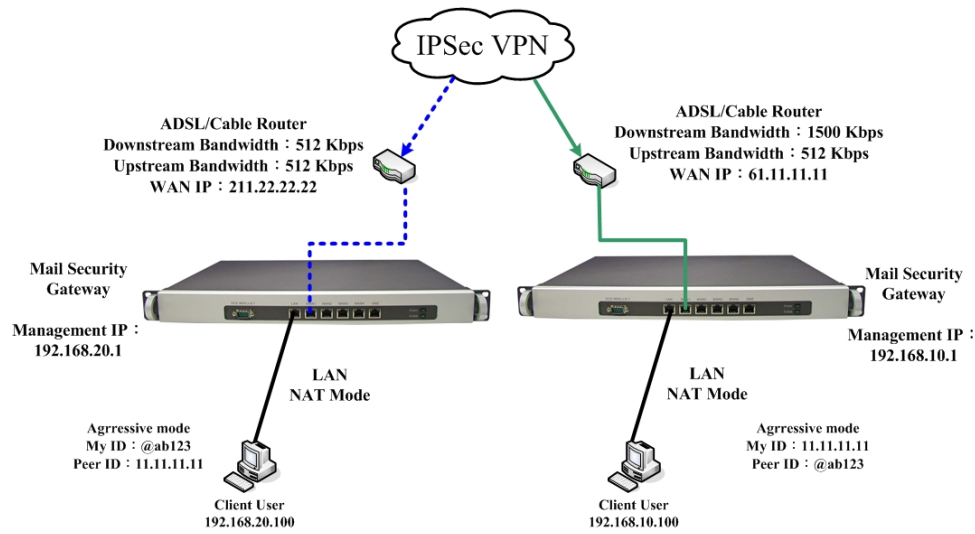


圖 11-134 IPsec VPN 連線 Aggressive mode 之架設環境

使用兩台 NUS-MS3000 設定 IPsec VPN 的 OutBound Load Balance 連線方法

(連線使用 **RSA-SIG** 認證方法和 **GRE/IPsec** 封包封裝演算法)

先前作業

甲公司 WAN1 IP 為 61.11.11.11
WAN2 IP 為 61.22.22.22
LAN IP 為 192.168.10.X
乙公司 WAN1 IP 為 211.22.22.22
WAN2 IP 為 211.33.33.33
LAN IP 為 192.168.20.X

甲公司和乙公司分別向不同的 CA Server 各申請簽署了兩份本地證書。

甲公司 WAN1 和乙公司 WAN1 建立 IPsec VPN 連線。

甲公司 WAN2 和乙公司 WAN2 建立 IPsec VPN 連線。

本範例以兩台 NUS-MS3000 作為平台操作。假設甲公司 **192.168.10.100** 要向乙公司 **192.168.20.100** 做【虛擬私有網路】連線並下載其分享檔案。(連線使用 **GRE/IPsec** 封包封裝演算法)

甲公司的預設閘道為 NUS-MS3000 的 LAN IP 192.168.10.1，以下為其設定步驟：

步驟1. 於【VPN】之【本地證書】功能中，新增、設定並匯入下列資料：

- 按下【新增】按鈕。(如圖 11-135)
- 【名稱】設為 Site_A_01。
- 【主旨】設為 VPN_01。
- 【國家】選擇 Taiwan。
- 【州/省】設為 Taiwan。
- 【地區(城市)】設為 Taipei。
- 【公司】設為 Nusoft。
- 【單位】設為 Support。
- 【電子郵件】設為 support@nusoft.com.tw。
- 【金鑰長度】選擇 2048。
- 按下【確定】鈕。(如圖 11-136)
- 於【下載】鈕上按下滑鼠右鍵，選擇【另存目標】和儲存資料夾，將本地自行設定並產生的 CSR (Certificate Signing Request)，下載回 PC 並至 CA Server (CA_Server_01) 進行簽署的動作。(如圖 11-137)
- 按下【匯入】鈕，進入【上傳證書】視窗，將本地經由 CA Server 簽署後取回之證書 (.pem 檔) 存放路徑填入【上傳本地證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。(如圖 11-138, 11-139)
- 再按下【新增】按鈕。(如圖 11-140)
- 【名稱】設為 Site_A_02。
- 【主旨】設為 VPN_02。
- 【國家】選擇 Taiwan。
- 【州/省】設為 Taiwan。

- 【地區（城市）】設為 Taipei。
- 【公司】設為 Nusoft。
- 【單位】設為 Sales。
- 【電子郵件】設為 sales@nusoft.com.tw。
- 【金鑰長度】選擇 2048。
- 按下【確定】鈕。(如圖 11-141)
- 於【下載】鈕上按下滑鼠右鍵，選擇【另存目標】和儲存資料夾，將本地自行設定並產生的 CSR（Certificate Signing Request），下載回 PC 並至 CA Server（CA_Server_01）進行簽署的動作。(如圖 11-142)
- 按下【匯入】鈕，進入【上傳證書】視窗，將本地經由 CA Server 簽署後取回之證書（.pem 檔）存放路徑填入【上傳本地證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。(如圖 11-143, 圖 11-144)
- 將乙公司所有經由 CA Server 簽署後取回之證書（.pem 檔），匯入 NUS-MS3000。(如圖 11-145, 圖 11-146, 圖 11-147, 圖 11-148)

新增 CSR	
名稱	Site_A_01
主旨	VPN_01
國家	Taiwan
州 / 省	Taiwan
地區 (城市)	Taipei
公司	Nusoft
單位	Support
電子郵件	support@nusoft.com.tw
金鑰長度	2048
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-135 新增第一筆 CSR 設定畫面



圖 11-136 第一筆 CSR 新增完成畫面

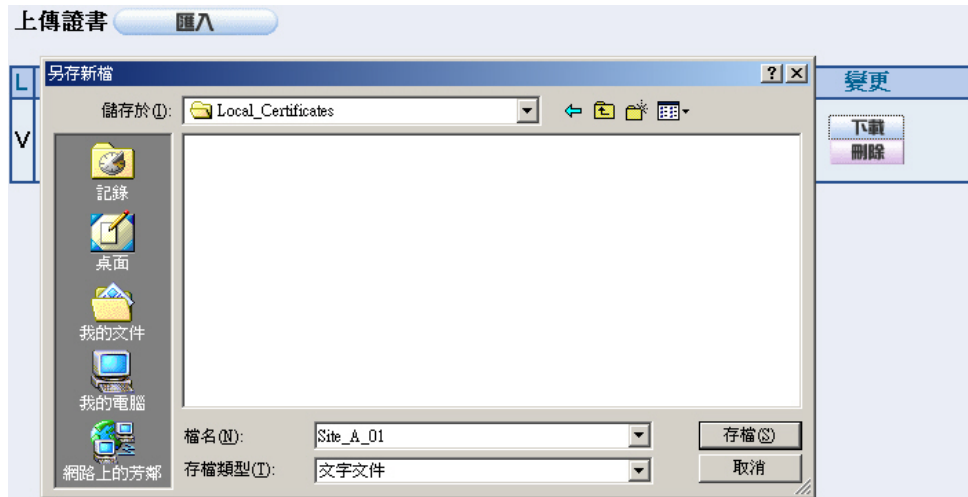


圖 11-137 下載第一筆 CSR 檔案畫面



圖 11-138 上傳第一筆本地證書畫面



圖 11-139 第一筆本地證書上傳完成畫面

新增 CSR	
名稱	Site_A_02
主旨	VPN_02
國家	Taiwan
州 / 省	Taiwan
地區 (城市)	Taipei
公司	Nusoft
單位	Sales
電子郵件	sales@nusoft.com.tw
金鑰長度	2048
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-140 新增第二筆 CSR 設定畫面

上傳證書

L	名稱	主旨	變更
V	Site_A_01	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
V	Site_A_02	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.tw	<input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-141 第二筆 CSR 新增完成畫面

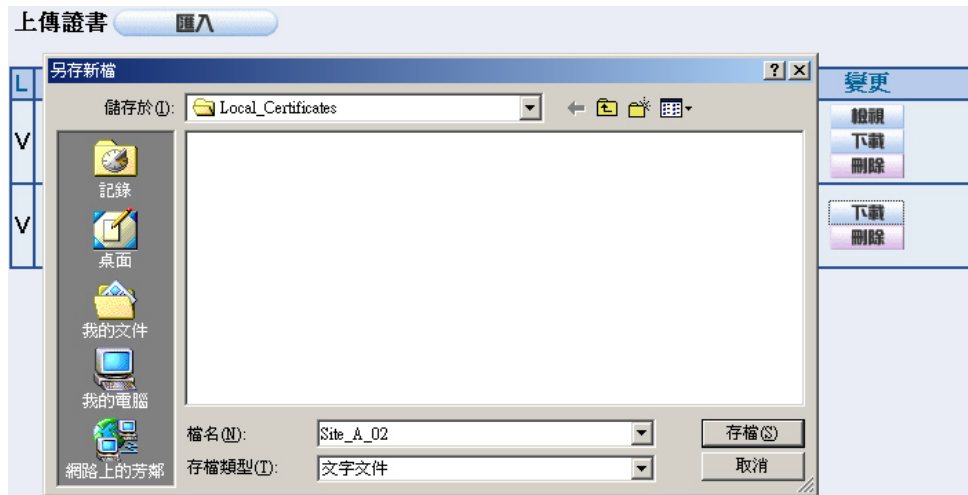


圖 11-142 下載第二筆 CSR 檔案畫面



圖 11-143 上傳第二筆本地證書畫面



圖 11-144 第二筆本地證書上傳完成畫面



圖 11-145 上傳第一筆乙公司證書畫面

上傳證書

L	名稱	主旨	變更
V	Site_A_01	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
V	Site_A_02	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-146 第一筆乙公司證書上傳完成畫面

上傳證書

上傳本地證書

圖 11-147 上傳第二筆乙公司證書畫面

上傳證書

L	名稱	主旨	變更
V	Site_A_01	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
V	Site_A_02	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
	Site_B_02	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-148 第二筆乙公司證書上傳完成畫面

步驟2. 於【VPN】之【CA 證書】功能中，匯入下列資料：

- 按下【匯入】鈕，進入【上傳證書】視窗，將本地 CSR（Certificate Signing Request）申請簽署的 CA Server 證書（CA_Server_01.pem 檔）存放路徑填入【上傳 CA 證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。（如圖 11-149、圖 11-150）
- 按下【匯入】鈕，進入【上傳證書】視窗，將乙公司 CSR（Certificate Signing Request）申請簽署的 CA Server 證書（CA_Server_02.pem 檔）存放路徑填入【上傳 CA 證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。（如圖 11-151、圖 11-152）

圖 11-149 上傳本地 CSR 申請簽署的 CA Server 證書畫面

名稱	主旨	變更
CA_Server_01	C=TW/ST=Taiwan/L=PH/O=Nusoft/OU=Certificate Authority /CN=Home	檢視 下載 刪除

圖 11-150 本地 CSR 申請簽署的 CA Server 證書上傳完成畫面

圖 11-151 上傳乙公司 CSR 申請簽署的 CA Server 證書畫面

上傳證書

名稱	主旨	變更
CA_Server_01	C=TW/ST=Taiwan/L=PH/O=Nusoft/OU=Certificate Authority /CN=Home	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
CA_Server_02	C=TW/ST=Some-State/L=City/O=Company/OU=Section /CN=Name /emailAddress=E-Mail	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-152 乙公司 CSR 申請簽署的 CA Server 證書上傳完成畫面

步驟3. 進入甲公司 NUS-MS3000 預設位址 192.168.10.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-153)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
新增					

圖 11-153 IPSec Autokey 視窗

步驟4. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_01，並選擇甲公司用來建立 VPN 連線的【外部網路介面】位址 WAN1。(如圖 11-154)

需填項目	
名稱	VPN_01
外部網路介面	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-154 IPSec VPN 連線名稱和使用的網路介面設定表單

步驟5. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線乙公司的遠端 (WAN1) IP 位址。(如圖 11-155)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	211.22.22.22
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-155 IPSec 到目的位址設定表單

步驟6. 於【認證方法】表單中，選擇 RSA-SIG，【本地 PEM】選擇 Site_A_01，【遠端 PEM】選擇 Site_B_01。(如圖 11-156)

認證方法	RSA-SIG
本地PEM	Site_A_01
遠端PEM	Site_B_01
加密金鑰	

圖 11-156 IPSec 認證方法設定表單

- 步驟7. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 MD5 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 1 來進行連線。(如圖 11-157)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	MD5
群組	GROUP 1

圖 11-157 IPSec 加密或認證設定表單

- 步驟8. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:
 【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-158)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-158 IPSec 演算法設定表單

步驟9. 【進階加密】(NO-PFS/ GROUP 1,2,5) 選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒，【使用模式】選擇 Main mode。(如圖 11-159)

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒
使用模式	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

圖 11-159 IPSec 進階加密設定表單

步驟10. 於【GRE/IPSec】功能中，輸入【GRE 來源端 IP/遮罩】192.168.50.100，【GRE 遠端 IP】192.168.50.200（此來源端 IP 和遠端 IP 需為同一 C Class 區段，需自行設定）。(如圖 11-160)

GRE/IPSec	
GRE 來源端 IP	192.168.50.100
GRE 遠端 IP	192.168.50.200

圖 11-160 GRE/IPSec 設定表單

步驟11. 完成【IPSec Autokey】VPN_01 設定。(如圖 11-161)

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_01	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-161 IPSec Autokey 設定完成畫面

步驟12. 進入甲公司 NUS-MS3000 預設位址 192.168.10.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-162)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
--	VPN_01	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-162 IPSec Autokey 視窗

步驟13. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_02，並選擇甲公司用來建立 VPN 連線的【外部網路介面】位址 WAN2。(如圖 11-163)

需填項目	
名稱	<input type="text" value="VPN_02"/>
外部網路介面	<input checked="" type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-163 IPSec VPN 連線名稱和使用的外網路介面設定表單

步驟14. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線乙公司的遠端 (WAN2) IP 位址。(如圖 11-164)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	<input type="text" value="211.33.33.33"/>
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-164 IPSec 到目的位址設定表單

步驟15. 於【認證方法】表單中，選擇 RSA-SIG，【本地 PEM】選擇 Site_A_02，【遠端 PEM】選擇 Site_B_02。(如圖 11-165)

認證方法	<input type="text" value="RSA-SIG"/>
本地PEM	<input type="text" value="Site_A_02"/>
遠端PEM	<input type="text" value="Site_B_02"/>
加密金鑰	<input type="text"/>

圖 11-165 IPSec 認證方法設定表單

步驟16. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 MD5 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 1 來進行連線。(如圖 11-166)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	MD5
群組	GROUP 1

圖 11-166 IPSec 加密或認證設定表單

步驟17. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:

【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-167)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-167 IPSec 演算法設定表單

步驟18. 【進階加密】（NO-PFS/ GROUP 1,2,5）選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒，【使用模式】選擇 Main mode。（如圖 11-168）

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒
使用模式	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

圖 11-168 IPSec 進階加密設定表單

步驟19. 於【GRE/IPSec】功能中，輸入【GRE 來源端 IP/遮罩】192.168.60.100，【GRE 遠端 IP】192.168.60.200（此來源端 IP 和遠端 IP 需為同一 C Class 區段，需自行設定）。（如圖 11-169）

GRE/IPSec	
GRE 來源端 IP	192.168.60.100
GRE 遠端 IP	192.168.60.200

圖 11-169 GRE/IPSec 設定表單

步驟20. 完成【IPSec Autokey】VPN_02 設定。（如圖 11-170）

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_01	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>
--	VPN_02	WAN2	211.33.33.33	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-170 IPSec Autokey 設定完成畫面

步驟21. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-171)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（乙公司）內部網路位址 192.168.20.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 VPN_01 和 VPN_02 之 IPSec VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-172)

新增Trunk	
名稱	IPSec_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.10.0 / 255.255.255.0
到目的位址	<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩
	192.168.20.0 / 255.255.255.0
	<input type="radio"/> 遠端用戶端
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> VPN_01 VPN_02 </div> <div style="text-align: center;"> <input type="button" value="刪除"/> <input type="button" value="新增"/> </div> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> VPN_01 VPN_02 </div> </div>
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-171 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	IPSec_VPN_Tr..	192.168.10.0	192.168.20.0	VPN_01, ...	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-172 完成新增 VPN Trunk 設定畫面

步驟22. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-173)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-174)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路介面 <input type="checkbox"/> 拒絕,所有外部網路介面 <input type="checkbox"/> 外部網路介面1 <input type="checkbox"/> 外部網路介面2 <input type="checkbox"/> 外部網路介面3 <input type="checkbox"/> 外部網路介面4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-173 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-174 完成 VPN Trunk 內部至外部管制條例的設定

步驟23. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-175)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-176)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-175 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-176 完成 VPN Trunk 外部至內部管制條例的設定

乙公司的預設閘道為 NUS-MS3000 的 LAN IP 192.168.20.1，以下為其設定步驟：

步驟1. 於【VPN】之【本地證書】功能中，新增、設定並匯入下列資料：

- 按下【新增】按鈕。(如圖 11-177)
- 【名稱】設為 Site_B_01。
- 【主旨】設為 VPN_01。
- 【國家】選擇 Great Britain (UK)。
- 【州/省】設為 Great Britain。
- 【地區(城市)】設為 London。
- 【公司】設為 Nusoft_Branch_Office。
- 【單位】設為 Support。
- 【電子郵件】設為 support@nusoft.com.uk。
- 【金鑰長度】選擇 2048。
- 按下【確定】鈕。(如圖 11-178)
- 於【下載】鈕上按下滑鼠右鍵，選擇【另存目標】和儲存資料夾，將本地自行設定並產生的 CSR (Certificate Signing Request)，下載回 PC 並至 CA Server (CA_Server_02) 進行簽署的動作。(如圖 11-179)
- 按下【匯入】鈕，進入【上傳證書】視窗，將本地經由 CA Server 簽署後取回之證書 (.pem 檔) 存放路徑填入【上傳本地證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。(如圖 11-180, 11-181)
- 再按下【新增】按鈕。(如圖 11-182)
- 【名稱】設為 Site_B_02。
- 【主旨】設為 VPN_02。

- 【國家】選擇 Great Britain (UK)。
- 【州/省】設為 Great Britain。
- 【地區（城市）】設為 London。
- 【公司】設為 Nusoft_Branch_Office。
- 【單位】設為 Sales。
- 【電子郵件】設為 sales@nusoft.com.uk。
- 【金鑰長度】選擇 2048。
- 按下【確定】鈕。(如圖 11-183)
- 於【下載】鈕上按下滑鼠右鍵，選擇【另存目標】和儲存資料夾，將本地自行設定並產生的 CSR (Certificate Signing Request)，下載回 PC 並至 CA Server (CA_Server_02) 進行簽署的動作。(如圖 11-184)
- 按下【匯入】鈕，進入【上傳證書】視窗，將本地經由 CA Server 簽署後取回之證書 (.pem 檔) 存放路徑填入【上傳本地證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。(如圖 11-185, 圖 11-186)
- 將甲公司所有經由 CA Server 簽署後取回之證書 (.pem 檔)，匯入 NUS-MS3000。(如圖 11-187, 圖 11-188, 圖 11-189, 圖 11-190)

新增 CSR	
名稱	Site_B_01
主旨	VPN_01
國家	Great Britain (UK)
州 / 省	Great Britain
地區 (城市)	London
公司	Nusoft_Branch_Office
單位	Support
電子郵件	support@nusoft.com.uk
金鑰長度	2048

圖 11-177 新增第一筆 CSR 設定畫面

上傳證書

L	名稱	主旨	變更
V	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support/CN=VPN_01/emailAddress=support@nusoft.com.uk	<input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-178 第一筆 CSR 新增完成畫面

上傳證書

L	變更
V	<input type="button" value="下載"/> <input type="button" value="刪除"/>

另存新檔

儲存於 (I): Local_Certificates

檔名 (N): Site_B_01
 存檔類型 (T): 文字文件

圖 11-179 下載第一筆 CSR 檔案畫面

上傳證書

上傳本地證書

圖 11-180 上傳第一筆本地證書畫面

上傳證書

L	名稱	主旨	變更
V	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support/CN=VPN_01 /emailAddress=support@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-181 第一筆本地證書上傳完成畫面

新增 CSR

名稱	<input type="text" value="Site_B_02"/>
主旨	<input type="text" value="VPN_02"/>
國家	<input type="text" value="Great Britain (UK)"/>
州 / 省	<input type="text" value="Great Britain"/>
地區 (城市)	<input type="text" value="London"/>
公司	<input type="text" value="Nusoft_Branch_Office"/>
單位	<input type="text" value="Sales"/>
電子郵件	<input type="text" value="sales@nusoft.com.uk"/>
金鑰長度	<input type="text" value="2048"/>

圖 11-182 新增第二筆 CSR 設定畫面

上傳證書

L	名稱	主旨	變更
V	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
V	Site_B_02	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.uk	<input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-183 第二筆 CSR 新增完成畫面

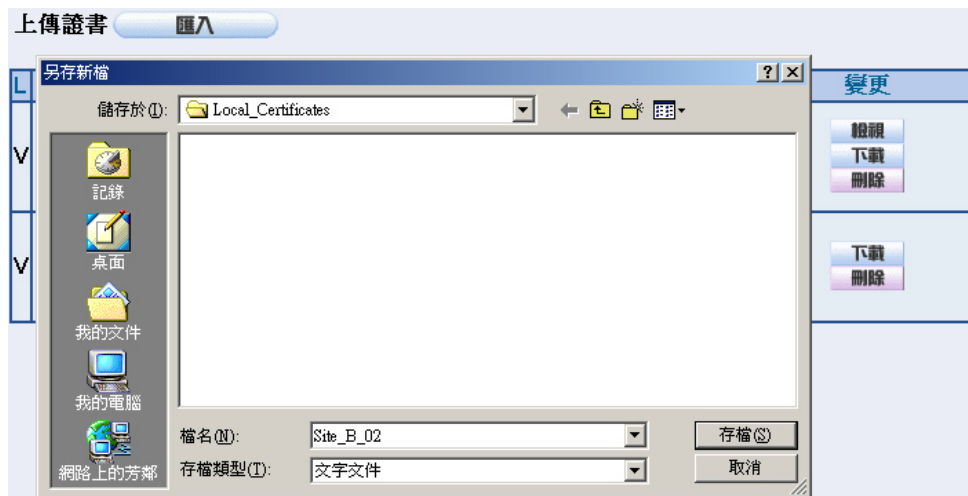


圖 11-184 下載第二筆 CSR 檔案畫面

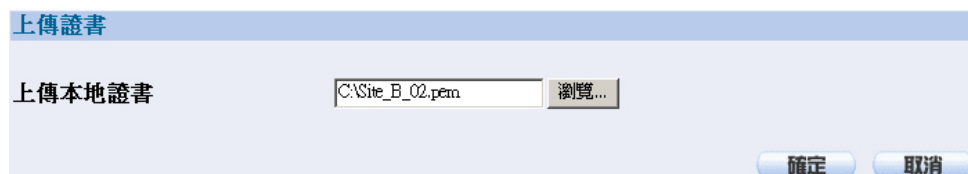


圖 11-185 上傳第二筆本地證書畫面

上傳證書

L	名稱	主旨	變更
V	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
V	Site_B_02	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-186 第二筆本地證書上傳完成畫面

上傳證書

上傳本地證書

圖 11-187 上傳第一筆甲公司證書畫面

上傳證書

L	名稱	主旨	變更
V	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
V	Site_B_02	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
	Site_A_01	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-188 第一筆甲公司證書上傳完成畫面

上傳證書

上傳本地證書

圖 11-189 上傳第二筆甲公司證書畫面

上傳證書

L	名稱	主旨	變更
V	Site_B_01	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
V	Site_B_02	/C=GB/ST=Great Britain/L=London/O=Nusoft_Branch_Office/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.uk	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
	Site_A_01	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Support /CN=VPN_01 /emailAddress=support@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
	Site_A_02	/C=TW/ST=Taiwan/L=Taipei/O=Nusoft/OU=Sales /CN=VPN_02 /emailAddress=sales@nusoft.com.tw	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-190 第二筆甲公司證書上傳完成畫面

步驟2. 於【VPN】之【CA 證書】功能中，匯入下列資料：

- 按下【匯入】鈕，進入【上傳證書】視窗，將本地 CSR（Certificate Signing Request）申請簽署的 CA Server 證書（CA_Server_02.pem 檔）存放路徑填入【上傳 CA 證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。（如圖 11-191、圖 11-192）
- 按下【匯入】鈕，進入【上傳證書】視窗，將甲公司 CSR（Certificate Signing Request）申請簽署的 CA Server 證書（CA_Server_01.pem 檔）存放路徑填入【上傳 CA 證書】欄位，按下【確定】鈕，匯入 NUS-MS3000。（如圖 11-193、圖 11-194）

圖 11-191 上傳本地 CSR 申請簽署的 CA Server 證書畫面

名稱	主旨	變更
CA_Server_02	C=TW/ST=Some-State/L=City/O=Company/OU=Section /CN=Name /emailAddress=E-Mail	檢視 下載 刪除

圖 11-192 本地 CSR 申請簽署的 CA Server 證書上傳完成畫面

圖 11-193 上傳甲公司 CSR 申請簽署的 CA Server 證書畫面

上傳證書

名稱	主旨	變更
CA_Server_02	C=TW/ST=Some-State/L=City/O=Company/OU=Section /CN=Name /emailAddress=E-Mail	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>
CA_Server_01	C=TW/ST=Taiwan/L=PH/O=Nusoft/OU=Certificate Authority /CN=Home	<input type="button" value="檢視"/> <input type="button" value="下載"/> <input type="button" value="刪除"/>

圖 11-194 甲公司 CSR 申請簽署的 CA Server 證書上傳完成畫面

步驟3. 進入乙公司 NUS-MS3000 預設位址 192.168.20.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-195)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
新增					

圖 11-195 IPSec Autokey 視窗

步驟4. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_01，並選擇乙公司用來建立 VPN 連線的【外部網路介面】位址 WAN1。(如圖 11-196)

需填項目	
名稱	VPN_01
外部網路介面	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-196 IPSec VPN 連線名稱和使用的網路介面設定表單

步驟5. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線甲公司的遠端 (WAN1) IP 位址。(如圖 11-197)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	61.11.11.11
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-197 IPSec 到目的位址設定表單

步驟6. 於【認證方法】表單中，選擇 RSA-SIG，【本地 PEM】選擇 Site_B_01，【遠端 PEM】選擇 Site_A_01。(如圖 11-198)

認證方法	RSA-SIG
本地PEM	Site_B_01
遠端PEM	Site_A_01
加密金鑰	

圖 11-198 IPSec 認證方法設定表單

- 步驟7. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 MD5 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 1 來進行連線。(如圖 11-199)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	MD5
群組	GROUP 1

圖 11-199 IPSec 加密或認證設定表單

- 步驟8. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:
 【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-200)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-200 IPSec 演算法設定表單

步驟9. 【進階加密】(NO-PFS/ GROUP 1,2,5) 選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒，【使用模式】選擇 Main mode。(如圖 11-201)

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒
使用模式	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

圖 11-201 IPSec 進階加密設定表單

步驟10. 於【GRE/IPSec】功能中，輸入【GRE 來源端 IP/遮罩】192.168.50.200，【GRE 遠端 IP】192.168.50.100（此來源端 IP 和遠端 IP 需為同一 C Class 區段，需自行設定）。(如圖 11-202)

GRE/IPSec	
GRE 來源端 IP	192.168.50.200
GRE 遠端 IP	192.168.50.100

圖 11-202 GRE/IPSec 設定表單

步驟11. 完成【IPSec Autokey】VPN_01 設定。(如圖 11-203)

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_01	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-203 IPSec Autokey 設定完成畫面

步驟12. 進入乙公司 NUS-MS3000 預設位址 192.168.20.1，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Autokey】次功能選項。並點選【新增】功能。(如圖 11-204)

i	名稱	WAN	閘道 IP 位址	IPSec演算法	變更
--	VPN_01	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-204 IPSec Autokey 視窗

步驟13. 於【IPSec Autokey】表單中，填寫所使用的 VPN 連線【名稱】VPN_02，並選擇乙公司用來建立 VPN 連線的【外部網路介面】位址 WAN2。(如圖 11-205)

需填項目	
名稱	<input type="text" value="VPN_02"/>
外部網路介面	<input checked="" type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4

圖 11-205 IPSec VPN 連線名稱和使用的外網路介面設定表單

步驟14. 於【到目的位址】表單中，選擇遠端閘道-固定 IP，填寫所要連線甲公司的遠端 (WAN2) IP 位址。(如圖 11-206)

到目的位址	
<input checked="" type="radio"/> 遠端閘道 -- 固定 IP	<input type="text" value="61.22.22.22"/>
<input type="radio"/> 遠端閘道或用戶端 -- 動態 IP	

圖 11-206 IPSec 到目的位址設定表單

步驟15. 於【認證方法】表單中，選擇 RSA-SIG，【本地 PEM】選擇 Site_B_02，【遠端 PEM】選擇 Site_A_02。(如圖 11-207)

認證方法	<input type="text" value="RSA-SIG"/>
本地PEM	<input type="text" value="Site_B_02"/>
遠端PEM	<input type="text" value="Site_A_02"/>
加密金鑰	<input type="text"/>

圖 11-207 IPSec 認證方法設定表單

步驟16. 於【加密或認證】表單中，選擇【ISAKMP 演算法】(請參閱名詞解說)，雙方開始進行連線溝通時，選擇建立連線時所需的演算法【加密演算法】(3DES/DES/AES)選擇 3DES 及【認證演算法】(MD5/SHA1)選擇 MD5 認證方式。另外，需選擇【群組】(GROUP 1,2,5)雙方需選擇同一群組，此處選擇 GROUP 1 來進行連線。(如圖 11-208)

加密或認證	
ISAKMP 演算法	
加密演算法	3DES
認證演算法	MD5
群組	GROUP 1

圖 11-208 IPSec 加密或認證設定表單

步驟17. 於【IPSec 演算法】表單中，可以選擇【資料加密+認證】或是僅選擇認證方式來溝通:

【加密演算法】(3DES/DES/AES/NULL)選擇 3DES 加密演算，【認證演算法】(MD5/SHA1)選擇 MD5 認證演算方式，來確保資料傳輸時所使用的加密認證方式。(如圖 11-209)

IPSec演算法	
<input checked="" type="radio"/> 資料加密 + 認證	
加密演算法	3DES
認證演算法	MD5
<input type="radio"/> 只選認證	

圖 11-209 IPSec 演算法設定表單

步驟18. 【進階加密】（NO-PFS/ GROUP 1,2,5）選擇 GROUP 1，並填寫【ISAKMP 更新週期】為 3600 秒，和【加密金鑰更新週期】為 28800 秒，【使用模式】選擇 Main mode。（如圖 11-210）

選擇項目	
進階加密	GROUP 1
ISAKMP 更新週期	3600 秒
加密金鑰更新週期	28800 秒
使用模式	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

圖 11-210 IPSec 進階加密設定表單

步驟19. 於【GRE/IPSec】功能中，輸入【GRE 來源端 IP/遮罩】192.168.60.200，【GRE 遠端 IP】192.168.60.100（此來源端 IP 和遠端 IP 需為同一 C Class 區段，需自行設定）。（如圖 11-211）

GRE/IPSec	
GRE 來源端 IP	192.168.60.200
GRE 遠端 IP	192.168.60.100

圖 11-211 GRE/IPSec 設定表單

步驟20. 完成【IPSec Autokey】VPN_02 設定。（如圖 11-212）

i	名稱	WAN	隧道 IP 位址	IPSec演算法	變更
--	VPN_01	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>
--	VPN_02	WAN2	61.22.22.22	3DES / MD5	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-212 IPSec Autokey 設定完成畫面

步驟21. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-213)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（乙公司）內部網路位址 192.168.20.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 VPN_01 和 VPN_02 之 IPSec VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-214)

新增Trunk	
名稱	IPSec_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.20.0 / 255.255.255.0
到目的位址	<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩
	192.168.10.0 / 255.255.255.0
	<input type="radio"/> 遠端用戶端
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> VPN_01 VPN_02 </div> <div style="text-align: center;"> <input type="button" value="刪除"/> <input type="button" value="新增"/> </div> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> VPN_01 VPN_02 </div> </div>
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-213 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	IPSec_VPN_Tr..	192.168.20.0	192.168.10.0	VPN_01, ...	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-214 完成新增 VPN Trunk 設定畫面

步驟22. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-215)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-216)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-215 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-216 完成 VPN Trunk 內部至外部管制條例的設定

步驟23. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-217)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 IPSec_VPN_Trunk。
- 按下【確定】鈕。(如圖11-218)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	IPSec_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-217 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-218 完成 VPN Trunk 外部至內部管制條例的設定

步驟24. 完成 IPsec VPN GRE/IPsec 連線。(如圖 11-219)

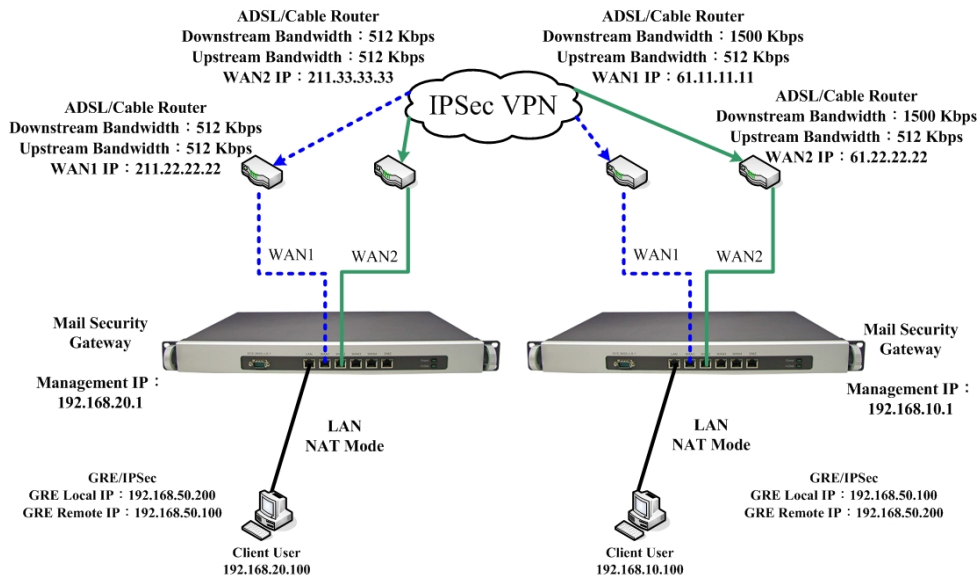


圖 11-219 IPsec VPN 連線 GRE/IPsec 之架設環境

使用兩台 NUS-MS3000 設定 PPTP VPN 的 OutBound Load Balance 連線方法

先前作業

甲公司 WAN1 IP 為 61.11.11.11
WAN2 IP 為 61.22.22.22
LAN IP 為 192.168.10.X
乙公司 WAN1 IP 為 211.22.22.22
WAN2 IP 為 211.33.33.33
LAN IP 為 192.168.20.X

甲公司 (Server) WAN1 和乙公司 (Client) WAN1 建立 IPSec VPN 連線。

甲公司 (Server) WAN2 和乙公司 (Client) WAN2 建立 IPSec VPN 連線。

本範例以兩台 NUS-MS3000 作為平台操作。假設乙公司 192.168.20.100 要向甲公司 192.168.10.100 做【虛擬私有網路】連線並下載其分享檔案。

甲公司的預設開道為 NUS-MS3000 的 LAN IP 192.168.10.1，以下為其設定步驟：

步驟1. 在甲公司 NUS-MS3000 【VPN】之【PPTP 伺服器】功能中，按下【修改】功能，啟動【PPTP 伺服器】：

- 勾選【加密認證】。
- 【用戶端 IP 範圍】設為 192.44.75.1 – 254
- 【閒置時間】設為 0。(如圖 11-220)

修改伺服器設定	
<input type="radio"/> 關閉 PPTP	
<input checked="" type="radio"/> 啟動 PPTP	
<input checked="" type="checkbox"/> 加密認證	
用戶端 IP 範圍：	192.44.75.1 -- 254
閒置 <input type="text" value="0"/> 分鐘自動斷線 (0: 表示永遠連線)	
<input type="checkbox"/> 開啓 RADIUS 伺服器認證	
(IP 或網域名稱)	<input type="text"/>
RADIUS 伺服器埠號	1812
Shared Secret	<input type="text"/>
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-220 開啟 PPTP VPN 伺服器設定



閒置時間：當 VPN 連線未被使用的情況下，會自動斷線的時間（單位：分鐘）。



RADIUS 伺服器認證：和【認證表】之【RADIUS】設定方法相同，但須再新增一條【使用者名稱】為【*】，【密碼】為【@radius】之 PPTP VPN 伺服器端連線設定，以供用戶端做認證連線之動做。

步驟2. 在甲公司 NUS-MS3000 【VPN】之【PPTP 伺服器】功能中，新增並設定下列資料：

- 按下【新增】按鈕。(如圖 11-221)
- 【使用者名稱】設為 PPTP_01。
- 【密碼】設為 123456789。
- 【用戶端的 IP 位址】選擇【使用配給的 IP 範圍】。
- 按下【確定】鈕。(如圖 11-222)
- 再按下【新增】按鈕。(如圖 11-223)
- 【使用者名稱】設為 PPTP_02。
- 【密碼】設為 987654321。
- 【用戶端的 IP 位址】選擇【使用配給的 IP 範圍】。
- 按下【確定】鈕。(如圖 11-224)

新增 PPTP 伺服器	
使用者名稱：	<input type="text" value="PPTP_01"/>
密碼：	<input type="password" value="*****"/>
用戶端的 IP 位址	
<input checked="" type="radio"/> 使用配給的 IP 範圍	
<input type="radio"/> 使用特定 IP 位址： <input type="text"/>	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-221 第一條 PPTP VPN 伺服器連線設定

PPTP 伺服器 (啟動, 加密認證: 啟動) :
 用戶端 IP 範圍: 192.44.75.1-254

i	使用者名稱	用戶端 IP 位址	連線歷時	設定
--	PPTP_01	0.0.0.0	---	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-222 完成第一條 PPTP VPN 伺服器連線設定

新增 PPTP 伺服器

使用者名稱：	PPTP_02
密碼：	*****
用戶端的 IP 位址	
<input checked="" type="radio"/> 使用配給的 IP 範圍	
<input type="radio"/> 使用特定 IP 位址：	

圖 11-223 第二條 PPTP VPN 伺服器連線設定

PPTP 伺服器 (啟動, 加密認證: 啟動):
 用戶端 IP 範圍: 192.44.75.1-254

i	使用者名稱	用戶端 IP 位址	連線歷時	設定
--	PPTP_01	0.0.0.0	---	<input type="button" value="修改"/> <input type="button" value="刪除"/>
--	PPTP_02	0.0.0.0	---	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-224 完成第二條 PPTP VPN 伺服器連線設定

步驟3. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-225)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（乙公司）內部網路位址 192.168.20.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 PPTP_Server_PPTP_01 和 PPTP_Server_PPTP_02 之 PPTP VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-226)

新增Trunk	
名稱	PPTP_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.10.0 / 255.255.255.0
到目的位址	
<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩	192.168.20.0 / 255.255.255.0
<input type="radio"/> 遠端用戶端	
通道	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 可選取的通道 ---> PPTP_Server_PPTP_01 PPTP_Server_PPTP_02 </div> <div style="text-align: center; width: 10%;"> 刪除 新增 </div> <div style="border: 1px solid black; padding: 5px; width: 45%;"> <--- 被選取的通道 ---> PPTP_Server_PPTP_01 PPTP_Server_PPTP_02 </div> </div>
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-225 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	PPTP_VPN_Tru...	192.168.10.0	192.168.20.0	PPTP_Ser...	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-226 完成新增 VPN Trunk 設定畫面

步驟4. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-227)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 PPTP_VPN_Trunk。
- 按下【確定】鈕。(如圖11-228)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	PPTP_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-227 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-228 完成 VPN Trunk 內部至外部管制條例的設定

步驟5. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-229)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 PPTP_VPN_Trunk。
- 按下【確定】鈕。(如圖11-230)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	PPTP_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-229 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-230 完成 VPN Trunk 外部至內部管制條例的設定

乙公司的預設閘道為 NUS-MS3000 的 LAN IP 192.168.20.1，以下為其設定步驟：

步驟1. 在乙公司 NUS-MS3000 【VPN】之【PPTP 用戶端】功能中，新增並設定下列資料：

- 按下【新增】按鈕。(如圖 11-231)
- 【使用者名稱】設為 PPTP_01。
- 【密碼】設為 123456789。
- 【伺服器位址】輸入填寫所要連線甲公司的遠端 (WAN1) IP 位址。
- 勾選【加密認證】。
- 【外部網路介面】位址選擇 WAN1。
- 按下【確定】鈕。(如圖 11-232)
- 再按下【新增】按鈕。(如圖 11-233)
- 【使用者名稱】設為 PPTP_02。
- 【密碼】設為 987654321。
- 【伺服器位址】輸入填寫所要連線甲公司的遠端 (WAN2) IP 位址。
- 勾選【加密認證】。
- 【外部網路介面】位址選擇 WAN2。
- 按下【確定】鈕。(如圖 11-234)

新增 PPTP 用戶端

使用者名稱：	<input type="text" value="PPTP_01"/>
密碼：	<input type="password" value="*****"/>
伺服器位址：	<input type="text" value="61.11.11.11"/> <input checked="" type="checkbox"/> 加密認證
外部網路介面：	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4
<input type="checkbox"/> NAT (與 Windows PPTP 伺服器連線用)	

圖 11-231 第一條 PPTP VPN 用戶端連線設定

PPTP 用戶端：

i	使用者名稱	伺服器位址	加密認證	連線歷時	設定
--	PPTP_01	61.11.11.11	啓動	---	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-232 完成第一條 PPTP VPN 用戶端連線設定

新增 PPTP 用戶端

使用者名稱：	<input type="text" value="PPTP_02"/>
密碼：	<input type="password" value="*****"/>
伺服器位址：	<input type="text" value="61.22.22.22"/> <input checked="" type="checkbox"/> 加密認證
外部網路介面：	<input type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4
<input type="checkbox"/> NAT (與 Windows PPTP 伺服器連線用)	

圖 11-233 第二條 PPTP VPN 用戶端連線設定

PPTP 用戶端：

i	使用者名稱	伺服器位址	加密認證	連線歷時	設定
--	PPTP_01	61.11.11.11	啓動	---	<input type="button" value="修改"/> <input type="button" value="刪除"/>
--	PPTP_02	61.22.22.22	啓動	---	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-234 完成第二條 PPTP VPN 用戶端連線設定



從 NUS-MS3000 之 PPTP VPN 用戶端建立連線至 Windows PPTP 伺服器時，要勾選【NAT(與 Windows PPTP 伺服器連線用)】選項，才可使 NUS-MS3000 下之 PC 存取 Windows 所架設網域中 PC 的資源。

步驟2. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-235)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（乙公司）內部網路位址 192.168.20.0 及遮罩 255.255.255.0
- 【到目的位址】選擇到目的位址 子網路 / 遮罩。
- 填入目的位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【通道】選擇並【新增】名稱爲 PPTP_Client_PPTP_01 和 PPTP_Client_PPTP_02 之 PPTP VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-236)

新增Trunk	
名稱	PPTP_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.20.0 / 255.255.255.0
到目的位址	
<input checked="" type="radio"/> 到目的位址 子網路 / 遮罩	192.168.10.0 / 255.255.255.0
<input type="radio"/> 遠端用戶端	
通道	
<div style="border: 1px solid black; padding: 5px;"> <-- 可選取的通道 --> PPTP_Client_PPTP_01(61.11.11.11) PPTP_Client_PPTP_02(61.22.22.22) </div>	<div style="border: 1px solid black; padding: 5px;"> <-- 被選取的通道 --> PPTP_Client_PPTP_01(61.11.11.11) PPTP_Client_PPTP_02(61.22.22.22) </div>
<input type="button" value="刪除"/> <input type="button" value="新增"/>	
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-235 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	PPTP_VPN_Tru...	192.168.20.0	192.168.10.0	PPTP_Cli...	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>

圖 11-236 完成新增 VPN Trunk 設定畫面

步驟3. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-237)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 PPTP_VPN_Trunk。
- 按下【確定】鈕。(如圖11-238)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	PPTP_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-237 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-238 完成 VPN Trunk 內部至外部管制條例的設定

步驟4. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-239)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 PPTP_VPN_Trunk。
- 按下【確定】鈕。(如圖11-240)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	PPTP_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-239 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-240 完成 VPN Trunk 外部至內部管制條例的設定

步驟5. 完成 PPTP VPN 連線。(如圖 11-241)

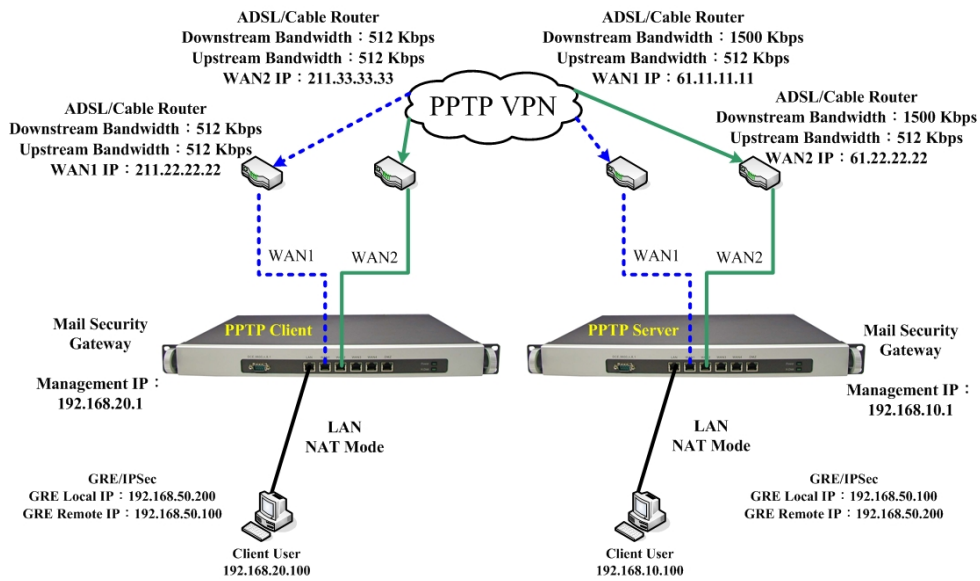


圖 11-241 PPTP VPN 連線之架設環境

使用一台 NUS-MS3000 與 Windows 2000 設定 PPTP VPN 連線的方法

先前作業

甲公司 使用 NUS-MS3000

WAN IP 為 61.11.11.11

LAN IP 為 192.168.10.X

乙公司 使用 Windows2000 之單一 PC

WAN IP 為 211.22.22.22

本範例以一台 NUS-MS3000 及 Windows 2000 VPN-PPTP 作為平台操作。
假設乙公司 211.22.22.22 要向甲公司 192.168.10.100 做【虛擬私有網路】連線並下載其分享檔案。

甲公司的預設開道為 NUS-MS3000 的 LAN IP 192.168.10.1，以下為其設定步驟：

步驟1. 在甲公司 NUS-MS3000 【VPN】之【PPTP 伺服器】功能中，按下【修改】功能，啟動【PPTP 伺服器】：

- 勾選【加密認證】。
- 【用戶端 IP 範圍】設為 192.44.75.1 – 254
- 【閒置時間】設為 0。(如圖 11-242)

修改伺服器設定	
<input type="radio"/> 關閉 PPTP	
<input checked="" type="radio"/> 啟動 PPTP	
<input checked="" type="checkbox"/> 加密認證	
用戶端 IP 範圍：	192.44.75.1 -- 254
閒置 <input type="text" value="0"/> 分鐘自動斷線 (0: 表示永遠連線)	
<input type="checkbox"/> 開啓 RADIUS 伺服器認證	
(IP 或網域名稱)	<input type="text"/>
RADIUS 伺服器埠號	1812
Shared Secret	<input type="text"/>
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-242 開啟 PPTP VPN 伺服器設定



閒置時間：當 VPN 連線未被使用的情況下，會自動斷線的時間（單位：分鐘）。

步驟2. 在甲公司 NUS-MS3000 【VPN】之【PPTP 伺服器】功能中，新增並設定下列資料：

- 按下【新增】按鈕。(如圖 11-243)
- 【使用者名稱】設為 PPTP_Connection。
- 【密碼】設為 123456789。
- 【用戶端的 IP 位址】選擇【使用配給的 IP 範圍】。
- 按下【確定】鈕。(如圖 11-244)

新增 PPTP 伺服器	
使用者名稱：	<input type="text" value="PPTP_Connection"/>
密碼：	<input type="password" value="*****"/>
用戶端的 IP 位址	
<input checked="" type="radio"/>	使用配給的 IP 範圍
<input type="radio"/>	使用特定 IP 位址： <input type="text"/>
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-243 PPTP VPN 伺服器連線設定

PPTP 伺服器 (啟動, 加密認證: 啟動):

用戶端 IP 範圍: 192.44.75.1-254

i	使用者名稱	用戶端 IP 位址	連線歷時	設定
--	PPTP_Connection	0.0.0.0	---	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-244 完成 PPTP VPN 伺服器連線設定

步驟3. 於【VPN】之【VPN Trunk】功能中，新增下列設定：(如圖 11-245)

- 填入 Trunk 所指定的【名稱】。
- 【從來源位址】選擇內部網路。
- 填入來源位址（甲公司）內部網路位址 192.168.10.0 及遮罩 255.255.255.0
- 【到目的位址】選擇遠端用戶端。
- 【通道】選擇並【新增】名稱爲 PPTP_Server_PPTP_Connection 之 PPTP VPN 連線設定。
- 勾選【顯示遠端網路芳鄰】。
- 按下【完成】鈕。(如圖 11-246)

新增Trunk	
名稱	PPTP_VPN_Trunk
從來源位址	<input checked="" type="radio"/> 內部網路 <input type="radio"/> 非軍事區
從來源位址 子網路 / 遮罩	192.168.10.0 / 255.255.255.0
到目的位址	
<input type="radio"/> 到目的位址 子網路 / 遮罩	
<input checked="" type="radio"/> 遠端用戶端	
通道	
<div style="border: 1px solid black; padding: 5px;"> <--- 可選取的通道 ---> PPTP_Server_PPTP_Connection </div>	<div style="border: 1px solid black; padding: 5px;"> <--- 被選取的通道 ---> PPTP_Server_PPTP_Connection </div>
<input type="button" value="刪除"/>	
<input type="button" value="新增"/>	
保持連線IP：	
<input checked="" type="checkbox"/> 顯示遠端網路芳鄰	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 11-245 新增 VPN Trunk 設定畫面

i	名稱	來源子網路	目的端子網路	通道	變更
	PPTP_VPN_Tru...	192.168.10.0	遠端用戶端	PPTP_Ser...	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>
<input type="button" value="新增"/>					

圖 11-246 完成新增 VPN Trunk 設定畫面

步驟4. 於【管制條例】之【內部至外部】功能中，新增下列設定：(如圖11-247)

- 【認證名稱】選擇 All_NET。
- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 PPTP_VPN_Trunk。
- 按下【確定】鈕。(如圖11-248)

新增管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3 <input type="checkbox"/> 外部網路埠4
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP <input type="checkbox"/> SMTP
認證名稱	All_NET
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	PPTP_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

圖 11-247 設定含有 VPN Trunk 的內部至外部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-248 完成 VPN Trunk 內部至外部管制條例的設定

步驟5. 於【管制條例】之【外部至內部】功能中，新增下列設定：(如圖11-249)

- 【自動排程】選擇 Schedule_1。
- 【頻寬管理】選擇 QoS_1。
- 【VPN Trunk】選擇 PPTP_VPN_Trunk。
- 按下【確定】鈕。(如圖11-250)

新增管制條例	
來源網路位址	Outside_Any
目的網路位址	Inside_Any
服務名稱	ANY
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許 <input type="checkbox"/> 拒絕
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
自動排程	Schedule_1
最高流量警示值	0.0 KBytes/Sec
頻寬管理	QoS_1
VPN Trunk	PPTP_VPN_Trunk
最多連線數	0 (0:表示不限制)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes
NAT	<input type="checkbox"/> 開啓

圖 11-249 設定含有 VPN Trunk 的外部至內部管制條例

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY	VPN	 	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	To 1

圖 11-250 完成 VPN Trunk 外部至內部管制條例的設定

乙公司的 PC 使用實體 IP (211.22.22.22)，以下為其設定步驟：

步驟1. 進入 Windows 2000，於【網路上的芳鄰】上按下滑鼠右鍵，選擇【內容】。(如圖 11-251)

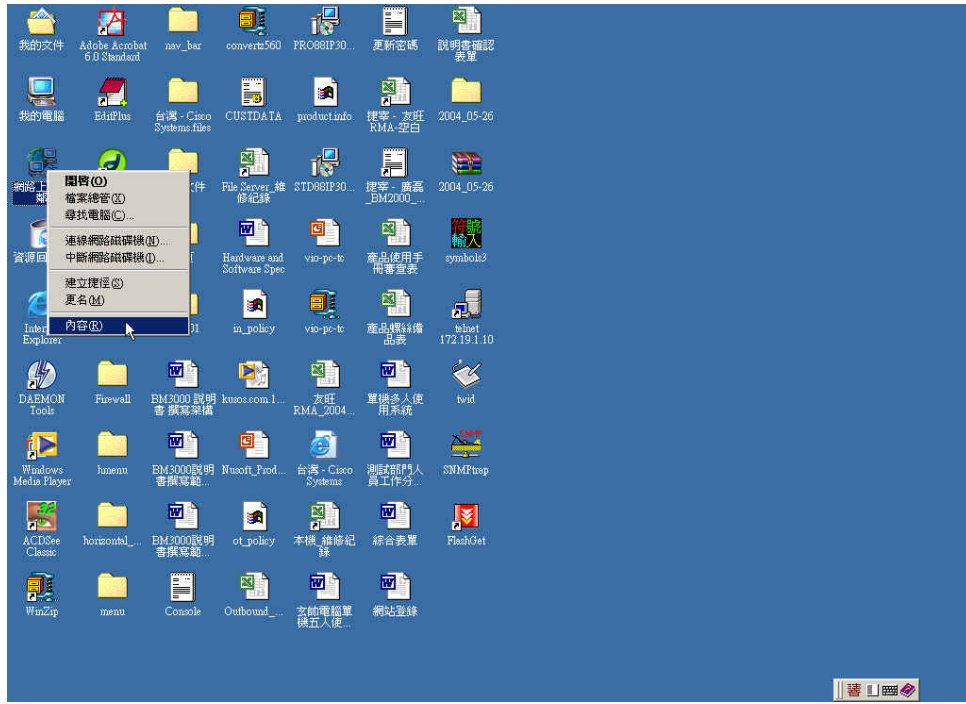


圖 11-251 開始 Windows 2000 PPTP VPN 設定

步驟2. 於【網路和撥號連線】視窗中，用滑鼠點選【建立新連線】功能。
(如圖 11-252)

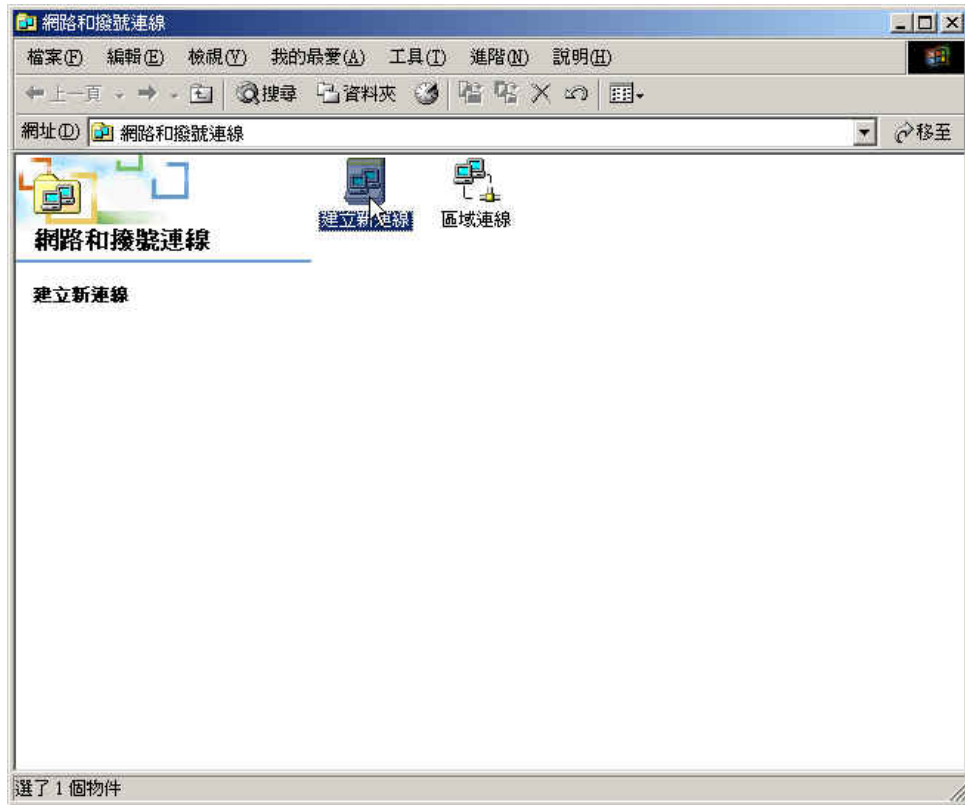


圖 11-252 網路和撥號連線視窗

步驟3. 於【位置資訊】視窗中，填入【所在位置】、【所在位置的區碼】和選擇【使用的電話系統】後，按下【確定】鈕。(如圖 11-253)

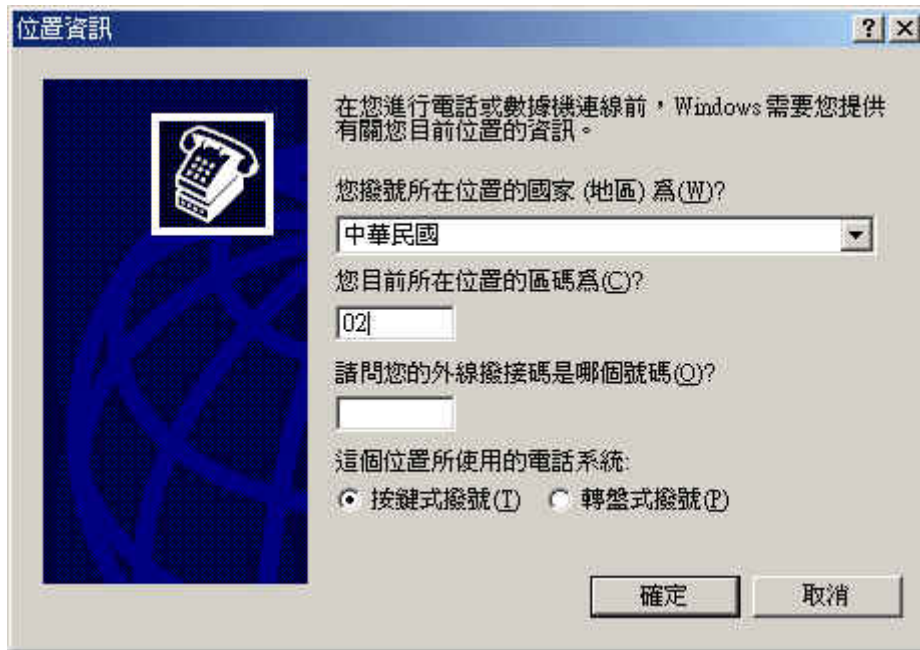


圖 11-253 位置資訊設定視窗

步驟4. 於【電話和數據機選項】視窗中，按下【確定】鈕。(如圖 11-254)

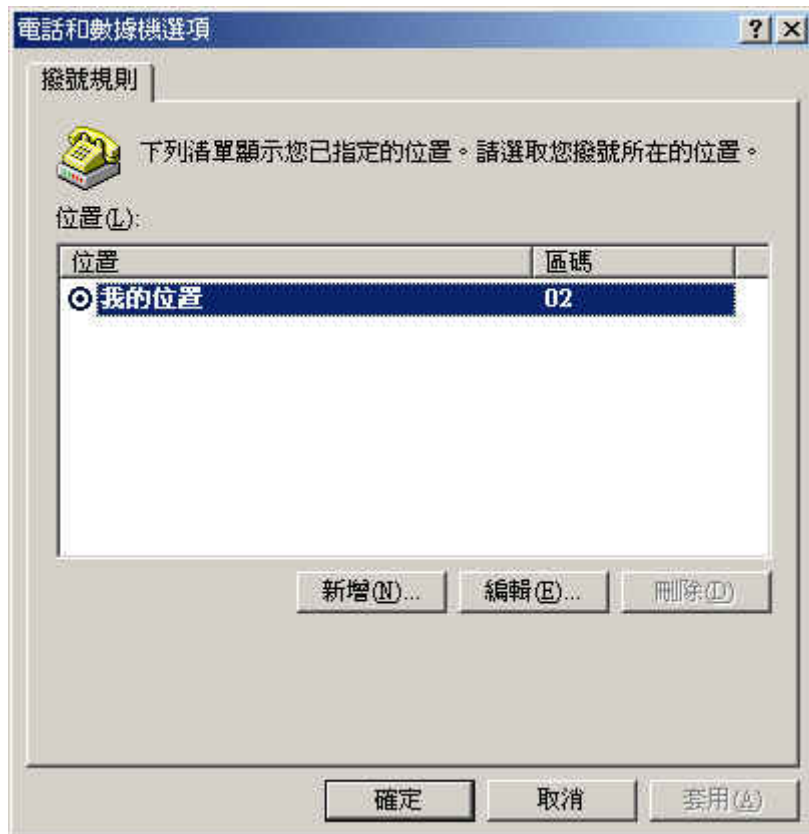


圖 11-254 電話和數據機選項視窗

步驟5. 於【網路連線精靈】視窗中，按【下一步】鈕。(如圖 11-255)

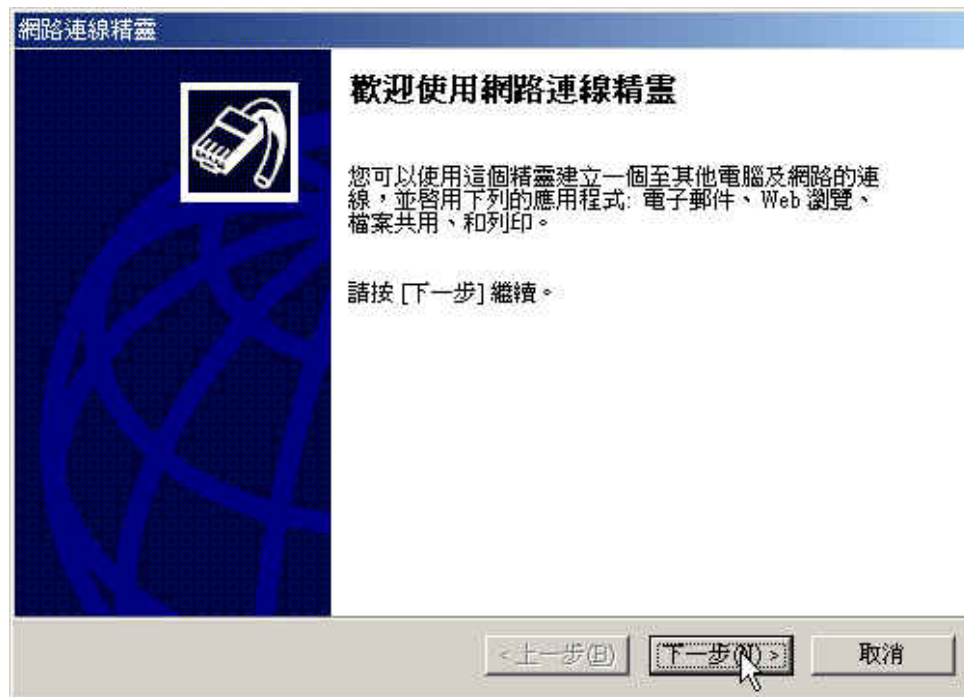


圖 11-255 網路連線精靈視窗

步驟6. 於【網路連線精靈】視窗中，選擇【透過 Internet 連線到私人網路】，並按【下一步】鈕。(如圖 11-256)

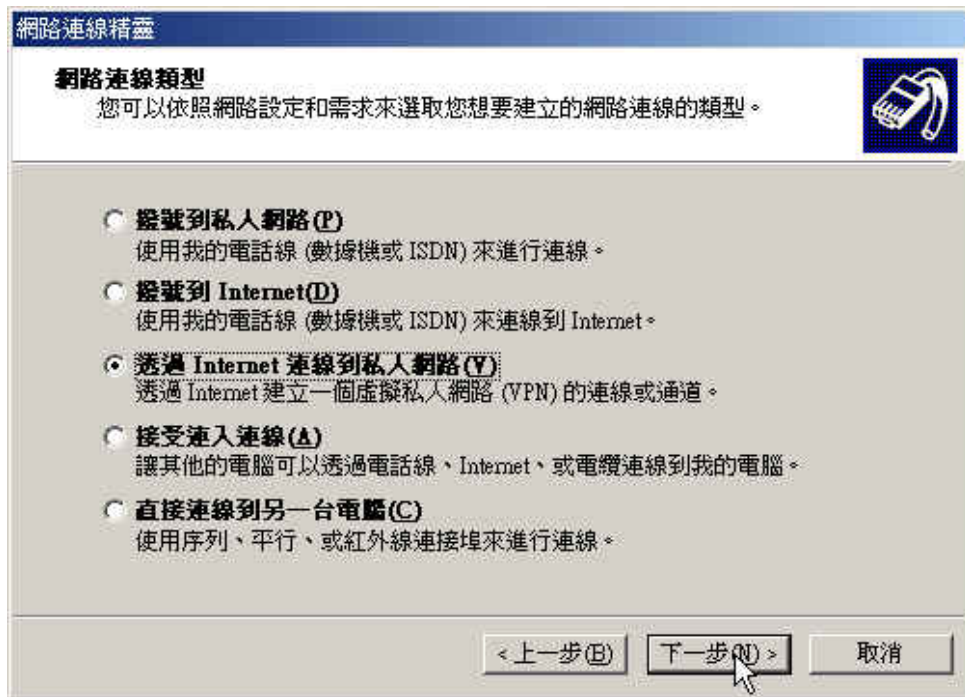


圖 11-256 設定透過 Internet 連線到私人網路

步驟7. 於【網路連線精靈】視窗中，填入【目的位址】，並按【下一步】鈕。(如圖 11-257)

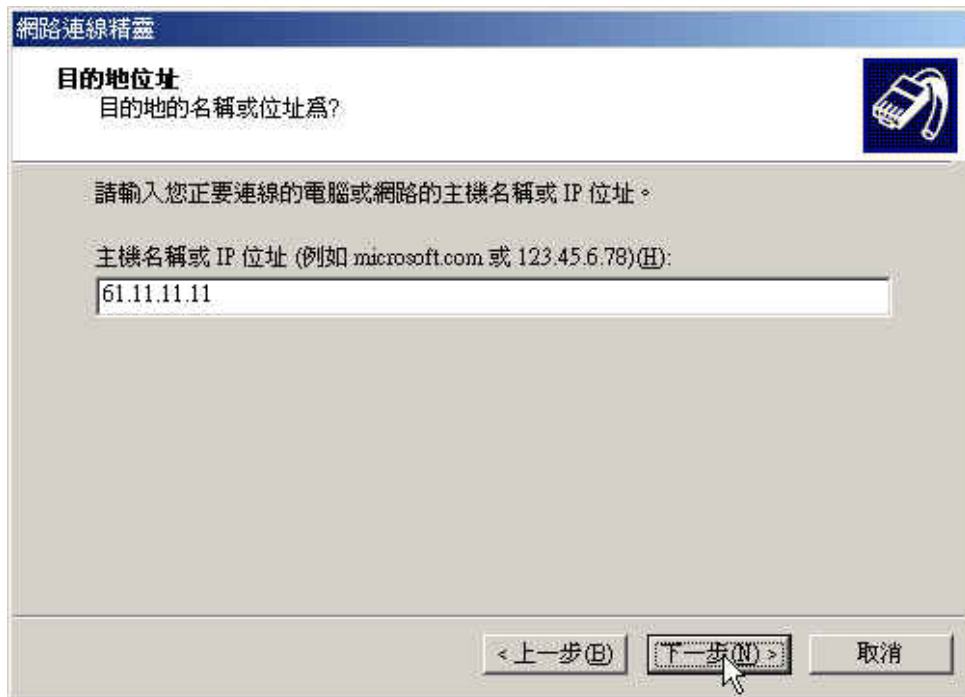


圖 11-257 設定目的主機名稱或 IP 位址

步驟8. 於【網路連線精靈】視窗中，選擇【連線可用性】之【提供給所有的使用者使用】的建立連線模式，並按【下一步】鈕。(如圖 11-258)

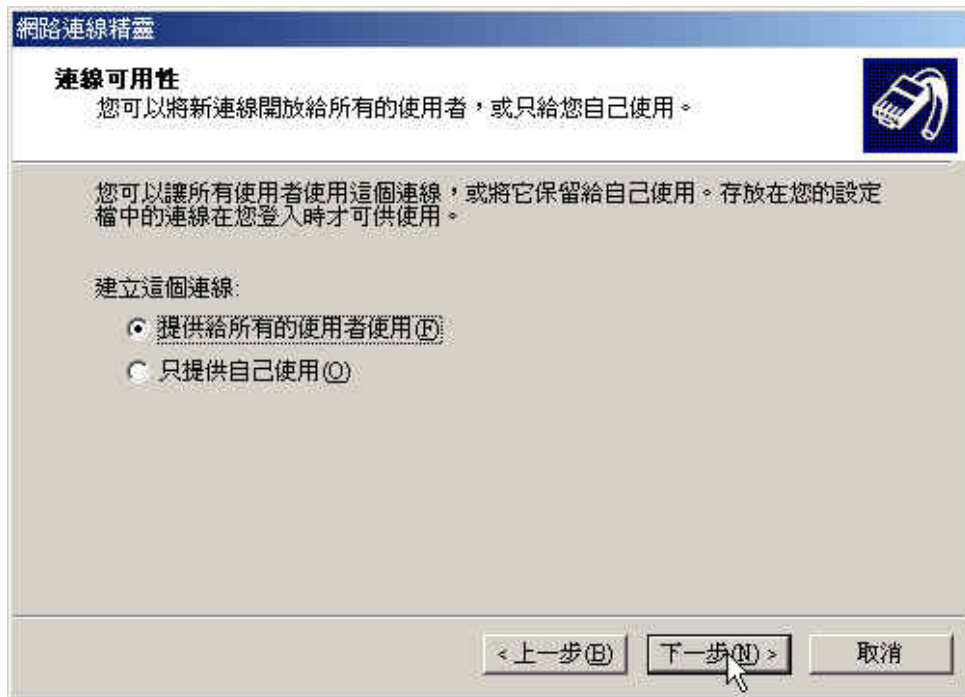


圖 11-258 設定連線可用性

步驟9. 於【網路連線精靈】視窗中，設定【連線的名稱】並按下【完成】鈕。(如圖 11-259)

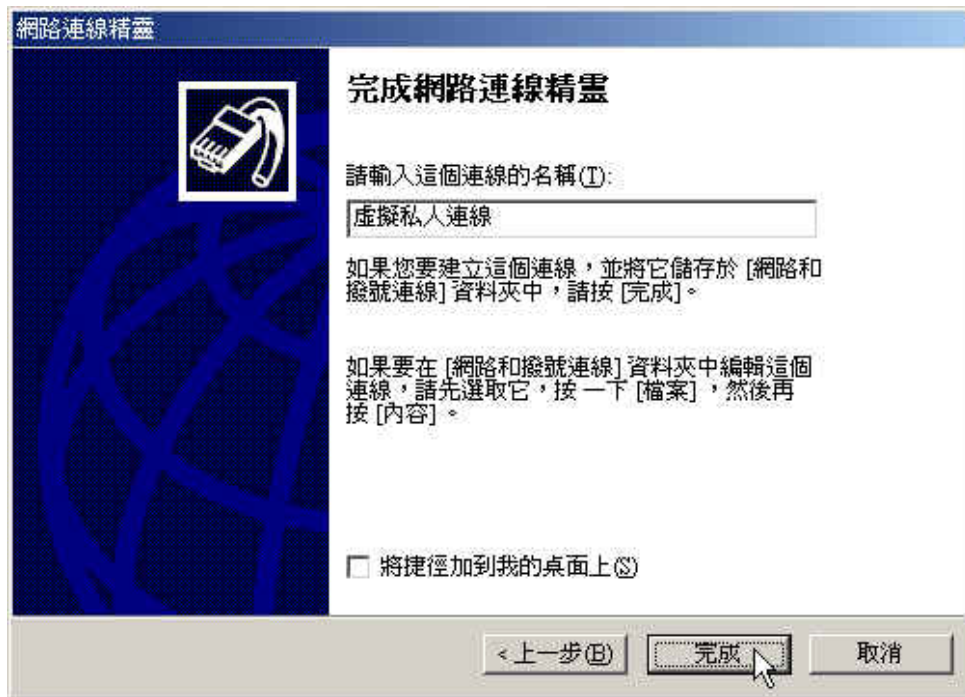


圖 11-259 完成網路連線精靈設定

步驟10. 於【連線到虛擬私人連線】視窗中，設定：。(如圖 11-260)

- 【使用者名稱】為 PPTP_Connection。
- 【密碼】為 123456789。
- 勾選【儲存密碼】。
- 按下【連線】鈕。
- 出現連線中之訊息視窗。(如圖 11-261)
- 最後出現【連線完成】視窗。(如圖 11-262)



圖 11-260 連線到虛擬私人連線設定視窗



圖 11-261 建立 PPTP VPN 連線中

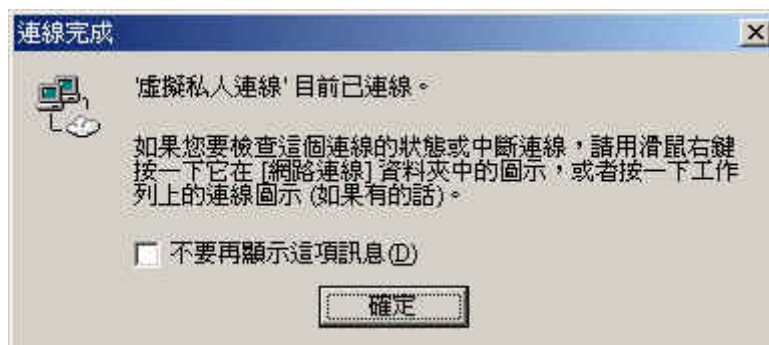


圖 11-262 完成 PPTP VPN 連線視窗

步驟11. 完成 PPTP VPN 連線。(如圖11-263)

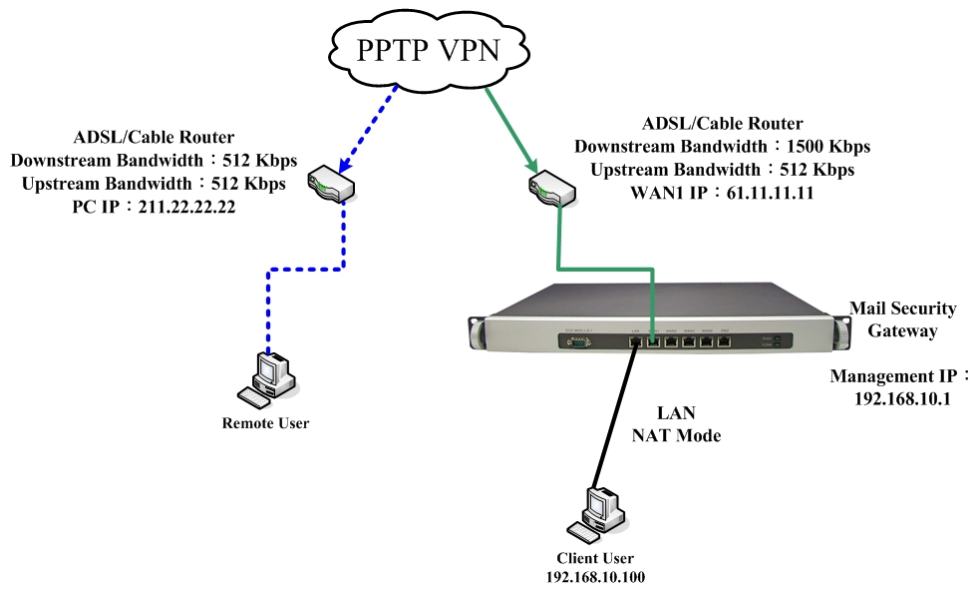


圖 11-263 PPTP VPN 連線之架設環境