MHG-2000

使 用 手 冊

目　　錄

快速安裝.....4

硬體安裝 5
軟體安裝 7
S.1 系統功能概述表 14

系統管理.....20

第 1 章 管理 21
1.1 管理員.....23
1.2 管理位址.....25
1.3 系統登出.....26
1.4 軟體更新.....28
第 2 章 組態 29
2.1 系統設定.....37
2.2 時間設定.....43
2.3 多重網段.....44
2.4 指定路由表.....56
2.5 DHCP.....60
2.6 DDNS.....64
2.7 主機名稱表.....65
2.8 SNMP.....66
2.9 電子佈告欄.....68
2.10 語言版本.....72

網路介面.....73

第 3 章 網路介面 74
3.1 網路介面功能使用範例.....83

管制條例選項 131

第 4 章 位址表 132
4.1 位址表功能使用範例.....135
第 5 章 服務表 143
5.1 自訂服務功能使用範例.....145
5.2 服務群組功能使用範例.....149
第 6 章 排程表 152
6.1 排程表功能使用範例.....154

第 7 章 頻寬表 158
7.1 頻寬表功能使用範例 160
第 8 章 認證表 164
8.1 認證帳戶和群組功能使用範例 177
8.2 RADIUS認證功能使用範例 181
8.3 POP3 認證功能使用範例 201
8.4 LDAP認證功能使用範例 203
第 9 章 應用程式管制 223
9.1 應用程式管制功能使用範例 226
第 10 章 虛擬伺服器 231
10.1 虛擬伺服器功能使用範例 233
第 11 章 VPN 252
11.1 VPN功能使用範例 266

網站管制 413

第 12 章 組態 414
12.1 網站管制功能使用範例 421
第 13 章 網站管制報告 435
13.1 統計 456
13.2 日誌 458

SSL Web VPN 459
第 14 章 SSL Web VPN 460
14.1 SSL Web VPN功能使用範例 469

管制條例 489

第 15 章 管制條例 490
15.1 管制條例功能使用範例 496

異常流量IP 517

第 16 章 異常流量IP 518
16.1 異常流量IP功能使用範例 519

進階功能 526

第 17 章 InBound負載平衡 527
17.1 InBound負載平衡功能使用範例 536
第 18 章 高可用性 568
18.1 高可用性功能使用範例 570
第 19 章 聯合防禦系統 576

19.1 聯合防禦系統功能使用範例.....580
第 20 章 證書管理 590
20.1 證書管理功能使用範例.....594
第 21 章 中央控管 613
21.1 中央控管功能使用範例.....615

監控報告.....622

第 22 章 監控記錄 623
22.1 封包記錄.....633
22.2 事件記錄.....636
22.3 連線記錄.....638
22.4 應用程式管制記錄.....640
22.5 連線數限制記錄.....642
22.6 傳輸量限制記錄.....645
22.7 監控備份.....648
第 23 章 流量排行 653
23.1 即時流量分析.....658
23.2 今日排行榜.....659
23.3 歷史排行榜.....664
第 24 章 流量圖表 665
24.1 外部網路.....667
24.2 虛擬外部網路.....669
24.3 管制條例.....671
第 25 章 網路偵測 673
25.1 Ping 674
25.2 Traceroute 677
第 26 章 遠端喚醒 678
26.1 遠端喚醒功能使用範例.....679
第 27 章 系統狀態 680
27.1 介面狀態.....685
27.2 系統效能.....687
27.3 認證狀態.....688
27.4 ARP表.....689
27.5 連線狀態.....692
27.6 DHCP用戶表.....694
27.7 主機資訊.....695

快速安裝

硬體安裝

H.1 MHG-2000 硬體外部介面說明：（如圖 H-1）

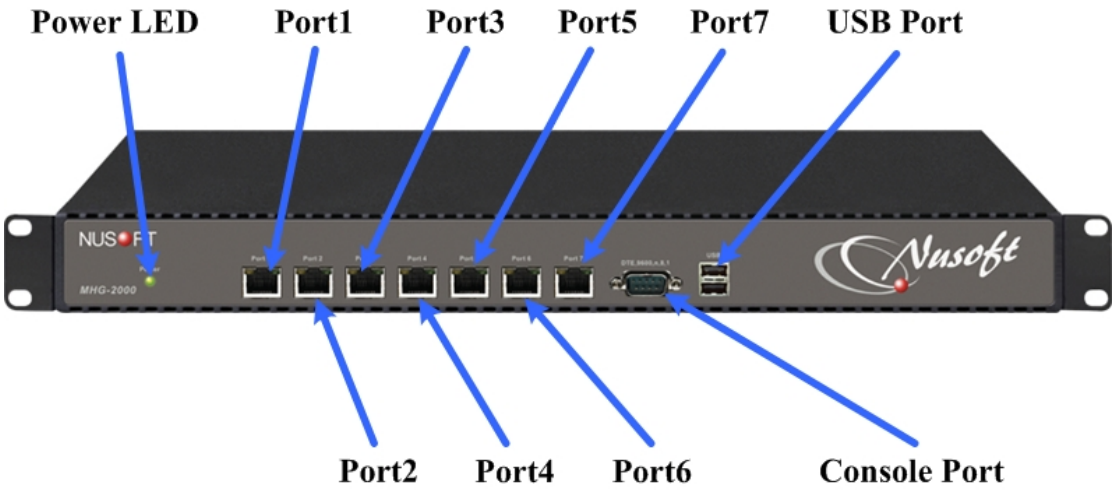


圖 H-1MHG-2000 接孔、指示燈說明

- **Power LED**：當 LED 亮綠色燈時，表示系統電源供應正常。
- **Console Port**：9pin 的串列埠接頭，主要的用途是查看 MHG-2000 系統網路介面設定和恢復原廠設定值。
- **Port 1/2/3/4/5/6/7**，可根據使用者設定為：
  - 內部網路介面：與內部交換器連接。
  - 外部網路介面：與外部路由器連接。
  - 非軍事區網路介面：用來提供一實體獨立區域與伺服器連接，以避免來自內部或外部網路的威脅。
- **USB Port**：當發生不可預期之情況，導致設備韌體毀損無法正常開機時，可使用 USB 裝置進行韌體回復。

說明：

1. Port 1/2/3/4/5/6/7 燈號狀態說明如下：
- 左燈：橘燈閃爍，代表封包通過。
- 右燈：綠燈恆亮，代表 10/100Mbps 網路速度；橘燈恆亮，代表 1000Mbps 網路速度。

H.2　MHG-2000 配置圖：（如圖 H-2）

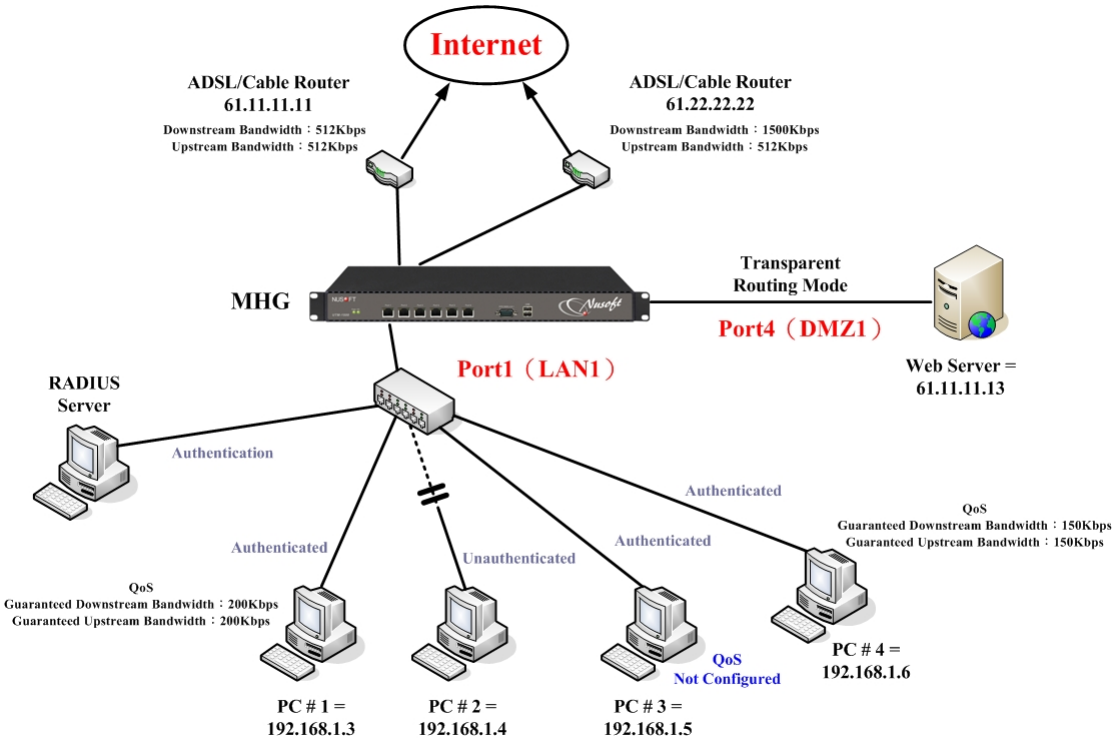


圖 H-2MHG-2000 配置圖

- MHG-2000 介面狀態：
  - Port1（LAN1）IP：192.168.1.1。
  - Port2（WAN1）IP：61.11.11.11。
  - Port3（WAN2）IP：61.22.22.22。
  - Port4（DMZ1）IP：61.11.11.13。

軟體安裝

步驟1. 首先將系統管理員的電腦和MHG-2000 Port1（LAN1）接到同一個HUB或Switch，再使用瀏覽器（IE或Firefox）登入MHG-2000。MHG-2000的管理界面IP位址內定值為 http://192.168.1.1。

步驟2. 於彈跳出來的登入驗證視窗，輸入使用者名稱與密碼（預設皆為admin）。（如圖 S-1）

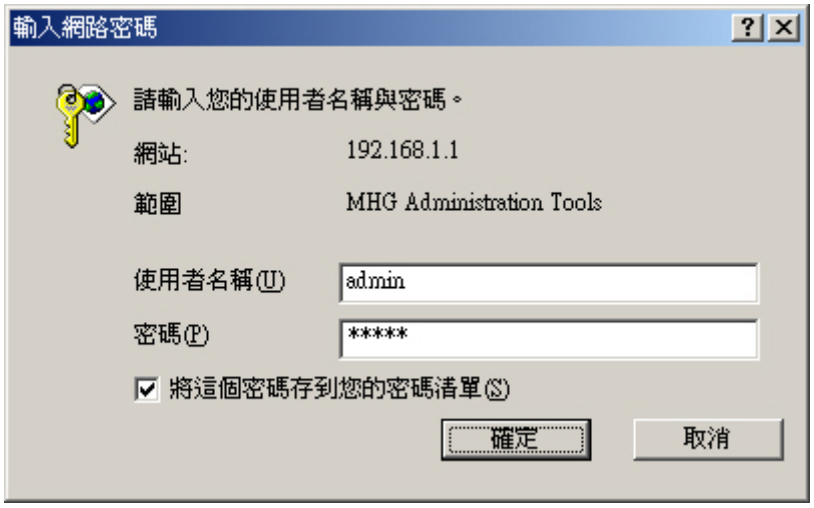


圖 S-1 輸入使用者名稱與密碼

步驟3. 登入 MHG-2000 後，顯示的系統管理介面，分為兩部份：**（如圖 S-2）**

- 索引區：用來選擇欲操作的功能項目。（可參照 系統功能概述表）
- 操作區：用來具體完成或顯示各項功能的設定、資訊。

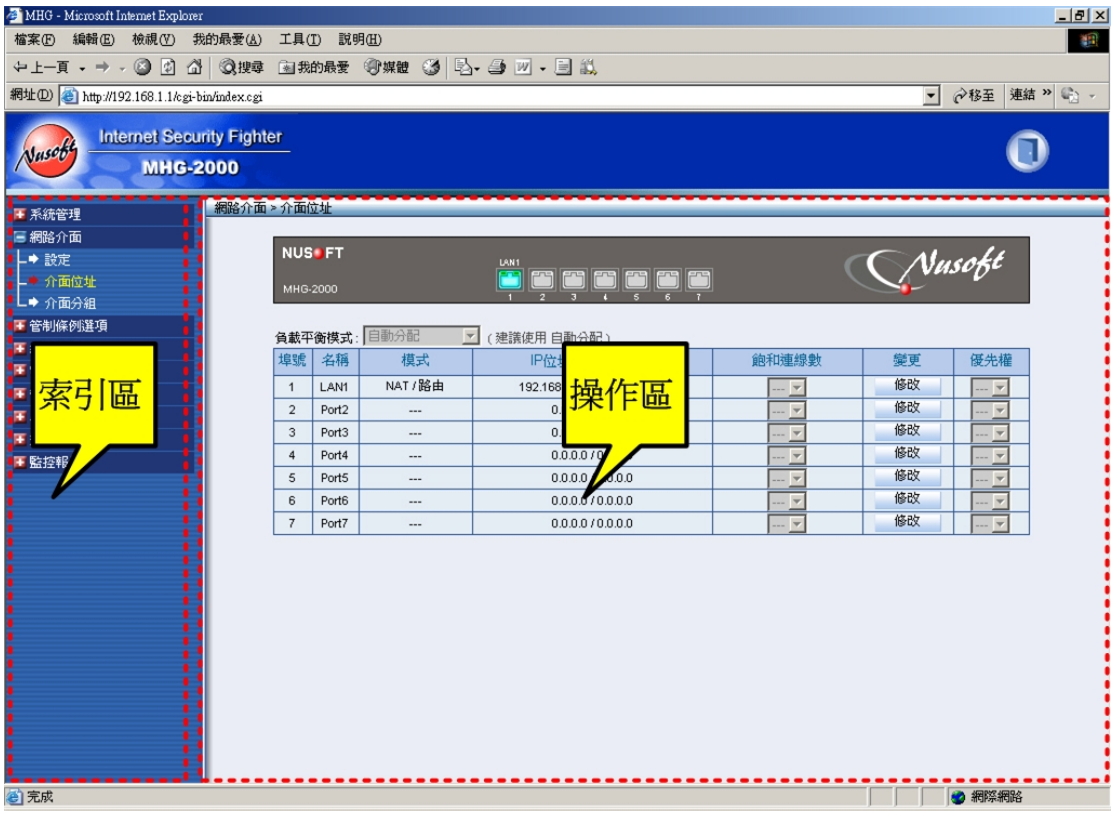


圖 S-2MHG-2000 的系統管理介面

說明：

1. 下列表格為標準虛擬 IP 位址範圍。

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

步驟4. 首次進入 MHG-2000 的管理界面時，系統會自動進入【安裝精靈】頁面。協助使用者做 MHG-2000 的基礎設定。（如圖 S-3）

圖 S-3 安裝精靈頁面

步驟5. 設定管理介面語言和【資料預設字元編碼】。（如圖 S-4）

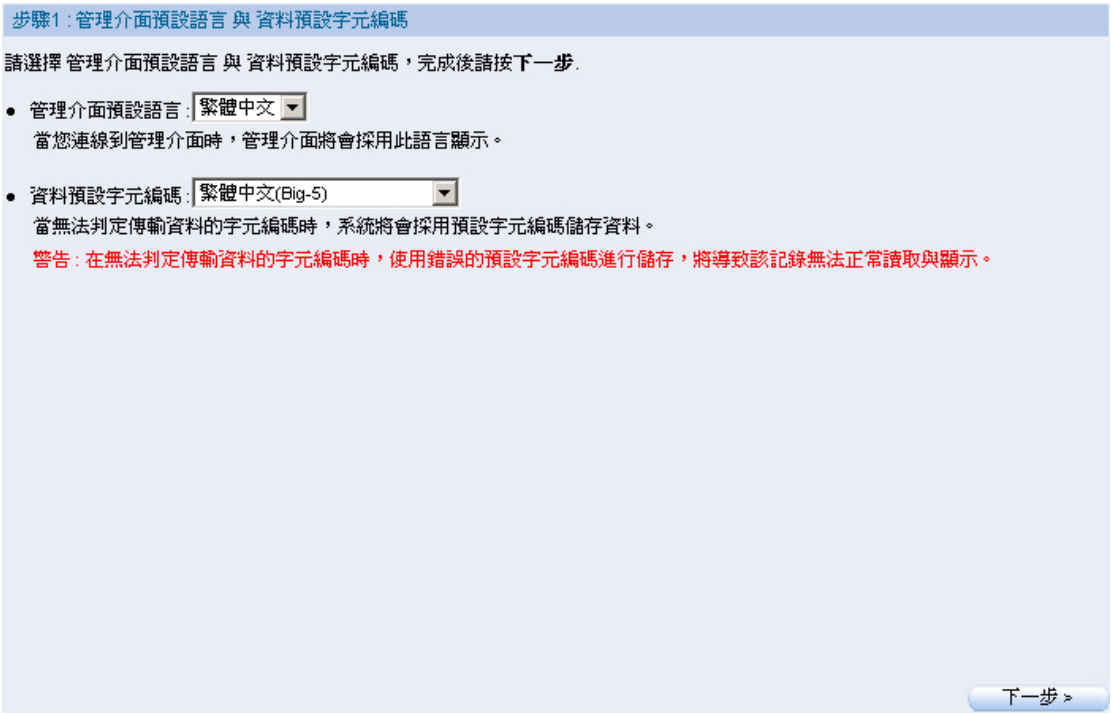


圖 S-4 選擇管理介面語言和資料預設字元編碼

注意：

1. 在無法判定傳輸資料（電子郵件、IM 訊息、...）的字元編碼時，MHG-2000 會採用【預設字元編碼】進行儲存。

步驟6. 設定內部網路介面位址（配合實際的網路環境做調整），如果更改後的內部網路介面位址不屬於系統預設網段 192.168.1.x/24，例如：內部網路介面位址改為 172.16.0.1（子網路遮罩 255.255.255.0），管理員必須設定電腦採用同網段且尚未被使用的 IP 位址。（如圖 S-5）

- 【介面編號】選擇 Port1（LAN1）。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。

圖 S-5 內部網路介面位址設定頁面

注意：

1. 如果更改了內部網路介面位址，要於瀏覽器之網址欄輸入更改後的內部網路介面位址，才能再登入 MHG-2000 之 Web UI。

步驟7. 設定外部網路介面位址（由 ISP 提供）。**（如圖 S-6）**

- 【介面編號】選擇 Port2（WAN1）。
- 【介面類型】選擇外部網路。
- 選擇指定的【外部網路連線模式】。
- 輸入指定的連線資訊。

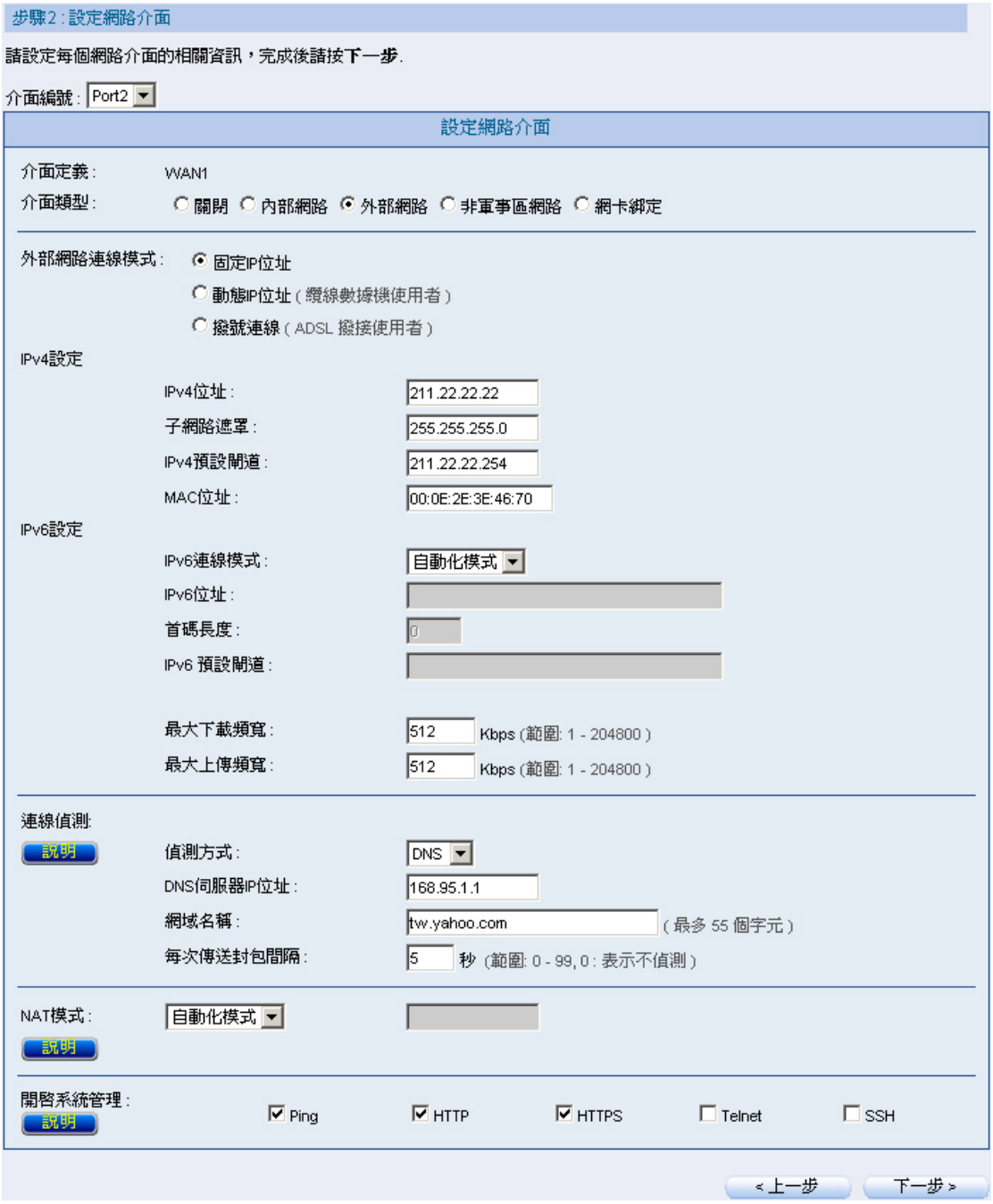


圖 S-6 外部網路介面連線設定頁面

步驟8.　【開啟與外部時間伺服器同步】機制（同步的時差請依所在時區自行調整），以提供系統正確的運作時間。（如圖 S-7）

圖 S-7 系統時間設定

步驟9.　開啟【內部至外部】管制條例。（如圖 S-8）

圖 S-8 開啟內部至外部管制條例

說明：

1. 此時會在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 S-9）
   - 【來源網路位址】為 Inside Any。
   - 【目的網路位址】為 Outside Any。
   - 【服務名稱】為 ANY。

圖 S-9 允許內部使用者存取所有外部網路資源之管制條例

2. 將區網內所有電腦設定與 MHG-2000 內部網路介面同一網段的 IP 位址、預設閘道指向 MHG-2000 的內部網路介面，或向 MHG-2000 自動取得 IP，內部網路可馬上連結至網際網路存取資料，如欲使用 MHG-2000 的管制功能，請搭配【管制條例選項】和【管制條例】功能增加相關設定值。

步驟10. 提示使用者 MHG-2000 的介面位址設定。（如圖 S-10）

圖 S-10 注意事項

步驟11. 按下【完成】鈕。（如圖 S-11）

圖 S-11 完成安裝精靈設定

S.1 系統功能概述表

功能模組	功能項目		功能簡介	參照章節
系統管理	管理	管理員	用於設定管理系統的帳號。	第 1 章
		管理位址	用於指定管理 PC 的 IP 位址，僅允許特定 IP 位址登入系統。	
		軟體更新	用於更新系統的軟體版本。	
	組態	系統設定	用於匯入/匯出(備份/還原)系統設定檔、恢復出廠設定、格式化內建硬碟、開啟電子郵件警訊通知、設定連線 Syslog 遠端記錄伺服器、進行管理介面連線(登入)設定、設定系統對外連線更新特徵碼要透過的代理伺服器、設定系統各報表每頁的資料顯示筆數及重啟系統等。	第 2 章
		時間設定	用於校正系統時間。	
		多重網段	用於建立多個內部網段，以利內部各區塊的網路配置。	
		指定路由表	用於設定各網路介面的動態路由，針對特定目的位址的封包指定傳送閘道。	
		DHCP	用於自動配發 IP 給內部電腦。	
		DDNS	用於將動態外部網路介面IP位址和特定網域名稱對應。	
		主機名稱表	用於將內部網路指定 IP 位址，對應至自訂私有域名，方便內網電腦查詢。	
		SNMP	用於即時取得系統的運作資訊。	
		電子佈告欄	用於發佈公告事項。	
		安裝精靈	用於快速安裝、設定系統。	
		語言版本	用於切換管理介面的語言版本，包括：繁體中文、簡體中文和英文。	
網路介面	設定		用於設定各網路介面的連線速率(Link Speed) / 雙工模式(Duplex Mode)、外部網路介面解析網域名稱採用的 DNS 伺服器等。	第 3 章
	介面位址		用於定義網路介面為：內部網路(進行	

			IP 位址、子網路遮罩、MAC 位址等設定)、外部網路(進行連線方式、下載/上傳頻寬等設定)、非軍事區網路(進行 IP 位址、子網路遮罩、MAC 位址等設定)。	
	虛擬外部網路		用來設定隸屬於特定實體外部網路介面的其他上網線路。	
	介面分組		用於將各實體網路介面分組，銜接獨立的網路區域。	
管制條例選項	位址表	內部網路	將設定為內部網路、外部網路和非軍事區網路的介面，所屬之 IP 位址分類群組。	第 4 章
		內部網路群組		
		外部網路		
		外部網路群組		
		非軍事區網路		
		非軍事區群組		
	服務表	基本服務	用於定義和歸類網路服務項目。	第 5 章
		自訂服務		
		服務群組		
	排程表	設定	用於規劃網路的使用排程。	第 6 章
		排程群組		
	頻寬表	設定	用於外部網路頻寬的規劃分配。	第 7 章
	認證表	認證設定	用於透過外部 RADIUS 伺服器、外部 POP3 伺服器、外部 LDAP 伺服器、本機內建用戶清單或動態密碼，進行內部電腦的上網授權驗證。	第 8 章
		認證帳戶		
		認證群組		
		外部 RADIUS		
		外部 POP3		
		外部 LDAP		
		動態密碼		
	應用程式管制	設定	用於限制內部 PC 透過特定即時通訊軟體、點對點軟體、影音軟體、網頁郵件、線上遊戲、通道軟體、遠端控制軟體存取網路資源。	第 9 章
	虛擬伺服器	IP 對應	用於將內部主機和外部真實 IP 位址做對應，提供指定的連線或服務(例如：	第 10 章
		連接埠對應		

		連接埠對應群組	PC-Anywhere、FTP、HTTP、...)。	
	VPN	IPSec 一步設定	用於建立安全的網路連線，保障透過此環境傳輸的資料不被竊取，有適合兩端點內網互連的 IPSec VPN 機制、適合使用固定電腦和特定端點內網互連的 PPTP VPN 機制。	第 11 章
		VPN 精靈		
		IPSec 自動加密		
		PPTP 伺服器		
		PPTP 用戶端		
		Trunk		
		Trunk 群組		
網站管制	組態	設定	用於匯入網站類別資料庫的使用授權碼、設定於存取所阻擋的網站時顯示之訊息、設定網站管制記錄的保存期限、設定透過管制條例要進行病毒掃描的 HTTP/FTP 傳輸檔案大小。	第 12 章
		網站白名單	用於限制內部電腦透過 HTTP 存取特定網址、網頁 MIME 資料/Script；透過 FTP 或 HTTP 下載/上傳特定副檔名的檔案。	
		網站黑名單		
		網站類別資料庫		
		檔案傳輸管制		
		MIME/Script 管制		
		網站管制群組		
	網站管制報告	設定	所有符合管制特徵、規則行為的處理結果，可以繪製成圖形化的統計報表，定時以電子郵件發送此統計報表給指定收件者；並可將其彙整成條列式的文字報表。	第 13 章
		統計		
		日誌		
SSL Web VPN	SSL Web VPN 精靈		用於快速建立 SSL Web VPN 連線設定。	第 14 章
	設定		用於設定用戶端和系統建立 Web VPN 連線時，所採用的加密方式、配發的 IP、允許存取的內部網段...。	
	硬體認證帳戶管理		用戶端建立 Web VPN 連線後的硬體資訊列表，用來做為簡化連線程序的	

			媒介。	
	SSL 應用		提供用戶端透過建立 Web VPN 連線的介面，直接存取內網指定 IP 位址的特定服務。	
	連線狀態		顯示目前系統 Web VPN 連線的狀態。	
管制條例	內部至外部		利用位址表、服務表、排程表、頻寬表、認證表、應用程式管制、虛擬伺服器、VPN、郵件過濾/歸檔/稽核、網站管制、入侵偵測防禦、網頁應用程式防火牆、SSL Web VPN 或 IM 側錄等管制項目，制定內部網路、外部網路和非軍事區網路存取網路資源的權限。	第 15 章
	外部至內部			
	外部至非軍事區			
	內部至非軍事區			
	非軍事區至外部			
	非軍事區至內部			
	內部至內部			
	非軍事區至非軍事區			
異常流量 IP	設定		用於設定異常流量的判別標準，啟動異常流量阻擋、異常流量警訊、核心交換器協同阻擋功能，設定異常流量警訊通知內容，指定不進行異常流量偵測的 IP。	第 16 章
	異常流量報告		用於顯示系統偵測到的內部異常流量 IP 清單。	
進階功能	InBound 負載平衡	設定	以 DNS 機制，分攤內部對外提供服務的流量於各對外線路，並具有斷線備援機制，避免服務中斷。	第 17 章
	高可用性	設定	提供雙主機備援機制，避免網路中斷。	第 18 章
	聯合防禦系統	核心交換器	用於指定要和異常流量 IP 機制聯合防禦的核心交換器，並可透過邊緣交換器的連線設定，取得指定交換器各埠所連接設備的 MAC、IP 資訊。	第 19 章
		邊緣交換器		
		交換器 MAC 表		
	證書管理	本地 CA 憑證	用於設定、匯入系統 VPN、SSL...機制所需的電子憑證。	第 20 章
		遠端 CA 憑證		
		授權憑證		
	中央控管	設定	用於將系統運作所產生的報表，同步傳送到所連線的遠端管理設備記錄，並透過該設備直接維護系統設定。	第 21 章
監控報告	監控記錄	設定	用於設定封包、事件、連線、病毒過濾、應用程式管制、連線數限制、傳輸量限制...監控記錄的電子郵件報告、Syslog 遠端記錄、SNMP Trap 警	第 22 章

			訊通知和 RSS feeds。	
		封包記錄	用於查看流量封包記錄。	
		事件記錄	用於查看系統事件記錄。	
		連線記錄	用於查看系統連線記錄。	
		應用程式管制記錄	用於查看管制條例應用程式管制記錄。	
		連線數限制記錄	用於查看達到管制條例連線控管臨界值記錄。	
		傳輸量限制記錄	用於查看達到管制條例傳輸量控管臨界值記錄。	
	流量排行	設定	用於觀察內部和外部使用者，彼此間透過系統存取的網站、服務、流量...資訊。	第 23 章
		即時流量分析		
		今日排行榜		
		歷史排行榜		
	流量圖表	外部網路	用於顯示對外線路頻寬的使用量。	第 24 章
		虛擬外部網路		
		管制條例	用於顯示特定管制條例頻寬的使用量。	
	網路偵測	Ping	以 Ping 和 Traceroute 功能，確認系統各介面連線狀態。	第 25 章
		Traceroute		
	遠端喚醒	設定	透過網卡啟動已關機，但仍有銜接電源的 PC。	第 26 章
	系統狀態	介面狀態	顯示目前系統介面的設定和運作狀態。	第 27 章
		系統效能	顯示系統運作所消耗的硬體資源。	
		認證狀態	顯示目前透過認證授權上網的使用者清單。	
		ARP 表	顯示目前透過系統存取網路資源的 IP 和 MAC 對應資訊。	
		連線狀態	顯示目前內部各電腦透過管制條例存取網路資源使用的連線數。	
		DHCP 用戶表	顯示目前透過 DHCP 機制取得 IP 的使用者清單。	
		主機資訊	顯示目前通過系統連線的 IP 和其對應 NetBIOS、DNS 名稱資訊。	

系統管理

第1章　管理

所謂的系統管理，是指 MHG-2000 的管理員權限、管理位址、系統登出與軟體更新等設定與管理。

MHG-2000 預設之主管理員可變更系統各項設定、監控系統運作狀態及瀏覽系統各項報表內容；針對次管理員可設定管理介面各功能項目的關閉、唯讀、讀/寫、瀏覽權限，建立分層管理機制。

【管理員】功能概述：

管理員名稱 / 次管理員名稱 說明如下：

- 登入系統的驗證名稱。
- 系統預設主管理員的名稱和密碼為 admin，不可被刪除。

權限 說明如下：

- 主管理員具有管理介面各功能項目【讀/寫/記錄內容】權限。亦即具有更改系統設定、瀏覽系統報表內容、管理系統登入帳號等權限。
- 針對次管理員給予管理介面各功能項目關閉、唯【讀】、【讀/寫】或【記錄內容】權限，可分層管理系統設定、瀏覽系統報表內容。

密碼 / 新密碼 / 確認密碼 說明如下：

- 輸入新增或修改主/次管理員之密碼。

1.1 管理員

1.1.1 新增次管理員

步驟1. 在【系統管理】>【管理】>【管理員】頁面中，做下列設定：(如圖 1-1)

- 按下【新增次管理員】鈕。
- 輸入指定的【次管理員名稱】、【密碼】。
- 【確認密碼】輸入和【密碼】相同的字串。
- 勾選唯讀【權限】。
- 按下【確定】鈕，完成設定。

圖 1-1 新增次管理員

說明：

1. 可針對管理介面各功能項目取消或勾選唯【讀】、【讀/寫】、【記錄內容】權限，以建立分層管理員。

1.1.2 修改管理員密碼、權限

步驟1. 在【系統管理】>【管理】>【管理員】頁面中，做下列設定：(如圖 1-2)

- 針對指定的管理員，按下【修改】鈕。
- 輸入原本的【密碼】、要置換的【新密碼】。
- 【確認密碼】輸入和【新密碼】相同的字串。
- 勾選指定的功能管理【權限】。
- 按下【確定】鈕，完成設定。

圖 1-2 變更管理員密碼、權限

1.2 管理位址

1.2.1 設定管理位址

步驟1. 在【系統管理】>【管理】>【管理位址】頁面中，做下列設定：(如圖 1-3)

- 輸入管理位址【名稱】。
- 【網際協定】選擇 IPv4。
- 輸入允許連線的【IP 位址】。
- 輸入【子網路遮罩】(255.255.255.255 代表 1 個 IP)。
- 【服務選項】勾選 Ping/Tracert、HTTP 和 HTTPS。
- 按下【確定】鈕，完成設定。

圖 1-3 管理位址設定頁面

注意：

1. 管理位址若要有實際的作用，必須將 MHG-2000 網路介面的【Ping/Tracert】、【HTTP】、【HTTPS】、【Telnet】與【SSH】功能全數關閉。
2. 在關閉網路介面的【HTTP】與【HTTPS】功能之前，務必要設定管理位址。否則，將會發生無法透過指定介面登入系統的窘境。

1.3 系統登出

1.3.1 登出 MHG-2000 管理介面

步驟1. 按下管理介面右上角之【系統登出】鈕，可使系統管理員隨時登出系統管理介面，避免他人更動或毀壞 MHG-2000 之設定。（如圖 1-4, 圖 1-5）

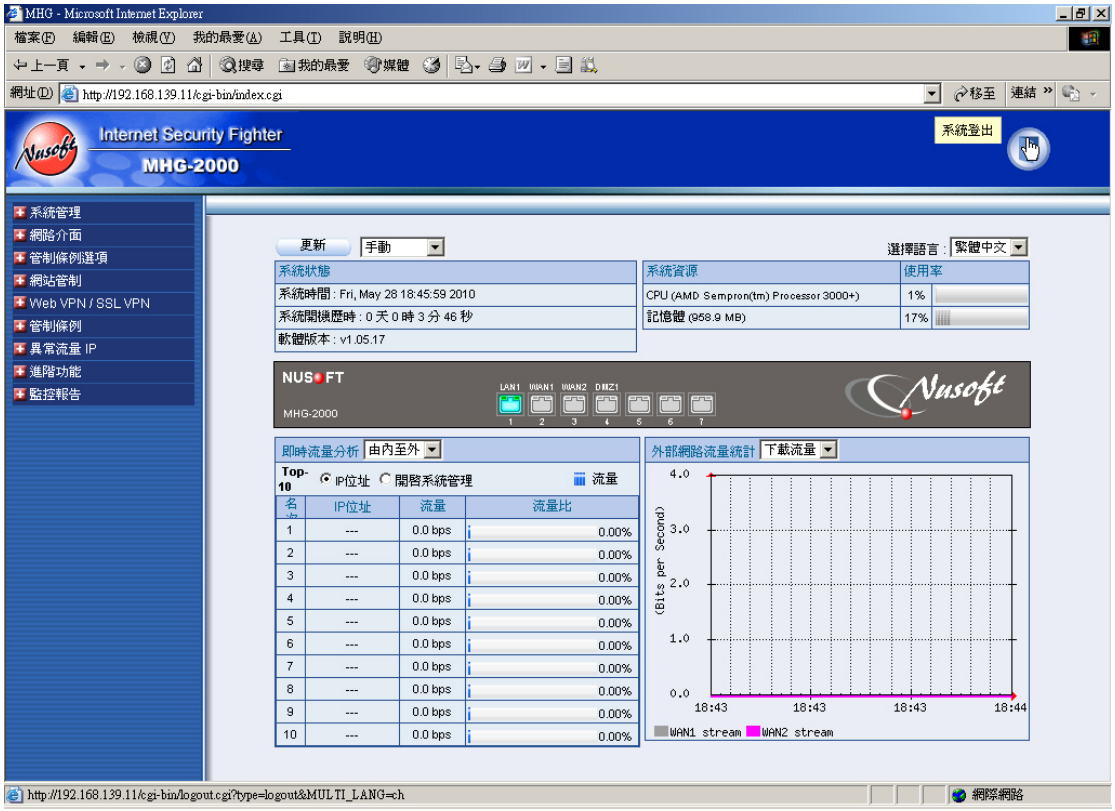


圖 1-4 登出 MHG-2000

圖 1-5 登出 MHG-2000 確認視窗

步驟2.　按下【確定】鈕，會於瀏覽器顯示登出訊息。**（如圖 1-6）**

圖 1-6 MHG-2000 登出訊息

1.4 軟體更新

步驟1. 在【系統管理】>【管理】>【軟體更新】頁面中，可依下列步驟更新軟體：

- 按下【瀏覽】鈕，選擇已下載的軟體檔案。
- 按下【確定】鈕，進行軟體更新。（如圖 1-7）

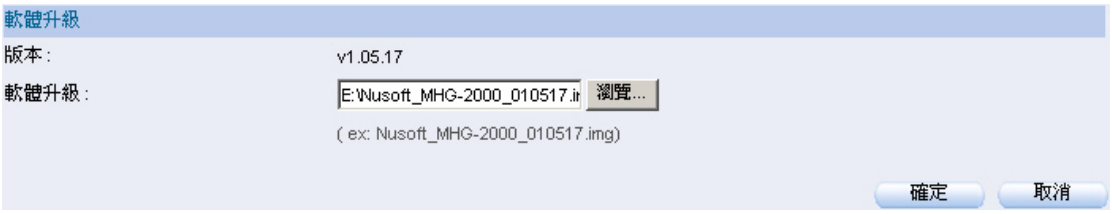


圖 1-7 更新 MHG-2000 軟體

⚠ 注意：

1. 軟體更新需 3 分鐘的時間，更新後系統將會自動重新開機；而在系統更新期間，切勿關機、斷線或是離開更新網頁，這可能會造成 MHG-2000 不可預期之錯誤。（強力建議於內部網路來更新軟體，以避免不必要的錯誤）

第2章　組態

所謂的系統組態，是指 MHG-2000 的系統設定、時間設定、多重網段、指定路由表、DHCP、DDNS、主機名稱表、SNMP、電子佈告欄和語言版本等設定。

【系統設定】功能概述：

系統組態 說明如下：

- 系統管理員可在此匯入或匯出系統設定檔，也可在此將系統恢復至出廠設定值。

備份 / 還原系統組態檔 說明如下：

- 用來將系統設定檔複製到系統內建的指定存放空間，讓管理人員可依備份日期還原該時間點的設定；亦可避免因系統設定缺損，本地端電腦遺失設定檔而無法還原的情形。
- 系統於每日 0:00 會自動進行此設定檔備份作業，管理人員亦可手動進行即時備份作業。
- 已備份的設定檔亦可匯出至本地端電腦儲存。

系統名稱設定 說明如下：

- 系統管理員可在此設定 MHG-2000 及其所隸屬單位的名稱。

電子郵件警告 / 報告設定 說明如下：

- 開啟此功能後，MHG-2000 可自動以電子郵件寄送警訊通知、系統運作報告給指定收件者。

Syslog 遠端記錄設定 說明如下：

- 用來連線指定的 Syslog 伺服器，以傳送監控記錄、網站管制日誌、...。

系統管理介面登入設定 說明如下：

- 系統管理員可在任何地方以 WebUI、Telnet、SSH 遠端管理 MHG-2000，並可在此變更登入 MHG-2000 所使用的埠號。
- 可在此設定系統管理員透過 WebUI 管理 MHG-2000 的閑置時間，若在登入 MHG-2000 後，持續未有管理或監控動作，當超過設定的閑置時間時，MHG-2000 會強制登出 WebUI。
- 當登入系統時輸入的驗證資料，達限定的錯誤次數；該登入系統的來源位址，於指定時間內可被阻擋。避免有心人士嘗試登入系統，竄改設定以瓦解系統運作。

注意：

1. 當HTTP或HTTPS埠號變更後，系統管理員如想從外部網路介面登入WebUI時，就要變更瀏覽器登入WebUI之埠號。（如：http://61.62.108.172:8080 和 https://61.62.108.172:1025）

說明：

1. 透過 HTTPS 登入 WebUI 時，可以將輸入 MHG-2000 的憑證申請書，經特定 Root CA 簽核後的【進階功能】>【證書管理】>【授權憑證】做為【SSL 憑證】。

代理伺服器設定（系統更新特徵檔專用） 說明如下：

- 若 MHG-2000 的外部網路介面，需透過指定的代理伺服器方可連線網際網路，於此必須進行連線該伺服器的設定。

SIP / H.323 協定設定 說明如下：

- 開啟此功能後，所有經 MHG-2000 傳輸的 SIP / H.323 封包，皆會被處理後再送出。

系統效能保存期限 說明如下：

- 可指定【監控報告】>【系統狀態】>【系統效能】記錄的保留時間，並於到期日刪除所有符合條件的報表。

系統表單顯示設定 說明如下：

- 可設定系統規則表（管制條例、位址表、服務表、…）、記錄清單（郵件安全日誌、網站管制日誌、…）每頁的資料顯示量。
- 當系統處理的資料未明確標定採用的字元編碼時，MHG-2000 會以預設的字元編碼來記錄並產生報表。

重新啟動系統 說明如下：

- 讓系統管理員可立即重新啟動 MHG-2000。
- 可依設定的指定時間，自動重啟 MHG-2000。

【時間設定】功能概述：

同步系統時間 說明如下：

- 可將 MHG-2000 的系統時間與系統管理員之電腦或是外部時間伺服器的時間同步化。

GMT 說明如下：

- 國際標準時間（格林威治標準時間）。

日光節約時間 說明如下：

- 啟用此功能，可調整系統時間和使用者所在地實施的夏令時間之時差。日光節約時間又稱夏令時間，是將原本的標準時間撥快一個小時，分與秒不變，恢復時再撥慢一個小時。作用在於令民眾能早一個小時起床，達到早睡早起、節約能源的目的。

【多重網段】功能概述：

名稱 說明如下：

- 為多重網段識別名稱。

網路介面 說明如下：

- 多重網段隸屬的網路介面，可為內部或非軍事區網路。

網際協定 說明如下：

- 多重網段採用的網際網路協定，可為 IPv4 或 IPv6。

IP（IPv6）位址/子網路遮罩（首碼長度） 說明如下：

- 該多重網段之網路遮罩和閘道位址。

VLAN ID 說明如下：

- 讓 MHG-2000 的網路介面支援 VLAN tag，來識別隸屬於內部或非軍事區網路的 VLAN 網段。

【指定路由表】功能概述：

動態路由 說明如下：

- 和路由器彼此交換路由資訊所產生的路由，會隨者網路架構的調整變化而更新，其更新收斂時間因網路架構大小及路由通訊協定不同而改變。
  - RIPv2：路由訊息協定（Route Information Protocol），對鄰近的路由器發送 RIPv2 要求封包，接受到封包的路由器若也採用 RIPv2 協定，便會將其路由表傳回來，發送要求的設備藉此統計抵達每個目的位置所要經過的節點數，並在自己的路由表中記錄最短路徑。

- OSPF：開放式最短優先路徑（Open Shortest Path First），對整體網路的路由器廣播，以距離參數（Distance metric）取代單純的經過節點數，並視連結狀況更新距離參數，然後用動態規劃（Dynamic Programming）演算法算出最短路徑。
- BGP：邊界閘道協定（Border Gateway Protocol），是網際網路的核心路由協定。它通過維護路由表來實現自治系統（AS）之間的可達性，屬於向量路由協定。BGP 不使用傳統域內路由協定的距離度量，而是根據路徑、網路策略和規則集來決定路由。當 BGP 在一個自治系統內部運行時，它被稱作內部邊界閘道協定（Interior Border Gateway Protocol，iBGP）；當 BGP 在 AS 之間運行時，它被稱作外部邊界閘道協定（Exterior Border Gateway Protocol，eBGP）。
  - 用於 BGP 路由中的每個自治系統都被分配一個唯一的自治系統編號（ASN）。對 BGP 來說，因為 ASN 是區別整個相互連接的網路中的各個網路的唯一標識，所以這個自治系統編號非常重要。

說明：

1. 動態路由協定依演算法可分為：
   - 距離向量路由協定（Distance Vector Routing Protocol）：根據 Bellman-Ford 演算法，使用節點數或向量來確定從一個設備到另一個設備的距離，允許的最大節點數為 16（超過此數則目標網路會被認為不可達），不考慮每個節點連結的速率，路由器將部分或全部的路由表傳遞給與其相鄰的路由器，主要有 RIP、IGRP（IGRP 為 Cisco 的私有協定）。適用少於 100 個路由器（節點），或需要較少路由更新和計算的小型網路環境。
   - 連結狀態路由協定（Link State Routing Protocol）：根據 Dijkstra 演算法，即最短優先路徑（Shortest Path First，SPF）演算法，沒有節點數的限制、有更短的收斂時間、支援 VLSM（可變長子網掩碼）和 CIDR，路由器將連結狀態訊息傳遞給在同一區域內的所有路由器，如 OSPF。不像距離向量路由協議那樣，更新時發送整個路由表，連結狀態路由協定只廣播更新或改變的網絡拓撲，這使得更新訊息更小，節省了頻寬和 CPU 使用率。

2. 動態路由協定依路由器在自治系統（AS）中的位置可分為：
   - 內部閘道協定（Interior Gateway Protocol，IGP）：包含 RIP、IGRP、EIGRP、OSPF、IS-IS 協定。
   - 外部閘道協定（External Gateway Protocol，EGP，也叫域間路由協定）：是為一個簡單的樹型拓撲結構而設計，在處理選路循環和設置選路策略時，具有明顯的缺點，目前已被 BGP 代替。

3. 在網際網路中，一個自治系統（AS，autonomous system）是指在一個（有時是多個）實體管轄下的所有 IP、網路和路由器，它們對網際網路執行共同的路由策略。多個組織可

使用各自私有的自治系統編號來與同一個將它們連接到網際網路的 ISP 之間執行 BGP 協定，儘管 ISP 支援了這多個自治系統，但對網際網路來說只能看到該 ISP 的路由策略。所以 ISP 必須具有一個公開且正式登記的自治系統編號（ASN）。

- 到 2007 年為止，自治系統編號都是 16 位長的整數，這最多能被分配給 65536 個自治系統。自治系統編號被分成兩個範圍：第一個範圍是公開的 ASN，從 1 到 64511，它們可在網際網路上使用；第二個範圍是被稱為私有編號，從 64512 到 65534，它們僅能在一個組織自己的網路內使用。
- 從 2007 年初開始，各 RIR 已開始分配 32 位長度的 ASN。這些編號將以<高 16 位數值的十進位形式>.<低 16 位數值的十進位形式>的形式來使用。例如：編號為 268468224（十六進位則為 10008000）的 ASN 寫做 4096.32768。

靜態路由 說明如下：

- 用來將傳送至特定目的端之封包導向固定網路節點。
- 可採用 IPv4 或 IPv6 網際網路協定。

【DHCP】功能概述：

配發指定 IP 至用戶端設定 說明如下：

- MHG-2000 可依 LAN 或 DMZ 下 PC 網卡的 MAC 位址，DHCP 配發指定的 IP。

【DDNS】功能概述：

網域名稱 說明如下：

- 系統管理員向 DDNS 服務提供者所申請之網域名稱。

外部網路位址 說明如下：

- 該網域名稱所對應的 MHG-2000 外部網路介面位址。

【主機名稱表】功能概述：

主機名稱 說明如下：

- 可由系統管理員自訂，讓內部使用者直接透過此名稱，存取相對應主機所提供的資源。

網際協定 說明如下：

- 主機名稱表採用的網際網路協定，可為 IPv4 或 IPv6。

IP 位址 說明如下：

- 主機名稱對應的 IP 位址，可為內部網路或非軍事區網路的 IP 位址。

【SNMP】功能概述：

SNMPv3 說明如下：

- SNMP 是專門用於管理網路節點（伺服器、工作站、路由器、交換機…）的協定。網路管理員透過 SNMP 接收到的訊息，能即時發現並解決網路問題，或協助其規劃網路資源的運用。
- SNMP 管理的網路有三個構成要素：被管理的設備、代理、網路管理系統（NMSs，Network-management systems）。
- 目前 SNMP 有 3 種版本：
  - SNMPv1：欠缺加密及認證功能，皆以明碼傳送字串，使任何人皆可輕易攔截密碼，安全性備受爭議。
  - SNMPv2：改進第一版的許多安全缺陷，但執速度能不如第一版快，且無法和其相容，因此不被廣泛接受。
  - SNMPv3：修正了前兩版的問題，不僅會對所有傳輸資料進行加密，而且可使 SNMP 代理程式對管理系統做認證動作，並確保數位簽章訊息的完整性。另外，針對每項訊息還會有存取清單的限制。

安全模式 說明如下：

- SNMPv3 規定了三個認證和隱私模式：
  - 無隱私模式，即 NoAuthNoPriv。類似 SNMPv1 的明碼字串，適用於 SNMP 網路實體處於一個可信賴的環境中時。
  - 無隱私認證模式，即 AuthNoPriv。
  - AuthPriv 模式。它不僅要進行認證，而且要對 SNMP 資料進行加密。

帳戶名稱 說明如下：

- 管理系統在取得 MHG-2000 的運作資訊時，所要輸入的認證名稱。

認證協定 說明如下：

- 支援 HMAC_MD5_96、HMAC_SHA_96 認證協定。

認證密碼 說明如下：

- 管理系統在取得 MHG-2000 的運作資訊時，所要輸入的認證密碼。

加密協定 說明如下：

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

加密密碼 說明如下：

- 管理系統以加密方式取得 MHG-2000 的運作資訊時，所要輸入的密碼。

【電子佈告欄】功能概述：

電子佈告欄連線設定 說明如下：

- 設定電子佈告欄管理介面連線登入的埠號、帳號和密碼。
- 設定電子佈告欄提示訊息。

電子佈告欄訊息設定 說明如下：

- 用來設定要對內部使用者發佈的公告事項。
- 系統會在特定內部網路或非軍事區網路的電腦透過 MHG-2000 存取網頁時，發布排程中的公告訊息。

2.1 系統設定

2.1.1 下載 MHG-2000 系統設定檔

步驟1. 在【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-1）

- 在【系統組態】設定欄位中，按下【匯出系統組態檔至用戶端】右方的 匯出 鈕。
- 在【檔案下載】視窗中，按下【儲存檔案】鈕，接著指定匯出檔案所要儲存的目的位置，再按下【存檔】鈕。MHG-2000 設定檔即會複製至指定儲存位置。

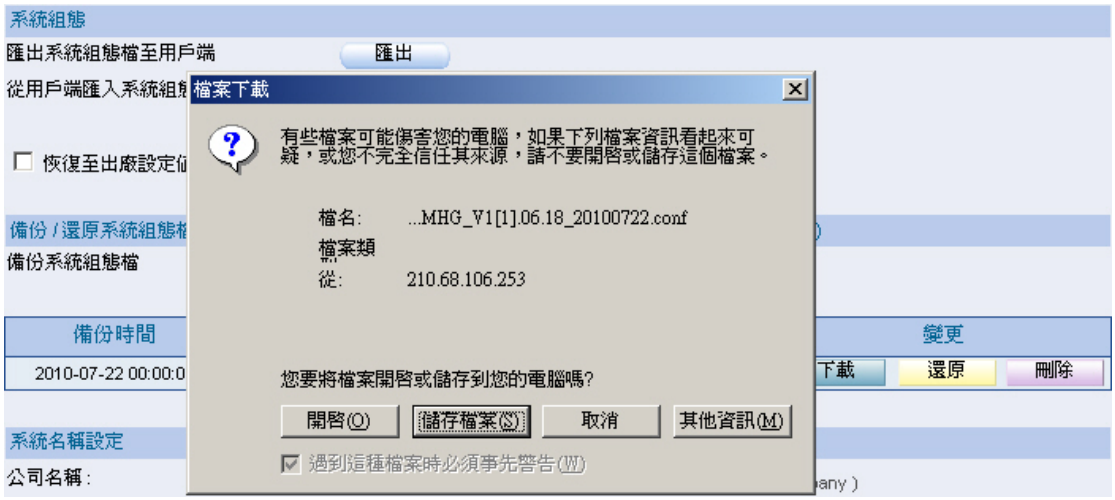


圖 2-1 匯出系統組態檔

2.1.2 匯入設定檔於 MHG-2000 中

步驟1. 在【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-2）

- 在【系統組態】設定欄位中，按下【從用戶端匯入系統組態檔】右方的【瀏覽】鈕。
- 在【選擇檔案】視窗中，【開啟】儲存在電腦的 MHG-2000 設定檔。
- 按下【確定】鈕。
- 在確認視窗中，【確定】將設定檔案匯入 MHG-2000。（如圖 2-3）

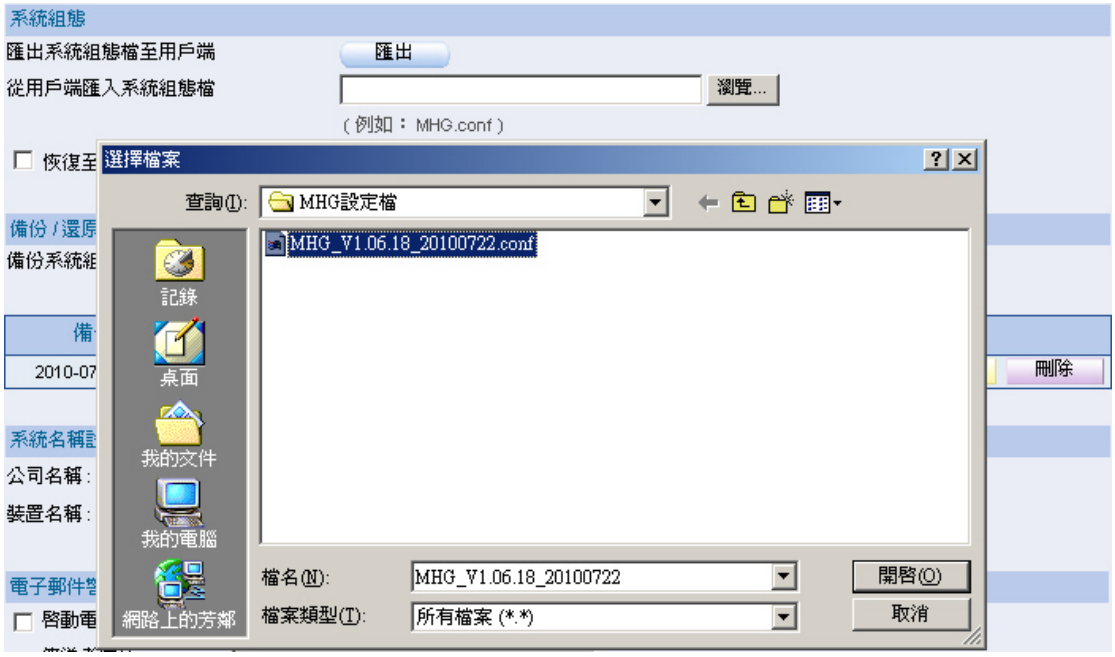


圖 2-2 匯入檔案所在目錄位置與檔名

圖 2-3 匯入設定檔確認視窗

2.1.3 將 MHG-2000 恢復為出廠設定值

步驟1. 在【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-4）

- 在【系統組態】設定欄位中，勾選【恢復至出廠設定值】。
- 按下【確定】鈕。
- 在確認視窗中，【確定】恢復 MHG-2000 為出廠時的原始設定值。（如圖 2-5）

圖 2-4 恢復至出廠設定值

圖 2-5 恢復出廠設定值確認視窗

2.1.4 設定電子郵件通知

步驟1. 在【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-6）

- 在【系統名稱設定】欄位中：
  - 【公司名稱】輸入 MHG-2000 所隸屬的單位名稱。
  - 【裝置名稱】輸入 MHG-2000 的名稱。
- 在【電子郵件警告 / 報告設定】欄位中：
  - 勾選【啟動電子郵件警告 / 報告】。
  - 輸入電子郵件通知的【傳送者位址】。
  - 【郵件 SMTP 伺服器】輸入遞送電子郵件的 SMTP 伺服器位址。
  - 【電子郵件位址 1】輸入第一筆接受訊息通知的電子郵件位址。
  - 【電子郵件位址 2】輸入第二筆接受訊息通知的電子郵件位址。
- 按下【確定】鈕，完成設定。

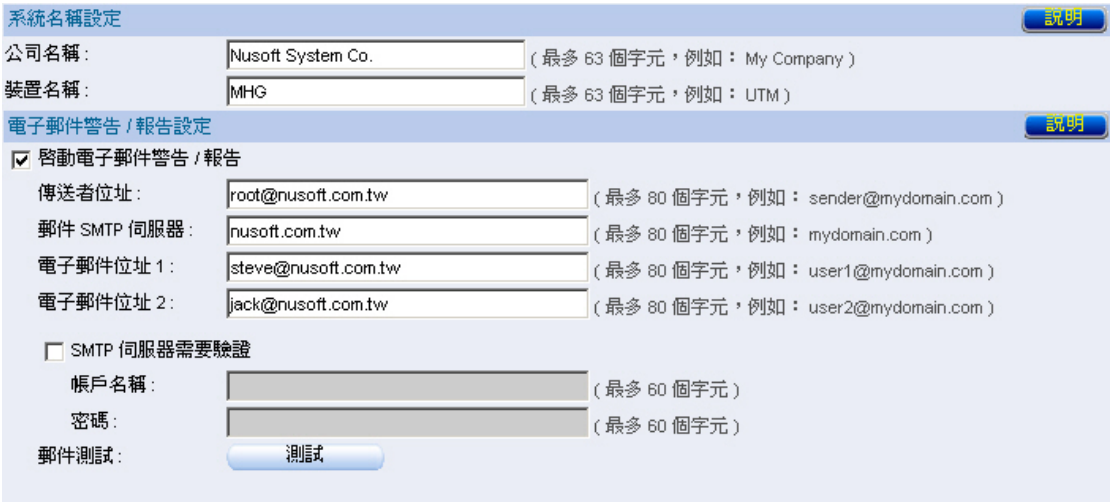


圖 2-6 開啟 MHG-2000 發送警告/報告信函功能

說明：

1. 按下【測試】鈕，可測試【電子郵件位址 1】和【電子郵件位址 2】，輸入的電子郵件帳號是否能正確收到警訊。

2. 當設定的【郵件 SMTP 伺服器】需要驗證才能透過其寄信時，就要啟動【SMTP 伺服器需要驗證】功能，並輸入相關的驗證設定。

2.1.5 重新啟動 MHG-2000

步驟1. 在【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-7）

- 在【重新啟動系統】設定欄位中，按下【系統將被重新啟動】右方的【重新啟動】鈕。
- 在確認視窗中，【確定】重新啟動 MHG-2000。（如圖 2-8）

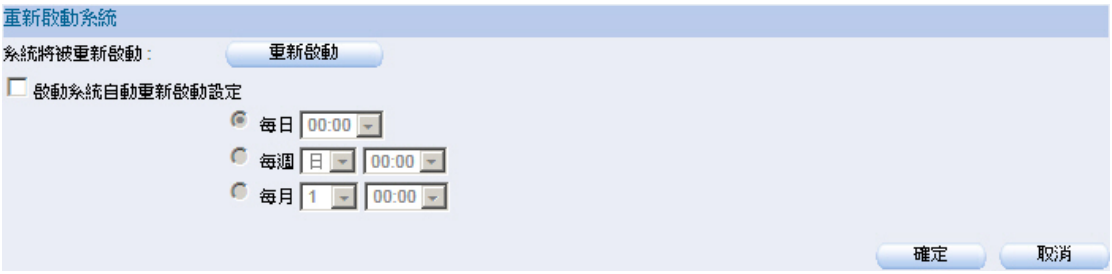


圖 2-7 重新啟動系統

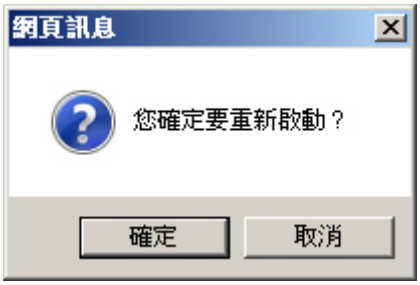


圖 2-8 重新啟動確認視窗

2.2 時間設定

2.2.1 MHG-2000 時間設定

步驟1. 在【系統管理】>【組態】>【時間設定】頁面中，做下列設定：（如圖 2-9）

- 設定所在時區和 GMT 的時差。
- 勾選【開啟與外部時間伺服器同步】。
- 輸入【時間伺服器位址】。
- 輸入 MHG-2000 的時間校正頻率。
- 按下【確定】鈕，完成設定。

圖 2-9 系統時間設定

說明：

1. 按下【系統時間與您的電腦同步】右方的【同步】鈕，MHG-2000 的系統時間會與目前連線管理的電腦時間同步。
2. 【與 GMT 相差】和【時間伺服器位址】可利用【輔助選取】進行設定。

2.3 多重網段

2.3.1 內部特定網段之電腦透過 MHG-2000 以 NAT 或 Routing 的方式連上網際網路

環境設定

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1（10.10.10.1）直接連到 ISP 機房之 Router（10.10.10.2）上網，由 ISP 配發給使用者之 IP 網段為 162.172.50.x/24。

Port2（WAN1）的 IP 位址（10.10.10.1，虛擬 IP）NAT 為 162.172.50.1（真實 IP），以連上網際網路更新系統特徵定義檔。

Port3 設為 WAN2（211.22.22.22）和 ATU-R 對接，連上網際網路。

步驟1. 在【系統管理】>【組態】>【多重網段】頁面中，做下列設定：（如圖 2-10）

- 輸入指定的【名稱】。
- 【網路介面】選擇 Port1（LAN1）。
- 【網際協定】選擇 IPv4。
- 【IP 位址】輸入 162.172.50.1。
- 【子網路遮罩】輸入 255.255.255.0。
- 按下【確定】鈕，完成設定。（如圖 2-11）

圖 2-10 設定多重網段

圖 2-11 完成多重網段設定

注意：

1. 若設定的網段或 IP 隸屬於不同的【網路介面】時，要在【管制條例】>【內部至內部】（或【非軍事區至非軍事區】）頁面中，設定一【來源網路位址】為 Inside Any（或 DMZ Any）、【目的網路位址】為 Inside Any（或 DMZ Any）、【服務名稱】為 ANY 的規則，讓內部網路（或非軍事區網路）的電腦可以相互存取。

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 2-12）

- 選擇【埠號】2，按下【修改】鈕。
- 【介面類型】選擇外部網路，並輸入由 ISP 所指定的連線設定。
- 【NAT 模式】選擇並輸入指定 IP 位址 162.172.50.1。

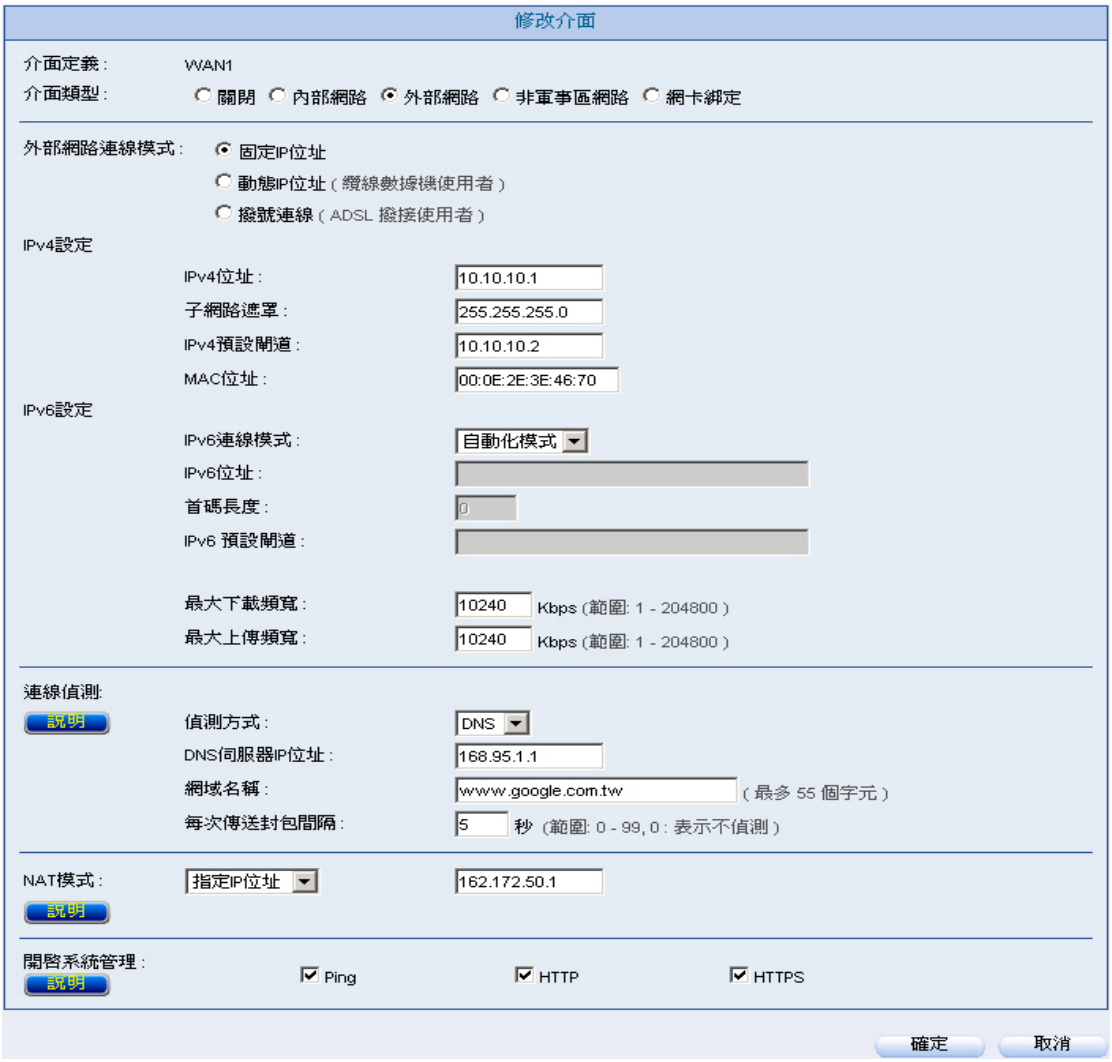


圖 2-12 輸入外部網路介面連線設定

步驟3. 在【管制條例選項】>【位址表】>【內部網路】頁面中，做下列設定：（如圖 2-13）

圖 2-13 內部網路位址表設定

步驟4. 在【管制條例】>【內部至外部】頁面中，做下列設定：

- 按下【新增】鈕。
- 【來源網路位址】選擇所設定的內部網路位址表規則（LAN1_Subnet1）。
- 【動作】勾選允許所有外部網路介面。
- Port2（WAN1）【傳送模式】選擇自動。
- Port3（WAN2）【傳送模式】選擇自動。
- 按下【確定】鈕。**（如圖 2-14）**
- 再次按下【新增】鈕。
- 【來源網路位址】選擇所設定的內部網路位址表規則（LAN1_Subnet2）。
- 【動作】勾選允許所有外部網路介面。
- Port2（WAN1）【傳送模式】選擇路由。
- Port3（WAN2）【傳送模式】選擇自動。
- 按下【確定】鈕，完成設定。**（如圖 2-15, 圖 2-16）**

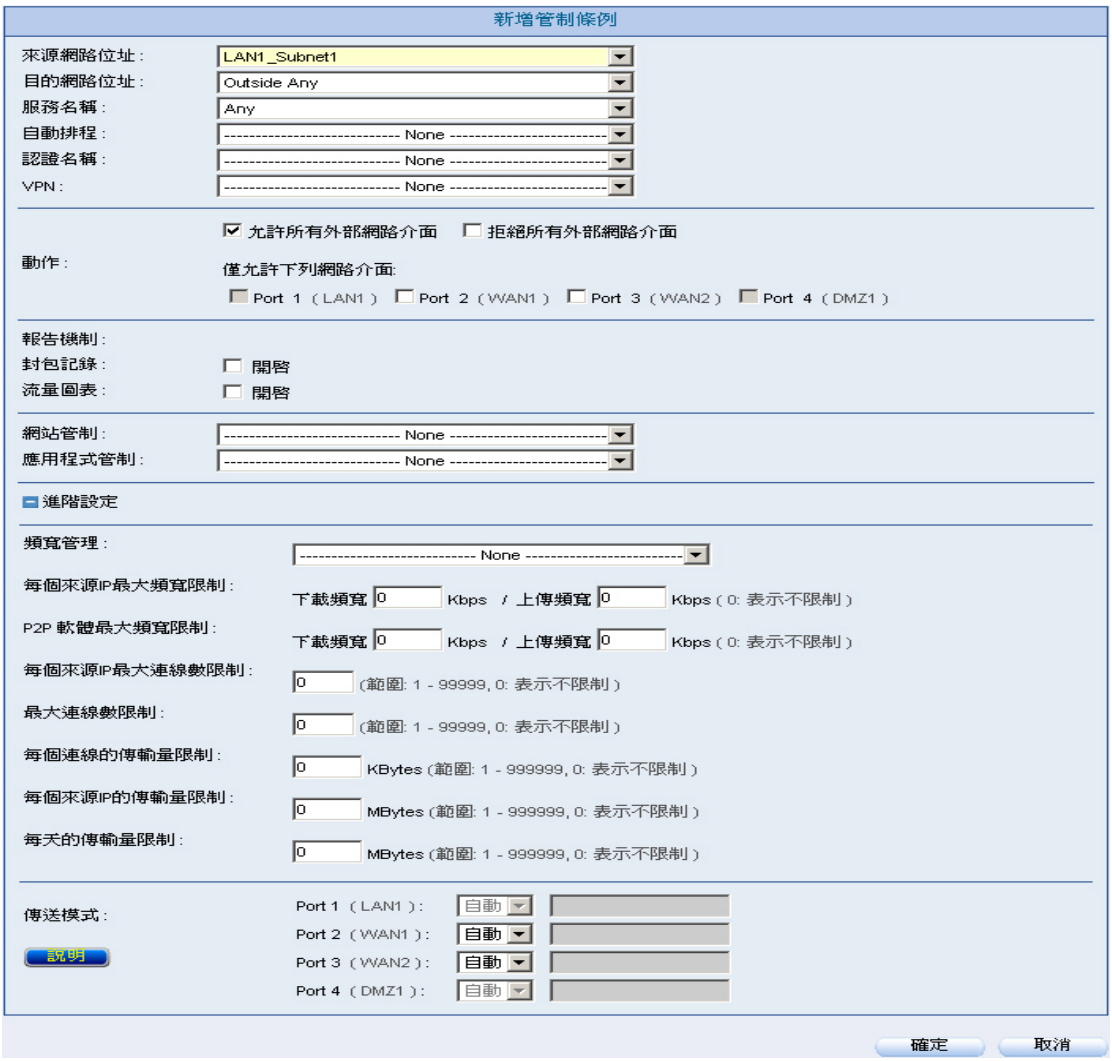


圖 2-14 設定第一筆內部指定網段對外連線模式之管制條例

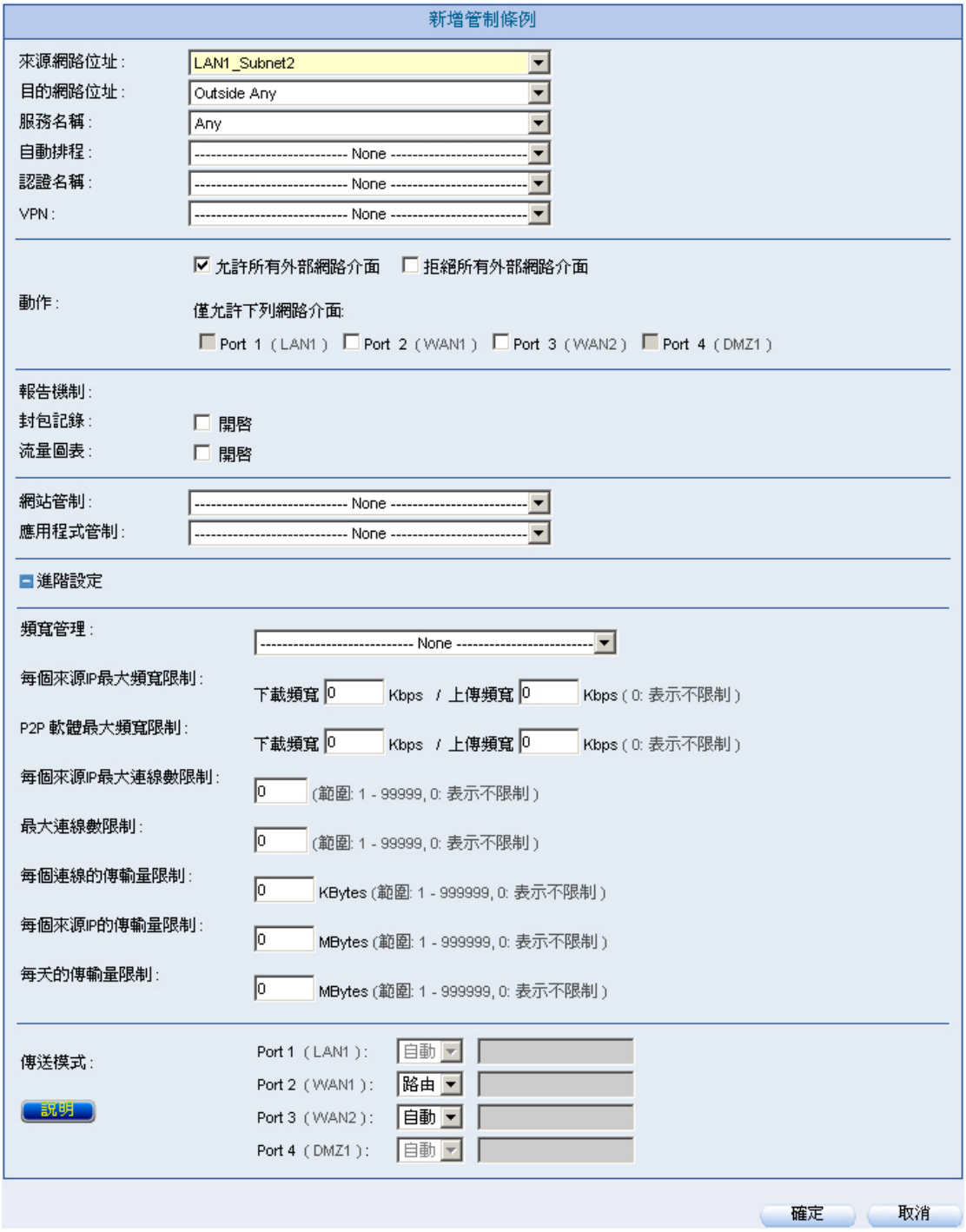


圖 2-15 設定第二筆內部指定網段對外連線模式之管制條例

圖 2-16 完成管制條例設定

步驟5. LAN1 所屬網段對外連線的網路環境。（如圖 2-17）

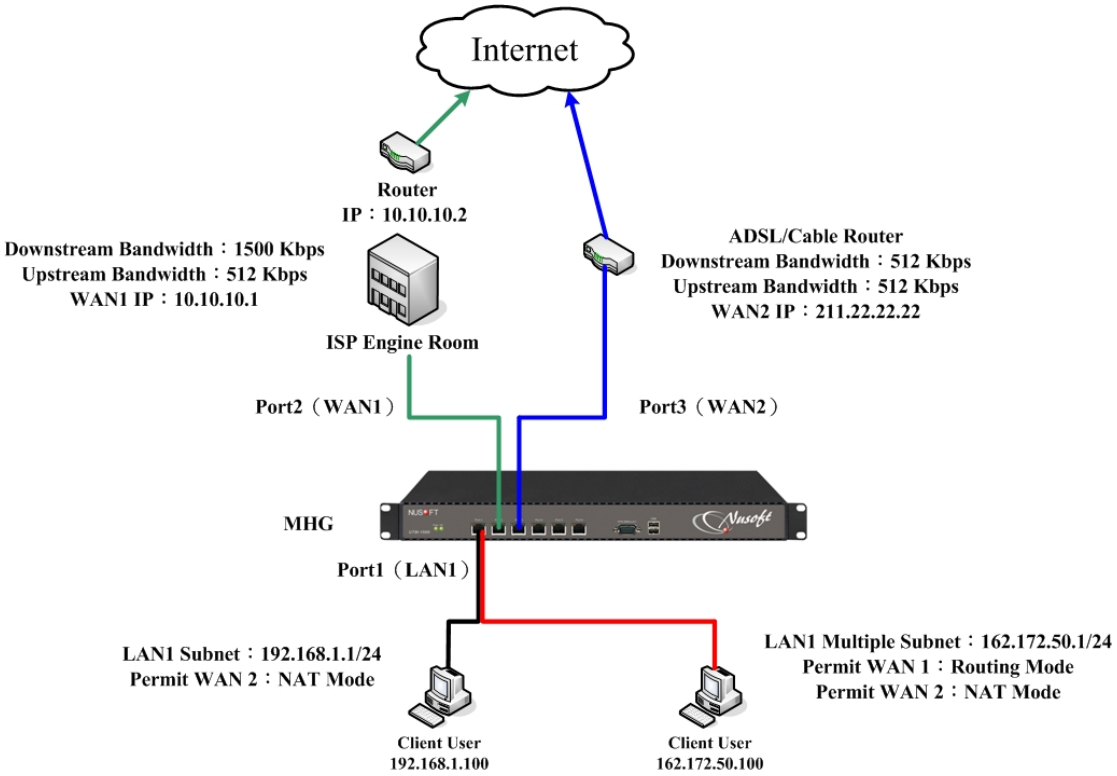


圖 2-17 多重網段對外連線環境

說明：

1. 192.168.1.x/24 網段可透過 WAN1 或 WAN2 以 NAT 模式上網。
2. 162.172.50.x/24 網段可透過 WAN1 以路由模式或 WAN2 以 NAT 模式上網。

2.3.2 透過多重網段建立內部 VLAN 網段之閘道位址，藉以控管 VLAN 存取網路資源權限

環境設定

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

內部網路有 VLAN ID 為 10 的 192.168.100.x/24、VLAN ID 為 20 的 192.168.200.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

Port3 設為 WAN2（211.22.22.22）和 ATU-R 對接，連上網際網路。

步驟1. 在【系統管理】>【組態】>【多重網段】頁面中，做下列設定：

- 按下【新增】鈕。
- 輸入指定的【名稱】。
- 【網路介面】選擇 Port1（LAN1）。
- 【網際協定】選擇 IPv4。
- 【IP 位址】輸入 192.168.100.1。
- 【子網路遮罩】輸入 255.255.255.0。
- 啟動並輸入【VLAN ID】10。
- 按下【確定】鈕。**（如圖 2-18）**
- 再次按下【新增】鈕。
- 輸入指定的【名稱】。
- 【網路介面】選擇 Port1（LAN1）。
- 【網際協定】選擇 IPv4。
- 【IP 位址】輸入 192.168.200.1。
- 【子網路遮罩】輸入 255.255.255.0。
- 啟動並輸入【VLAN ID】20。
- 按下【確定】鈕，完成設定。**（如圖 2-19, 圖 2-20）**

圖 2-18 設定第一筆多重網段

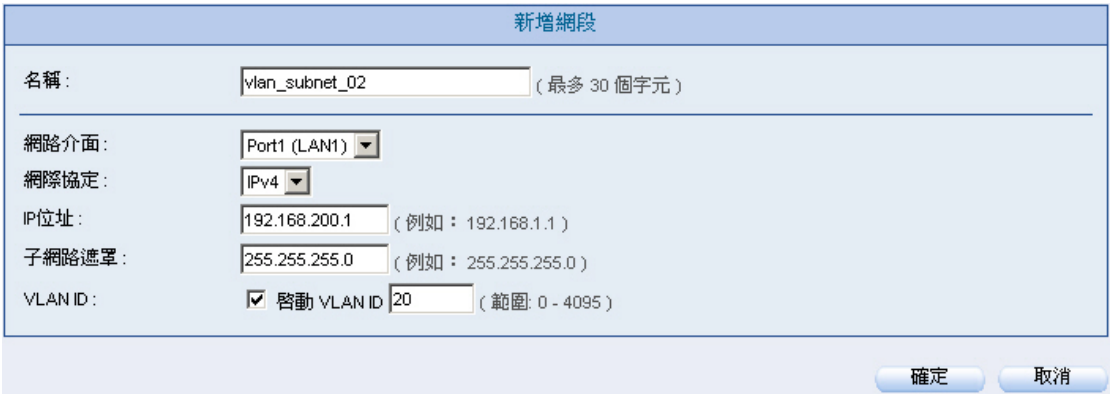


圖 2-19 設定第二筆多重網段

圖 2-20 完成多重網段設定

說明：

1. 可在 MHG-2000 的網路介面上設定多個 VLAN 網段之閘道位址，控管各 VLAN 的 PC 透過 MHG-2000 上網。
2. 若設定的網段或 IP 隸屬於不同的【網路介面】時，要在【管制條例】>【內部至內部】（或【非軍事區至非軍事區】）頁面中，設定一【來源網路位址】為 Inside Any（或 DMZ Any）、【目的網路位址】為 Inside Any（或 DMZ Any）、【服務名稱】為 ANY 的規則，讓內部網路（或非軍事區網路）的電腦可以相互存取。

步驟2. 在【管制條例選項】>【位址表】>【內部網路】頁面中，做下列設定：（如圖 2-21）

圖 2-21 內部網路位址表設定

步驟3. 在【管制條例選項】>【位址表】>【內部網路群組】頁面中，做下列設定：（如圖 2-22）

圖 2-22 內部網路位址群組設定

步驟4. 在【管制條例】>【內部至外部】頁面中，做下列設定：

- 按下【新增】鈕。
- 【來源網路位址】選擇所設定的內部網路位址表規則（VLAN_Group）。
- 按下【確定】鈕，完成設定。**（如圖 2-23, 圖 2-24）**

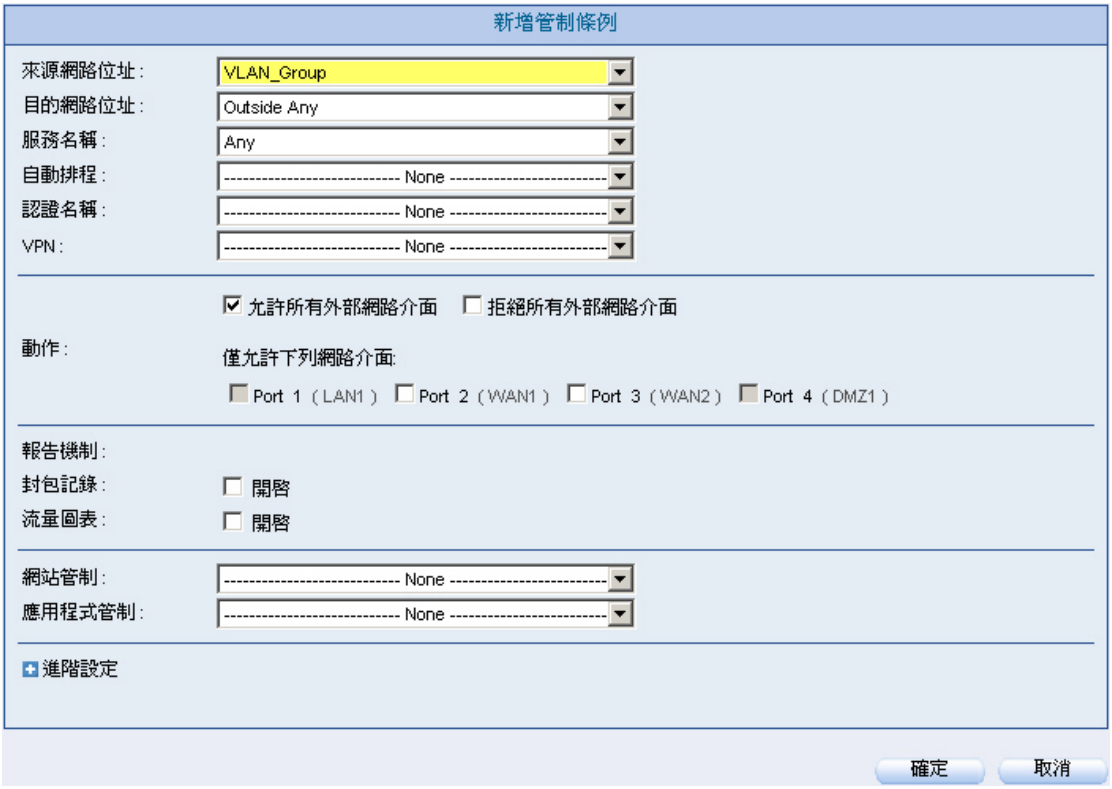


圖 2-23 管制條例套用位址表規則

圖 2-24 完成管制條例設定

步驟5. 內部 VLAN 網路環境。（如圖 2-25）

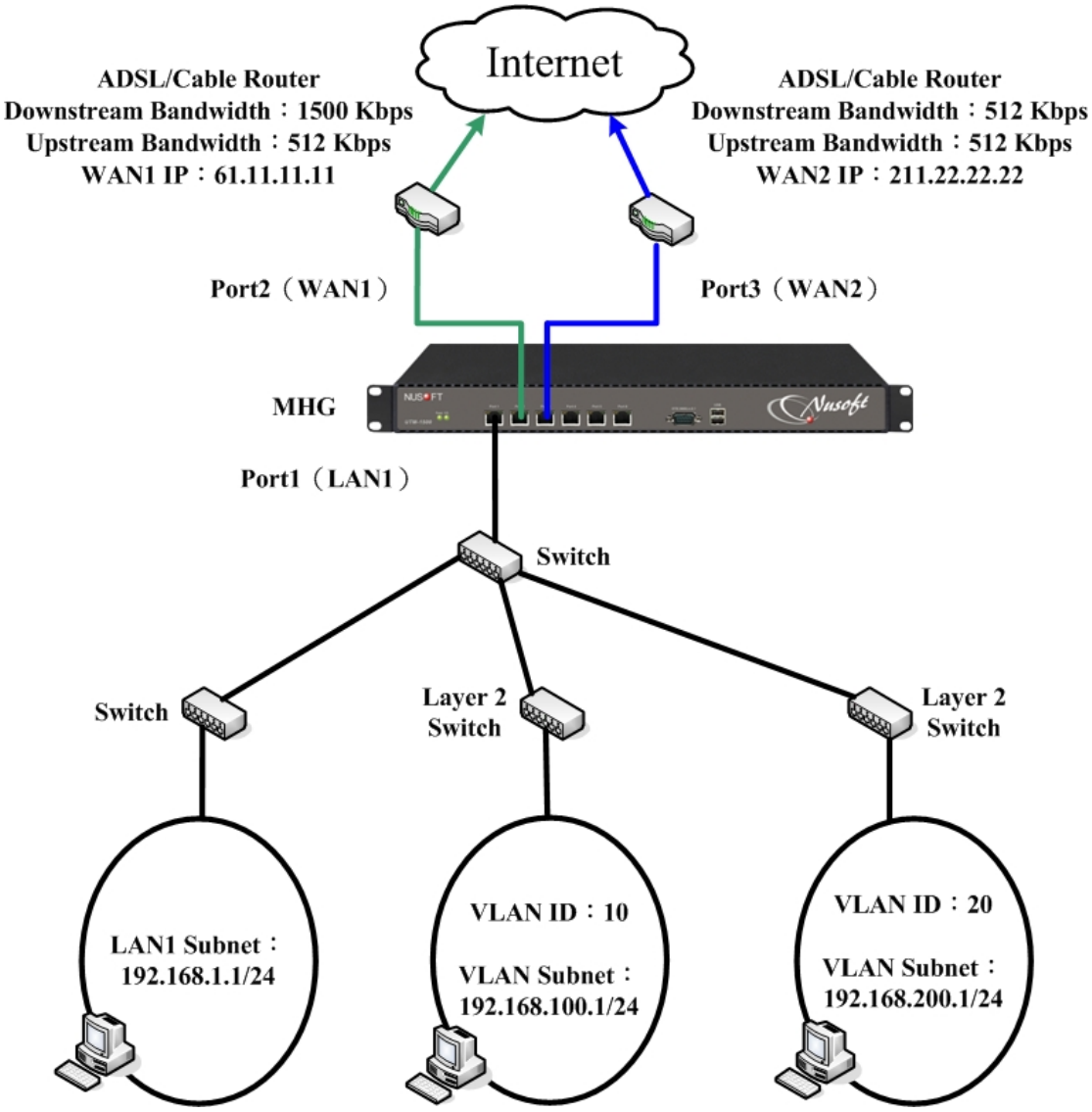


圖 2-25 多重網段 VLAN 網路環境

2.4 指定路由表

2.4.1 使串接於 MHG-2000 下之 Router，將互連的網段透過 MHG-2000 連上網際網路

環境設定

甲公司 Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

內部網路有 Router1（10.10.10.1，支援 RIPv2）和 192.168.10.x/24 網段相連。Router1 與內部網路連接的介面位址為 192.168.1.252。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

Port3 設為 WAN2（211.22.22.22）和 ATU-R 對接，連上網際網路。

乙公司 Router2（10.10.10.2，支援 RIPv2）和 192.168.20.x/24 網段相連。

甲公司 Router1（10.10.10.1）和乙公司 Router2（10.10.10.2）直接以專線相連。

步驟1. 在【系統管理】>【組態】>【指定路由表】頁面的【靜態路由】設定欄位中，做下列設定：

- 按下【新增】鈕。
- 【網際協定】選擇 IPv4。
- 【IP 位址】輸入 192.168.10.0。
- 【子網路遮罩】輸入 255.255.255.0。
- 【閘道位址】輸入 192.168.1.252。
- 【網路介面】選擇 Port1（LAN1）。
- 按下【確定】鈕。**（如圖 2-26）**
- 再次按下【新增】鈕。
- 【網際協定】選擇 IPv4。
- 【IP 位址】輸入 192.168.20.0。
- 【子網路遮罩】輸入 255.255.255.0。
- 【閘道位址】輸入 192.168.1.252。
- 【網路介面】選擇 Port1（LAN1）。
- 按下【確定】鈕。**（如圖 2-27）**
- 再次按下【新增】鈕。
- 【網際協定】選擇 IPv4。
- 【IP 位址】輸入 10.10.10.0。
- 【子網路遮罩】輸入 255.255.255.0。
- 【閘道位址】輸入 192.168.1.252。
- 【網路介面】選擇 Port1（LAN1）。
- 按下【確定】鈕，完成設定。**（如圖 2-28, 圖 2-29）**

圖 2-26 設定第一筆靜態路由

圖 2-27 設定第二筆靜態路由

圖 2-28 設定第三筆靜態路由

圖 2-29 完成靜態路由表設定

注意：

1. 若路由的網段或 IP 隸屬於不同的【介面】時，要在【管制條例】>【內部至內部】(或【非軍事區至非軍事區】)頁面中，設定一【來源網路位址】為 Inside Any (或 DMZ Any)、【目的網路位址】為 Inside Any（或 DMZ Any)、【服務名稱】為 ANY 的規則，讓內部網路（或非軍事區網路）的電腦可以相互存取。

步驟2. 此時 192.168.10.x/24、192.168.20.x/24 和 192.168.1.x/24 網段之電腦可互相連通，且皆可由 MHG-2000 NAT 成真實 IP 連上網網路。（如圖 2-30）

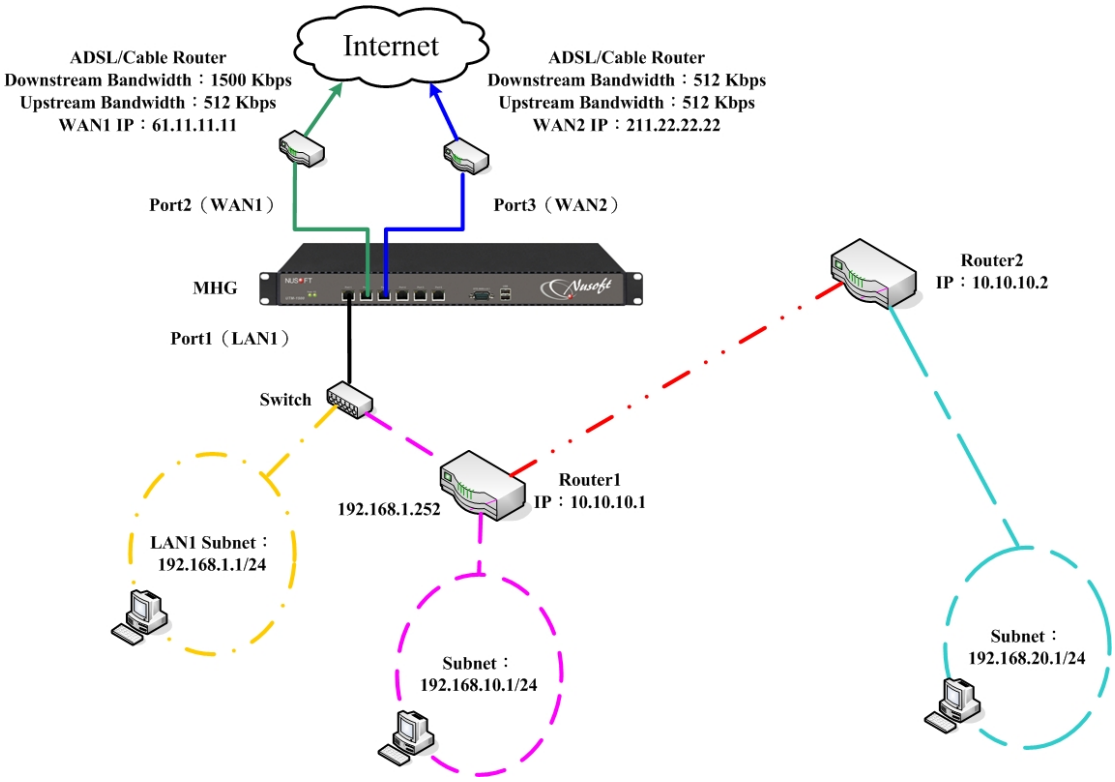


圖 2-30 指定路由表運用環境

2.5 DHCP

2.5.1 透過外部 DHCP 伺服器，配發 IP 給內網 PC

步驟1. 在【系統管理】>【組態】>【DHCP】頁面中，做下列設定：（如圖 2-31）

- 【啟動 DHCP 代轉】功能。
- 選擇【DHCP 代轉介面】。
- 輸入【DHCP 伺服器 IP】位址。
- 按下【確定】鈕，完成設定。

圖 2-31DHCP Relay 設定

說明：

1. 當【啟動 DHCP 代轉】功能時，內部 PC 可透過 MHG-2000【DHCP 代轉介面】向特定的外部 DHCP 伺服器動態取得 IP。

2.5.2 內網 PC 逕向 MHG-2000 取得 IP

步驟1. 在【系統管理】>【組態】>【DHCP】頁面中，做下列設定：（如圖 2-32）

- 選擇【啟動 DHCP】。
- 取消【自動取得 DNS】。
- 輸入欲配發的【IPv4 DNS 伺服器 1】IP 位址。
- 輸入欲配發的【IPv4 DNS 伺服器 2】IP 位址。
- 輸入欲配發的【IPv4 WINS 伺服器 1】IP 位址。
- 輸入欲配發的【IPv4 WINS 伺服器 2】IP 位址。
- 輸入所配發 IP 的【租用時間】，預設為 24 小時。
- 在內部或非軍事區網路介面所屬子網路設定欄位中：
  - 【IP 位址範圍 1】：輸入欲配發的第 1 組可使用之起始 IP 位址和結束 IP 位址，預設為 192.168.1.2 到 192.168.1.254。（須為同一網段）
  - 【IP 位址範圍 2】：輸入欲配發的第 2 組可使用之起始 IP 位址和結束 IP 位址，但必須與【IP 位址範圍 1】為同一網段，且其範圍不可重複。
- 按下【確定】鈕，完成設定。

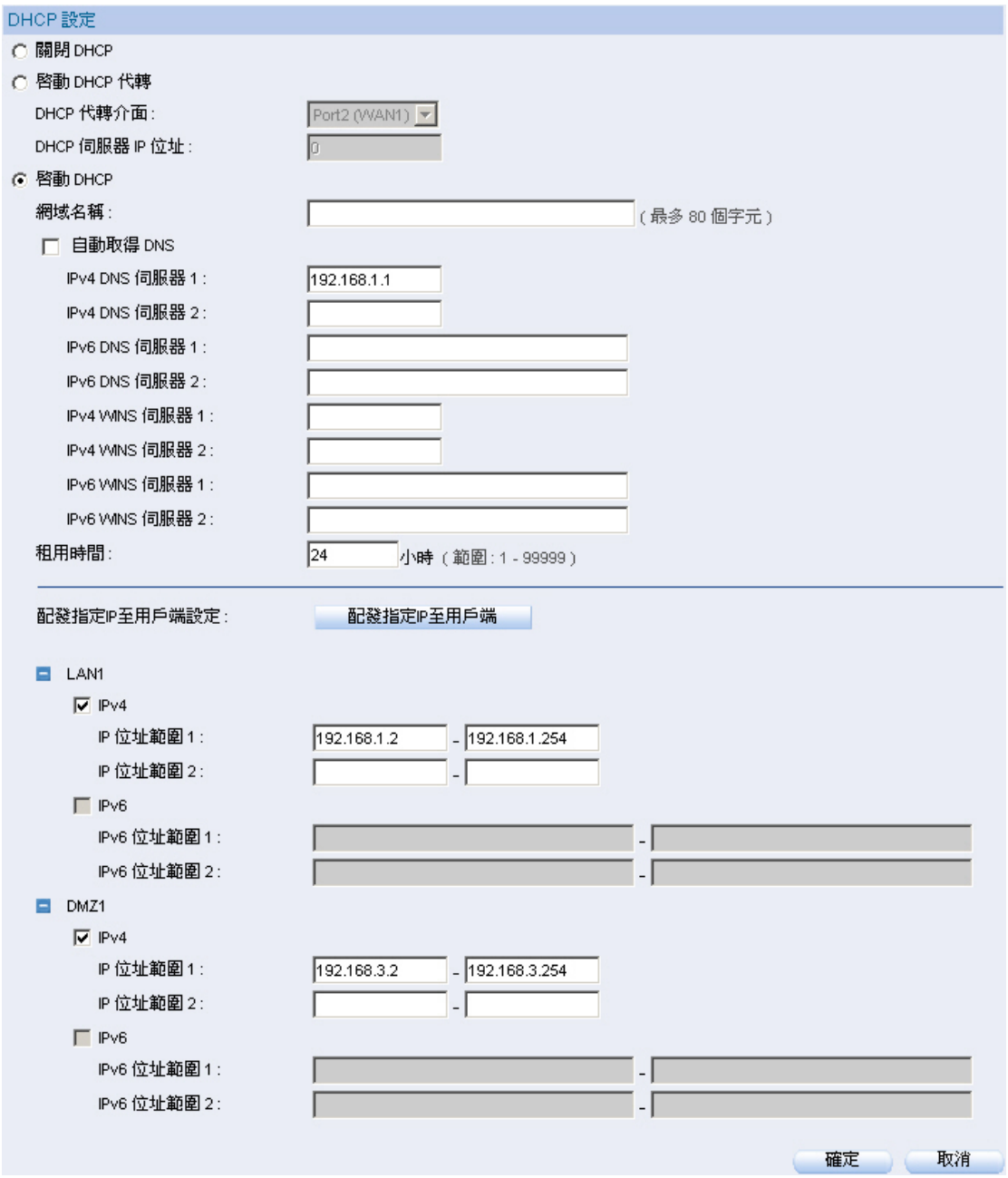


圖 2-32DHCP 設定頁面

說明：

1. 當啟用【自動取得 DNS】功能時，內部 PC 可自動取得 MHG-2000 內部網路介面位址做為 DNS 伺服器位址。(使用場合：內部使用者透過系統認證機制上網時，PC 的第一個(主) DNS 伺服器位址指向 MHG-2000 內部網路介面位址，可自動導向認證頁面。)

2.5.3 MHG-2000 配發指定 IP 給內網 PC

步驟1. 在【系統管理】>【組態】>【DHCP】頁面中，做下列設定：（如圖 2-33）

- 按下【配發指定 IP 至用戶端】鈕。
- 按下【新增】鈕。
- 選擇指定【介面】、【網際協定】。
- 輸入指定【IP 位址】、【MAC 位址】。
- 按下【確定】鈕，完成設定。（如圖 2-34）

圖 2-33 設定 DHCP 配發指定 IP 給內網 PC

圖 2-34 完成 DHCP 配發指定 IP 給內網 PC 設定

說明：

1. 系統管理員可利用點選 填入MAC 的方式，讓 MHG-2000 自動填入指定 IP 位址對應的 MAC 位址。
2. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 MHG-2000【配發指定 IP 至用戶端】位址表錯亂時，可清除規則表重新【匯入】。

2.6 DDNS

步驟1. 在【系統管理】>【組態】>【DDNS】頁面中，做下列設定：（如圖 2-35）

- 選擇【服務提供者】。
- 勾選【自動對應外部網路介面位址】，並選擇所要對應的外部網路介面。
- 輸入所申請的【帳戶名稱】、【密碼】和【網域名稱】。
- 按下【確定】鈕，完成設定。（如圖 2-36）

圖 2-35 設定 DDNS

圖 2-36 完成 DDNS 設定

說明：

1. DDNS 連線狀態圖示說明如下：

圖例			
代表涵義	連線成功	連線失敗	連線中

2. 如未申請 DDNS 帳號，可選擇適合的 DDNS 服務提供者，點擊【註冊去..】進入該服務提供者之註冊網頁。
3. 如無勾選【自動對應外部介面位址】，則可在【外部網路位址】欄位輸入特定之 IP，讓 DDNS 對應至該特定 IP。

2.7 主機名稱表

步驟1. 在【系統管理】>【組態】>【主機名稱表】頁面中，做下列設定：（如圖 2-37）

- 【主機名稱】輸入自訂的網域名稱。
- 【網際協定】選擇 IPv4。
- 輸入所對應之【IP 位址】。
- 按下【確定】鈕，完成設定。

圖 2-37 主機名稱表設定頁面

說明：

1. 使用者 PC 網卡的第一個（主）DNS 伺服器位址設定，一定要為 MHG-2000 的內部或非軍事區網路介面 IP 位址，才能透過 MHG-2000 主機名稱表，以特定的網域名稱連至指定的內部虛擬 IP 位址。

2.8 SNMP

2.8.1 SNMP Agent 設定

步驟1. 在【系統管理】>【組態】>【SNMP】頁面的【SNMP Agent 設定】欄位中，做下列設定：（如圖 2-38）

- 勾選可傳送 SNMP Agent 訊息的網路介面。
- 輸入指定【裝置名稱】(預設為 MHG)、【裝置所在地】、【群組名稱】（預設為 public）、【聯絡人】、【註解】(預設為 MHG appliance)。
- 按下【確定】鈕，完成設定。
- 系統管理員可利用安裝於管理端電腦之 SNMP Agent 訊息接收軟體，隨時監控 MHG-2000 的運作狀況。

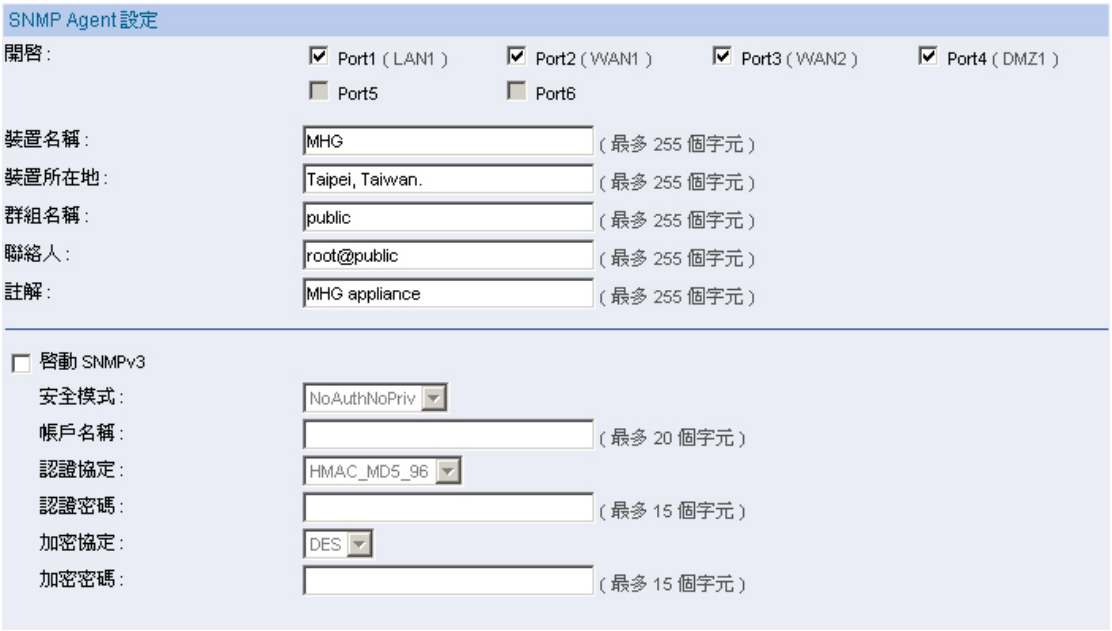


圖 2-38SNMP Agent 設定

2.8.2 SNMP Trap 設定

步驟1. 在【系統管理】>【組態】>【SNMP】頁面的【SNMP Trap 設定】欄位中，做下列設定：（如圖 2-39）

- 勾選【開啟 SNMP Trap 警訊通知】。
- 輸入指定【SNMP Trap 訊息接收位址】、【SNMP Trap 埠號】（預設為 UDP Port 162）。
- 按下【確定】鈕，完成設定。
- 系統管理員可利用安裝於管理端電腦之 SNMP Trap 用戶端軟體，隨時接收來自於 MHG-2000 的異常警訊。

圖 2-39SNMP Trap 設定

說明：

1. 系統管理員可按 Trap 測試 鈕來測試 SNMP Trap 功能是否正常啟用。

2.9 電子佈告欄

2.9.1 透過 MHG-2000 對內部和非軍事區網路的使用者發布公告訊息

步驟1. 在【系統管理】>【組態】>【電子布告欄】頁面的【電子佈告欄連線設定】欄位中，做下列設定：（如圖 2-40）

- 勾選【啟動電子佈告欄管理介面】。
- 輸入指定的【電子佈告欄連線埠號】。
- 輸入登入電子佈告欄管理介面的驗證【帳戶名稱】、【密碼】。
- 輸入指定的【公告提示訊息】。
- 按下【確定】鈕，完成設定。

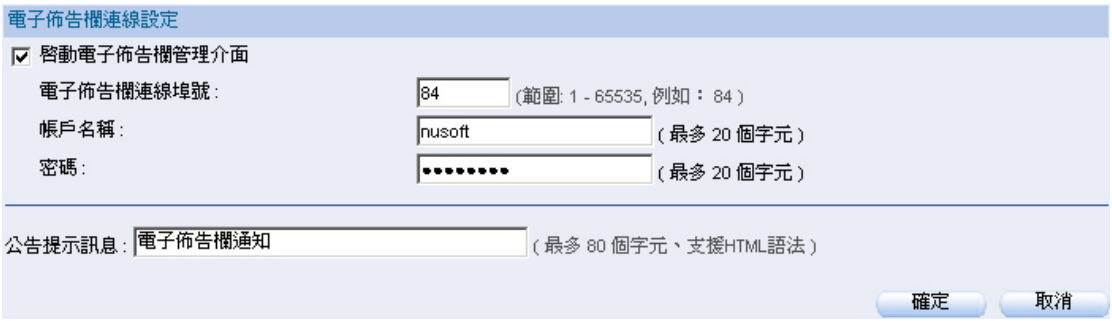


圖 2-40 電子佈告欄連線設定

步驟2. 在【系統管理】>【組態】>【電子布告欄】頁面的【電子佈告欄訊息設定】欄位中，做下列設定：

- 按下【新增】鈕。（如圖 2-41）
- 輸入指定的【公告主旨】。
- 選擇指定的【公告期間】。
- 勾選【內部網路】並選擇 Inside Any、【非軍事區網路】並選擇 DMZ Any 為【公告對象】。
- 輸入欲發布的訊息【內容】。
- 按下【確定】鈕，完成設定。（如圖 2-42）

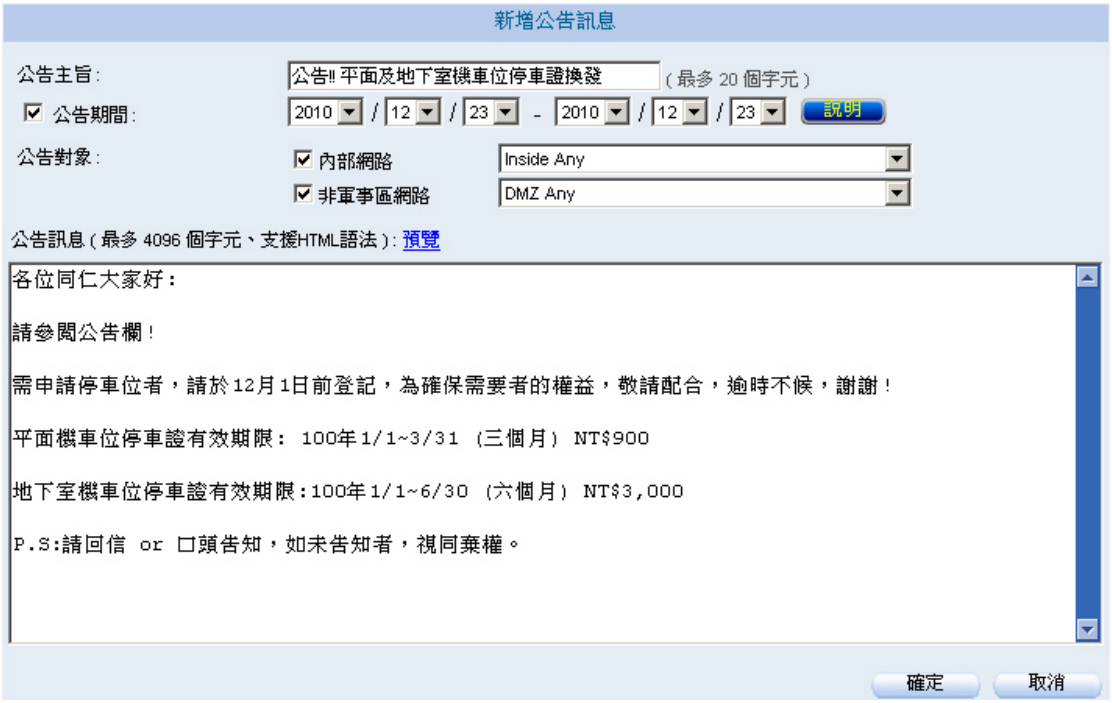


圖 2-41 設定公告訊息

圖 2-42 完成公告訊息設定

說明：

1. 可透過【管制條例選項】>【位址表】>【內部網路】、【內部網路群組】、【非軍事區網路】、【非軍事區群組】來指定【公告對象】。

步驟3. 當內部和非軍事區網路的使用者透過 MHG-2000 存取網頁時，系統會自動發布排程公告。（如圖 2-43, 圖 2-44）

圖 2-43 公告提示訊息顯示於瀏覽網頁的上方

圖 2-44 瀏覽公告內容

說明：

1. 可在【系統管理】>【組態】>【電子布告欄】頁面的【電子佈告欄訊息設定】欄位中，【瀏覽】公告訊息的發布情形。
2. 可讓指定的人員，於瀏覽器網址列輸入 http://MHG-2000 網路介面 IP 位址:所設定的電子佈告欄連線埠號，直接驗證登入【電子佈告欄訊息設定】頁面，以管理欲發布的訊息。**（如圖 2-45，圖 2-46）**

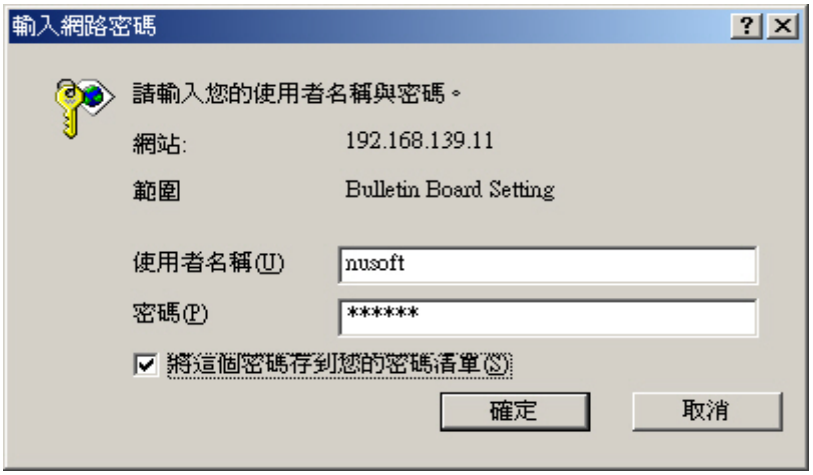


圖 2-45 公告管理頁面登入驗證視窗

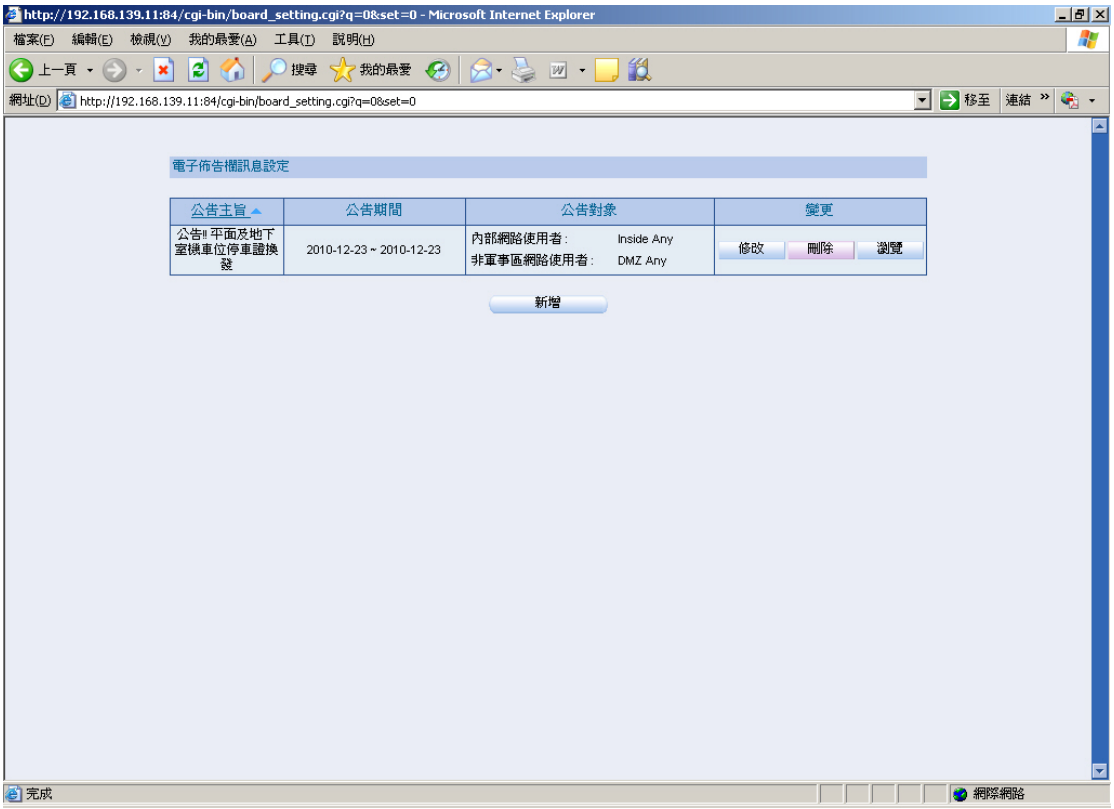


圖 2-46 電子佈告欄訊息設定頁面

2.10 語言版本

2.10.1 選擇語言版本

步驟1. 在【系統管理】>【組態】>【語言版本】頁面中，選擇欲使用之管理介面語言版本，按下【確定】鈕。（如圖 2-47）

圖 2-47 管理介面語言版本設定

網路介面

第3章　網路介面

用來設定 MHG-2000 的網路介面為內部、外部或非軍事區介面位址，及其連線、傳送封包基準。亦可視架設環境的需求將指定介面分組，彼此相互隔絕以分別針對特定區域網段進行網路控管。

【設定】功能概述：

DNS 設定 說明如下：

- 用來定義外部網路介面解析網域名稱時所採用的 DNS 伺服器。

MTU 設定 說明如下：

- 用於設定通過 MHG-2000 傳送的封包最大值，預設值為 1500 Bytes。

記錄到系統的封包 說明如下：

- 可將來源位址或目的位址為 MHG-2000 之封包資訊，記錄在【監控報告】>【監控記錄】>【封包記錄】報表中，以供系統管理員查詢。

連線速率 / 雙工模式設定 說明如下：

- 可藉此設定網路介面與其他設備連接時的傳輸速率和模式。

【介面位址】功能概述：

負載平衡模式 說明如下：

- 自動分配：MHG-2000 依照外部網路下載和上傳頻寬使用情形，會自動調整連外線路的使用率。(適用於採用不同頻寬線路的環境)
- 循環分配：MHG-2000 強制採用 1:1 循環分配網路下載連線。(適用於採用相同頻寬線路的環境)
- 依流量分配：MHG-2000 會依照累積的流量狀態來分配網路下載連線。
- 依連線數分配：MHG-2000 依照使用者設定的飽和連線數來分配對外網路連線。
- 依封包數分配：MHG-2000 會依照累積的封包狀態來分配網路下載連線。
- 線上遊戲模式：判別內部用戶是否已有通過 MHG-2000 對外存取封包的連線，於對外連線全部終止（完成）前，依此連線所走的對外線路，指定後續對外連線路徑。
- 依目的位址分配：判別內部用戶是透過 MHG-2000 的哪條對外線路，和遠端設備建立連線，於終止(完成)所有和同一設備的連線前，維持由此連線路徑，彼此互傳封包。

埠號 說明如下：

- 標示 MHG-2000 所具有的實體網路介面。

介面定義 說明如下：

- 將 MHG-2000 的網路介面，依設定類型由系統自動指定其名稱。

介面類型 說明如下：

- 可將 MHG-2000 的網路介面設定為：
  - 內部網路介面。
  - 外部網路介面。
  - 非軍事區網路介面。
  - 網卡綁定。

內部網路介面模式 說明如下：

- 內部網路有三種模式：
  - NAT / 路由 模式：可設定內部網段（不可和系統已設定、使用的網段相同）及其閘道位址，讓內網電腦的 IP 透過管制條例 NAT 成外部網路介面位址、以本身位址連上網際網路。
  - 透通橋接模式：允許內網電腦根據所採用的閘道位址，透過管制條例以本身 IP 位址，和位於特定網路介面的設備溝通。（在【網路介面】>【介面分組】要做相關設定，該網路介面才會有作用）
  - 透通路由模式：內網電腦可與特定外部網路介面為同一網段，以本身 IP 位址連上網際網路。

IPv4 設定 說明如下：

- 即網際網路協議（Internet Protocol，IP）的第四版，為構成現今網際網路技術基石的協議。
- IP 位址採二進位制，由 32 位元的 0、1 代碼組成，例如：11000000101010000000000100000001；常用點分十進位法來表示 IP 位址（將 32 位元代碼分成 4 組每組 8 位元中間用.分隔，代碼就可以 11000000.10101000.00000001.00000001 表示，其中每組 8 位元代碼稱為一個位元組，一個 IP 位址由 4 個位元組組成；再用十進位法則將 4 組 8 位元代碼用數字來表示，它就變成 192.168.1.1）。
- 可依架設環境所需，適時修改 MHG-2000 網路介面的 IP 位址、子網路遮罩、MAC 位址。

IPv6 設定 說明如下：

- 為次世代網際網路協定（Internet Protocol Next Generation，IPng），主要目的是能與目前版本的 IP (IPv4) 共存，以應付日漸增加的網路、主機數目及資料傳輸量。

- IP 位址採二進位制，由 128 位元的 0、1 代碼組成，例如：00100001110110101001000011010011000000000101000000101111001110110000001010101010000000001111111111111110001010001001110001011010，可以下列方法來表示 IP 位址：
  - 冒號分十六進位法:將 128 位元代碼分成 8 組每組 16 位元中間用:分隔，代碼就可以 0010000111011010:1001000011010011:0000000001010000:0010111100111011:0000001010101010:0000000011111111:1111111000101000:1001110001011010 表示；再用十六進位法則將 8 組 16 位元代碼用數字來表示，它就變成 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A。
  - 壓縮形式：在冒號分十六進位格式中，設為 0 的一串連續 16 位元區塊可壓縮為::，例如：FE80:0:0:0:2AA:FF:FE9A:4CA2 可以壓縮為 FE80::2AA:FF:FE9A:4CA2。
  - 混合形式：
    - IPv4 相容位址：雙堆疊節點使用 IPv4 相容位址 0:0:0:0:0:0:w.x.y.z 或::w.x.y.z(此處 w.x.y.z 是 IPv4 位址的點分十進位表示法)，在 IPv4 基礎結構上與 IPv6 通訊，例如：IPv4 當中的位址 12.34.56.78，在 IPv6 當中成為 0:0:0:0:0:0:12.34.56.78；雙堆疊節點是具有 IPv4 和 IPv6 網際協定的節點，當使用 IPv4 相容位址做為 IPv6 目的位址時，IPv6 通訊自動使用 IPv4 標頭進行壓縮，並使用 IPv4 基礎結構傳送到目的。
    - IPv4 對應位址：0:0:0:0:0:FFFF:w.x.y.z 或::FFFF:w.x.y.z 用來將只用於 IPv4 的節點表示為 IPv6 節點，例如：IPv4 當中的位址 12.34.56.78，在 IPv6 當中成為 0:0:0:0:0:FFFF:12.34.56.78。
- IPv4 建置通常使用點分十進位數字表示前置字元（稱為子網路遮罩）；IPv6 不使用子網路遮罩，只支援前置字元長度表示法。位址中的前置位元定義了特定 IPv6 位址類型，含有這些前置字元的可變長度欄位稱為格式前置字元（Format Prefix，FP），功能有如 IPv4 中的前幾個位元用來代表各 class 分類。
  - 表示 IPv6 位址/前置字元組合的簡潔方法：IPv6 位址/前置字元長度，例如：3FFE:FFFF:0:CD30:0:0:0:0/64，前置字元是 3FFE:FFFF:0:CD30，表示成壓縮形式為 3FFE:FFFF:0:CD30::/64；帶有前置字元的節點位址可用於衍生子網路識別碼，例如：21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/64，所衍生的子網路識別碼為 21DA:D3:0:2F3B::/64。

- ◆ 可以沿位元邊界定義前置字元，但 IPv6 位址的冒號分十六進位表示法以半位元組（4 位元）為界，要正確表示一個字首長度不是 4 的倍數的子網路，必須將十六進位轉換為二進位，才能確定適當的子網路識別碼。例如：要表示位址和字首為 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/59 的子網路，就必須將 2F3B 中的 3 轉換為二進位（0011），在第 3 個和每 4 個二進位數字之間畫分半位元組，然後轉換回到十六進位，結果子網路識別碼為 21DA:D3:0:2F20::/59。

■ 資料傳輸位址有三種：

- ◆ 單點傳送（Unicast）位址：
  - ● 連結-本機位址：格式為 FE80::InterfaceID，主要用在設備啟動系統尚未取得大範圍的位址時。相當於 Microsoft Windows 系統上使用 169.254.0.0/16 前置字元自動組態的 IPv4 位址。
  - ● 站台-本機位址：格式為 FEC0::SubnetID:InterfaceID，主要是用在站台內定址，不需要具有全域前置字元；相當於 IPv4 專用位址空間（10.0.0.0/8、172.16.0.0/12 和 192.168.0.0/16）。
  - ● 全域 IPv6 單點傳送位址：可在網際網路上進行全域路由和連線，與公用 IPv4 位址相同；其格式為 001（FP，3 位元）TLA ID（13 位元）保留位置（8 位元）NLA ID（24 位元）SLA ID（16 位元）InterfaceID（64 位元）。
- ◆ 多點傳送（Multicast）位址：供介面組使用的識別碼（通常分屬不同節點），傳送到此位址的封包會被送到以此位址識別的所有介面，多點傳送位址類型會取代 IPv4 廣播位址；其二進位制前置字元為 11111111，以冒號分十六進位法表示 IPv6 為 FF00::/8，例如：多重廣播所有節點的位址 FF02::1、多重廣播所有路由器的位址 FF02::2。
- ◆ 任意傳送（Anycast）位址：可以指定給多個介面，而封包根據路徑協定會傳送給最近的介面；典型的使用是用來辨識一組的路由器（在 ISP 中），當封包到達 ISP 時會送到最近的路由器處理。

說明：

1. EUI-64 轉換到 IPv6 介面識別碼：

- ■ Ethernet MAC 位址 00-AA-00-3F-2A-1C，在第 3 和第 4 個位元組之間插入 FF-FE 轉換為 EUI-64 格式，結果是 00-AA-00-FF-FE-3F-2A-1C。
- ■ 對 U/L 位元（它是第 1 個位元組的第 7 位元）進行取補數操作，第 1 個位元組的二進位元格式為 00000000，對第 7 位元取補數後它就變成 00000010（0x02）。

- 最終結果是 02-AA-00-FF-FE-3F-2A-1C，以冒號分十六進位法表示為 2AA:FF:FE3F:2A1C；與 MAC 位址為 00-AA-00-3F-2A-1C 的網路配接卡對應的連結-本機位址是 FE80::2AA:FF:FE3F:2A1C。

MAC 位址 說明如下：

- 可依架設環境所需，適時修改 MHG-2000 網路介面的 MAC 位址。

啟動任意 IP 路由 說明如下：

- 讓電腦只需要插上網路線，不需要變更設備原先的 IP 位址、子網路遮罩、預設閘道、DNS 伺服器...設定，就可以直接上網。
- 可減少使用者修改設備網路組態的困擾，另一方面管理者也不需到處協助使用者設定網路。

注意：

1. 任意 IP 路由僅適用於飯店、酒店、賓館、旅社、民宿...旅館業者，提供網路服務給旅客使用時。
2. 任意 IP 路由並不適合在一般企業環境中啟用。且使用者 PC 的 IP 若恰巧重複時，會有 IP 衝突的可能。

說明：

1. 當網路介面採用內部網路模式時，才有任意 IP 路由功能。

Ping / Tracert 說明如下：

- 讓使用者可 Ping/Tracert 到該網路介面之 IP 位址，以確認 MHG-2000 在運作中。

HTTP 說明如下：

- 讓使用者可透過該網路介面之 IP 位址，以 HTTP 協定登入 MHG-2000 之 Web UI。

HTTPS 說明如下：

- 讓使用者可透過該網路介面之 IP 位址，以 HTTPS 協定登入 MHG-2000 之 Web UI。

Telnet 說明如下：

- 讓使用者可透過該網路介面之 IP 位址，以 Telnet 協定登入 MHG-2000。

SSH 說明如下：

- 讓使用者可透過該網路介面之 IP 位址，以 SSH 協定登入 MHG-2000。

外部網路連線模式 說明如下：

- 外部網路介面連線模式可分為：
  - 固定 IP 位址。
  - 動態 IP 位址（纜線數據機使用者）。
  - 撥號連線（ADSL 撥接使用者）。

連線偵測 說明如下：

- 測試該外部網路介面是否成功連線。測試之方法，分為下列兩種：
  - ICMP：以 Ping 所設定的 IP 位址來測試是否成功連線。
  - DNS：以查詢指定網域名稱來測試是否成功連線。

NAT 模式 說明如下：

- 用來轉換內部網路連上網際網路採用的外部網路 IP 位址：
  - 自動化模式：轉換為目前外部網路介面連線的 IP 位址。
  - 指定 IP 位址：轉換為目前外部網路介面連線允許的任一 IP 位址。

最大下載頻寬＆上傳頻寬 說明如下：

- 系統管理員必須在此設定該外部網路介面的正確頻寬，以做為 MHG-2000 運作的依據。

閒置時間 說明如下：

- 系統管理員在外部網路介面採用撥號連線（ADSL 撥接使用者）模式時，可輸入當該條線路未被使用的情況下，多久之後自動斷線的時間（單位：分鐘）。

非軍事區介面模式 說明如下：

- 和內部網路一樣分為 NAT / 路由、透通橋接、透通路由三種模式。

網卡綁定 說明如下：

- 用來將指定的 MHG-2000 實體連接埠結合成一個邏輯連接埠，以此整合各連接埠的傳輸速率提升網路資料傳送速度。

綁定介面 說明如下：

- 用來設定欲結合的內部、外部或非軍事區網路介面。

綁定模式 說明如下：

- 網卡綁定有三種模式：
  - 循環分配模式：會依序使用綁定的連接埠，其中一個連接埠失效仍可持續運作，所連接的 switch 需支援 Port Trunk 或是 Link Aggregation 設定才能發揮實質效果。
  - 備援模式：同一時間內只有一個綁定的連接埠運作，當此連接埠失效時會自動啟用次一順位的連接埠，不需所連接 switch 的設定支援。
  - 鏈路匯整（IEEE 802.3ad）模式：合併綁定連接埠的頻寬，並具有備援機制與容錯的功能，其中一個連接埠失效仍可持續運作，所連接的 switch 需支援 IEEE 802.3ad 功能才能發揮實質效果。

偵測模式 說明如下：

- 在採用循環分配、備援模式綁定網卡時，可以網路埠連結狀態、發送 ARP 至另一端點介面位址，來偵測網路介面的斷、連線。

飽和連線數 說明如下：

- 在負載平衡模式為依照流量、連線數或是封包數的情況下，可在此設定外部網路介面循環分配之連線比例。

優先權 說明如下：

- 設定外部網路介面連線分配的優先權。

【虛擬外部網路】功能概述：

i 說明如下：

- 虛擬外部網路介面連線狀態。

名稱 說明如下：

- 虛擬外部網路介面辨識名稱。

介面 說明如下：

- 用於設定虛擬外部網路介面隸屬的實體外部網路介面。

說明：

1. 當實體外部網路介面採用固定 IP 連線模式時，才可設定虛擬外部網路介面。
2. 虛擬外部網路介面僅支援固定 IP 連線模式。
3. 可利用虛擬外部網路介面設定【管制條例】>【內部至外部】、【非軍事區至外部】和【管制條例選項】>【虛擬伺服器】>【IP 對應】、【連接埠對應】規則。
4. 透過指定實體外部網路介面和所屬虛擬外部網路介面上網時，會循環分配相關連線需求。

【介面分組】功能概述：

介面分組 說明如下：

- 當 MHG-2000 同時有內部或非軍事區網路類型並採用透通橋接模式、外部網路類型並採用固定 IP 連線的網路介面；此時，可將這些網路介面分組，讓各組介面分隔運作。
- 當 MHG-2000 有採用透通路由模式的網路介面時，會透過設定為內部或非軍事區網路類型的介面，將對外連線的來源位址直接轉換為外部網路介面的 IP 位址。

3.1 網路介面功能使用範例

編碼	範例環境	頁碼
3.1.1	更改內部網路介面位址（NAT / 路由模式）	**84**
3.1.2	設定外部網路介面位址	**85**
3.1.3	以MHG-2000 做為閘道器，設定兩個內部（NAT / 路由模式）網路介面，分別連接兩個不同網段的使用者電腦，管理存取網路資源權限	**91**
3.1.4	以MHG-2000 做為閘道器，於設定為內部（NAT / 路由模式）網路的介面連接使用者電腦，存取網際網路資源；於設定為非軍事區（透通路由模式）網路的介面連接伺服器，對外提供服務	**94**
3.1.5	將MHG-2000 置於原有的閘道器和內部網路（有兩個不同網段）之間，設定兩個內部（一個採透通路由模式，另一個採NAT / 路由模式）網路介面，分別連接原有內部網路的兩個不同網段，管理存取網路資源權限	**97**
3.1.6	將MHG-2000 置於原有的閘道器和內部網路之間，於設定為內部（NAT / 路由模式）網路的介面連接使用者電腦、設定為非軍事區（透通橋接模式）網路的介面連接原有內部網路，管理存取網路資源權限	**100**
3.1.7	將MHG-2000 置於原有的閘道器和內部網路、非軍事區網路之間，分別加強管理原有閘道器內部網路、非軍事區網路存取網路資源權限	**107**
3.1.8	以MHG-2000 做為閘道器，設定兩個內部（一個採NAT / 路由模式，另一個採透通橋接模式）網路介面，分別連接不同部門的使用者電腦，管理存取網路資源權限	**113**
3.1.9	將MHG-2000 置於原有的閘道器和內部網路之間，於設定為內部（NAT / 路由模式）網路和所屬綁定的介面連接原有內部網路、設定為外部（固定IP位址連線模式）網路和所屬綁定的介面連接使用者電腦，增加彼此資料傳輸量	**118**
3.1.10	以MHG-2000 做為閘道器，設定一個外部（固定IP位址連線模式）網路介面和所屬虛擬網路介面，將不同的上網線路連接到同一實體網路埠，同時處理網路連線需求	**124**

3.1.1 更改內部網路介面位址（NAT / 路由模式）

環境設定

Port1 為系統預設的內部網路介面 LAN1（192.168.1.1，NAT / 路由模式）。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-1）

- 選擇【埠號】1，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入新的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-1 內部網路介面位址設定頁面

說明：

1. MHG-2000 的預設內部網路介面網段為 192.168.1.x/24。系統管理員在更動內部網路介面網段後，內部電腦必須更改 IP 位址，使其隸屬於變更後的網段。這樣才可再次以變更後的 MHG-2000 內部網路介面位址登入 Web UI。
2. 在尚未設定【系統管理】>【管理】>【管理位址】之前，千萬不要關閉 HTTP 和 HTTPS 系統管理功能。這會導致系統管理員無法從內部網路登入 MHG-2000 之 Web UI。

3.1.2 設定外部網路介面位址

步驟1. 在【網路介面】>【介面位址】頁面中，按下【埠號】2 的【修改】鈕，並選擇外部網路【介面類型】。

步驟2. 設定【連線偵測】方式（有 ICMP 和 DNS 兩種方式）：

- 【ICMP】：輸入可持續 Ping 之外部 IP 位址。**（如圖 3-2）**
- 【DNS】：輸入欲連線的【DNS 伺服器 IP 位址】，與欲解析的【網域名稱】。**（如圖 3-3）**
- 設定發送測試連線封包之間隔秒數。

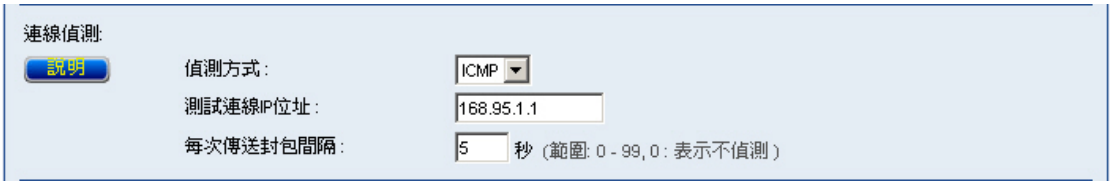


圖 3-2ICMP 連線偵測

圖 3-3DNS 連線偵測

注意：

1. 【連線偵測】為 MHG-2000 在偵測該外部網路是否暢通的依據。故在【連線偵測】中所設定之【測試連線 IP 位址】、【DNS 伺服器 IP 位址】和【網域名稱】皆必須永久運作。否則會造成 MHG-2000 的判斷錯誤。

步驟3. 選擇【外部網路連線模式】:

- 固定 IP 位址：（如圖 3-4）
  - 輸入 ISP 提供連線的【IPv4 位址】、【子網路遮罩】和【IPv4 預設閘道】。
  - 輸入【最大下載頻寬】及【最大上傳頻寬】。（依照申請的網路頻寬做設定）
  - 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
  - 按下【確定】鈕，完成設定。（如圖 3-5）
- 動態 IP 位址（纜線數據機使用者）:（如圖 3-6）
  - 按下【IP 位址】欄位右方的【更新】鈕，即可自動取得 IP。
  - 若 ISP 要求依據 MAC 位址建立連線，則可按下【MAC 位址】欄位右方的【填入 MAC】鈕，來自動取得本機 MAC 位址。
  - 【用戶名稱】: 某些 ISP 要求輸入配發的帳號名稱。
  - 【網域名稱】: 某些 ISP 要求輸入配發的網域名稱。
  - 輸入【最大下載頻寬】及【最大上傳頻寬】。（依照申請的網路頻寬做設定）
  - 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
  - 按下【確定】鈕，完成設定。（如圖 3-7）
- 撥號連線 (ADSL 撥接使用者)：（如圖 3-8）
  - 輸入連線的驗證【帳戶名稱】。
  - 輸入連線的驗證【密碼】。
  - 【ISP 提供的 IP 位址類型】選擇動態模式。（依使用者情況而定，一般皆採用預設的動態模式）
  - 輸入【最大下載頻寬】及【最大上傳頻寬】。（依照申請的網路頻寬做設定）
  - 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
  - 按下【確定】鈕，完成設定。（如圖 3-9）

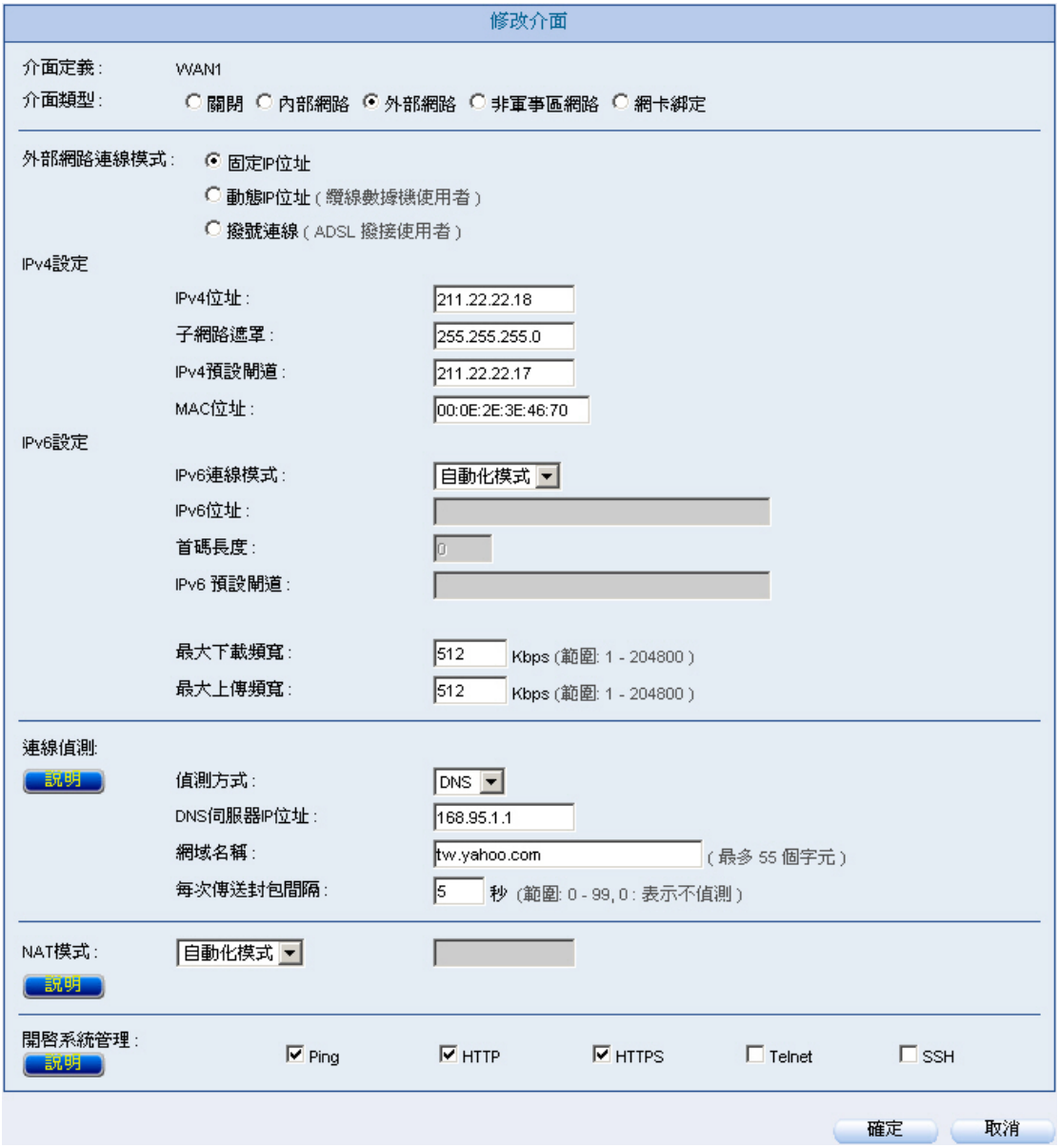


圖 3-4 設定固定 IP 位址連線

埠號	名稱	傳送模式	IP位址 / 子網路遮罩	飽和連線數	變更	優先權
1	LAN1	NAT	192.168.1.1 / 255.255.255.0	---	修改	---
2	WAN1	固定IP	211.22.22.18 / 255.255.255.248	---	修改	1
3	Port3	---	0.0.0.0 / 0.0.0.0	---	修改	---
4	Port4	---	0.0.0.0 / 0.0.0.0	---	修改	---
5	Port5	---	0.0.0.0 / 0.0.0.0	---	修改	---
6	Port6	---	0.0.0.0 / 0.0.0.0	---	修改	---
7	Port7	---	0.0.0.0 / 0.0.0.0	---	修改	---

圖 3-5 完成固定 IP 位址連線設定

圖 3-6 設定動態 IP 位址連線

埠號	名稱	傳送模式	IP位址 / 子網路遮罩	飽和連線數	變更	優先權
1	LAN1	NAT	192.168.1.1 / 255.255.255.0	---	修改	---
2	WAN1	動態IP	210.33.241.25 / 255.255.255.255	---	修改	1
3	Port3	---	0.0.0.0 / 0.0.0.0	---	修改	---
4	Port4	---	0.0.0.0 / 0.0.0.0	---	修改	---
5	Port5	---	0.0.0.0 / 0.0.0.0	---	修改	---
6	Port6	---	0.0.0.0 / 0.0.0.0	---	修改	---
7	Port7	---	0.0.0.0 / 0.0.0.0	---	修改	---

圖 3-7 完成動態 IP 位址連線設定

圖 3-8 設定撥號連線

埠號	名稱	傳送模式	IP位址 / 子網路遮罩	飽和連線數	變更	優先權
1	LAN1	NAT	192.168.1.1 / 255.255.255.0	---	修改	---
2	WAN1	撥號連線	61.228.189.205 / 255.255.255.255	---	修改	1
3	Port3	---	0.0.0.0 / 0.0.0.0	---	修改	---
4	Port4	---	0.0.0.0 / 0.0.0.0	---	修改	---
5	Port5	---	0.0.0.0 / 0.0.0.0	---	修改	---
6	Port6	---	0.0.0.0 / 0.0.0.0	---	修改	---
7	Port7	---	0.0.0.0 / 0.0.0.0	---	修改	---

圖 3-9 完成撥號連線設定

說明：

1. 可在【網路介面】>【設定】頁面的【DNS 設定】欄位中，指定外部網路介面採用的 DNS 伺服器。
2. 當在外部網路介面中【開啟系統管理】的 Ping/Tracert、HTTP、HTTPS、Telnet 和 SSH 功能時，使用者將可從外部網路 Ping/Tracert 到 MHG-2000 與登入 MHG-2000 的 Web UI。這有可能會影響到網路的安全性。故建議系統管理員在確定所有設定無虞後，關閉 Ping/Tracert、HTTP、HTTPS、Telnet 和 SSH 等系統管理功能。若是系統管理員需從外部網路登入 Web UI，則可利用【系統管理】>【管理】>【管理位址】設定允許登入 Web UI 的特定外部 IP 位址。

3.1.3 以 MHG-2000 做為閘道器，設定兩個內部（NAT / 路由模式）

網路介面，分別連接兩個不同網段的使用者電腦，管理存取網路資源

權限

環境設定

Port1 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。
Port2 設為 LAN1（192.168.1.1，NAT / 路由模式）為 192.168.1.x/24 網段，連接的使用者電腦轉址為 WAN1（61.11.11.11）存取網際網路資源。
Port3 設為 LAN2（192.168.2.1，NAT / 路由模式）為 192.168.2.x/24 網段，連接的使用者電腦轉址為 WAN1（61.11.11.11）存取網際網路資源。
接於 LAN1 和 LAN2 的電腦需透過管制條例互通。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-10）

- 選擇【埠號】2，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-10 內部網路介面 1 位址設定頁面

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-11）

- 選擇【埠號】3，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-11 內部網路介面 2 位址設定頁面

步驟3. 接於 LAN1、LAN2 的使用者電腦，皆轉換成 WAN1 真實 IP 位址（61.11.11.11）存取網際網路資源；彼此需透過管制條例互通。（如圖 3-12）

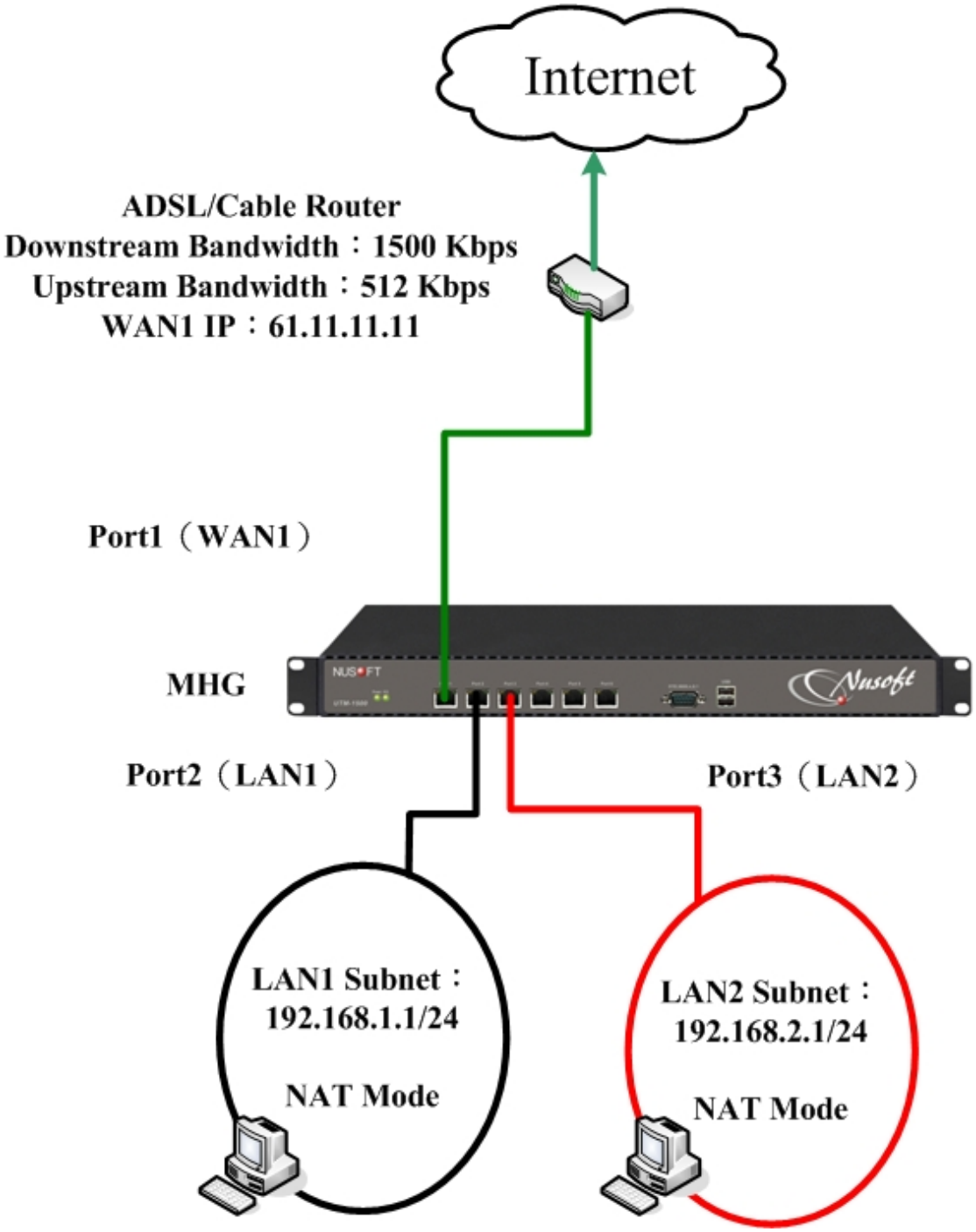


圖 3-12 內部網路 NAT / 路由模式適用環境

3.1.4 以 MHG-2000 做為閘道器，於設定為內部（NAT / 路由模式）

網路的介面連接使用者電腦，存取網際網路資源；於設定為非軍事區

（透通路由模式）網路的介面連接伺服器，對外提供服務

環境設定

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

內部網路電腦（192.168.1.100）轉址為 WAN1（61.11.11.11）來存取網際網路資源。

Port3 設為 DMZ1（透通路由模式）連接對外服務的伺服器（採用 WAN1 線路 ISP 配發的可用真實 IP 位址 61.11.11.12）。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-13）

- 選擇【埠號】1，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-13 內部網路介面位址設定頁面

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-14）

- 選擇【埠號】3，按下【修改】鈕。
- 【介面類型】選擇非軍事區網路。
- 【非軍事區介面模式】選擇透通路由模式。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-14 非軍事區網路透通路由模式設定頁面

說明：

1. 一定要有【外部網路】介面採用固定 IP 位址連線，【非軍事區網路】介面方可選擇透通模式。

步驟3. 接於非軍事區網路介面的伺服器，以 ISP 配發的真實 IP 位址（61.11.11.12）對外服務。接於內部網路介面的使用者電腦，轉換成 WAN1 真實 IP 位址（61.11.11.11）存取網際網路資源。（如圖 3-15）

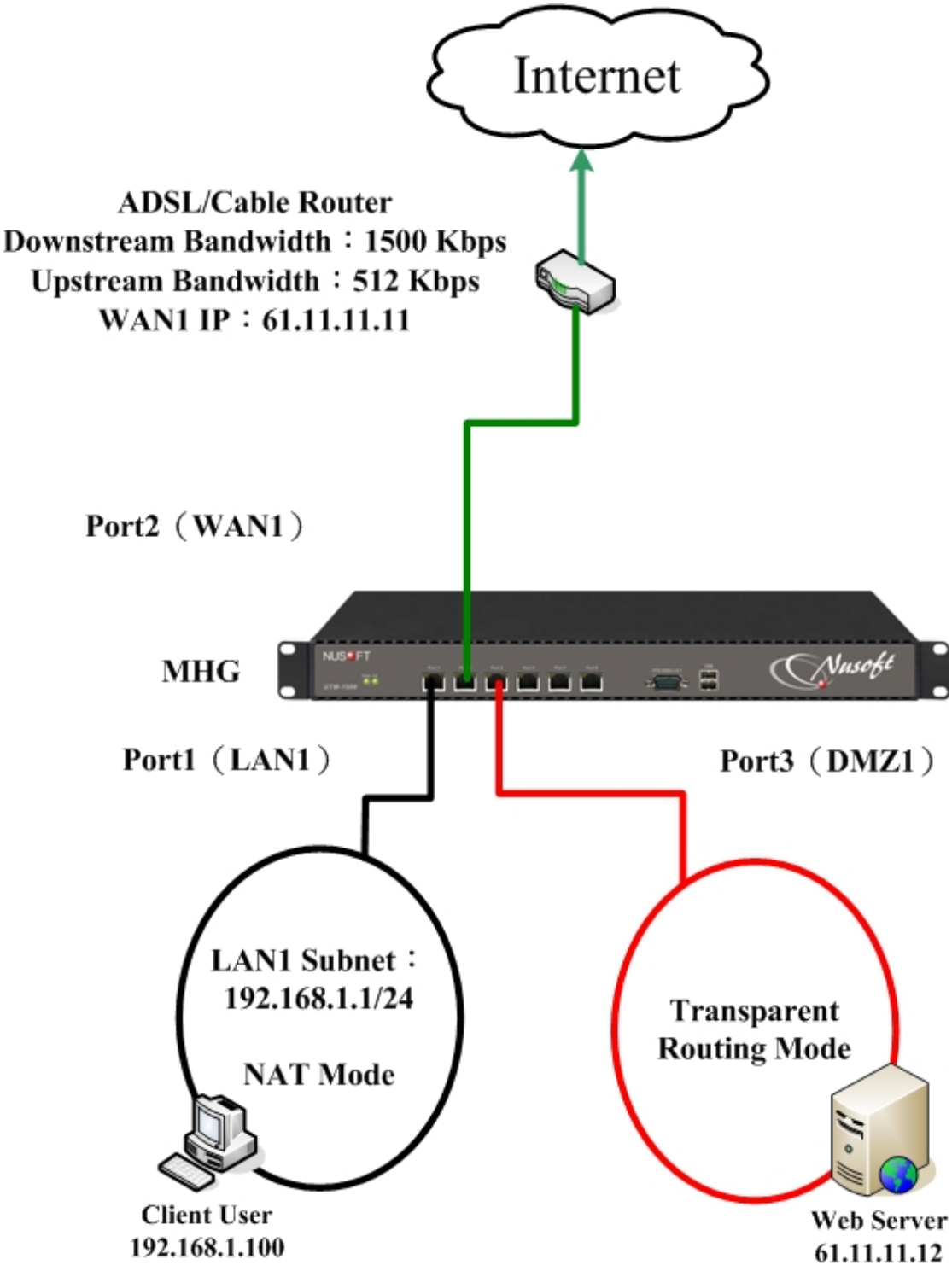


圖 3-15 非軍事區網路透通路由模式適用環境

3.1.5 將 MHG-2000 置於原有的閘道器和內部網路（有兩個不同網段）之間，設定兩個內部（一個採透通路由模式，另一個採 NAT / 路由模式）網路介面，分別連接原有內部網路的兩個不同網段，管理存取網路資源權限

環境設定

原有閘道器之 LAN 有 192.168.1.x/24（閘道位址為 192.168.1.1）、192.168.2.x/24（閘道位址為 192.168.2.1）網段。

Port1 設為 WAN1（192.168.1.2）和原有閘道器之 LAN 對接。

將原有閘道器 192.168.2.x/24 網段以一指定路由取代，讓所有要到 192.168.2.x/24 網段的封包皆傳送至 WAN1。

Port2 設為 LAN1（透通路由模式）連接原有內部網路電腦（隸屬於 192.168.1.x/24 網段，網卡的預設閘道皆設為 192.168.1.1），直接以本機 IP 位址經原有閘道器轉換為真實 IP 位址存取網際網路資源。

Port3 設為 LAN2（192.168.2.1，NAT / 路由模式）為 192.168.2.x/24 網段，連接的使用者電腦（網卡的預設閘道皆設為 192.168.2.1），直接以本機 IP 位址經原有閘道器轉換為真實 IP 位址存取網際網路資源。

接於 LAN1 和 LAN2 的電腦需透過管制條例互通。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-16）

- 選擇【埠號】2，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇透通路由模式。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-16 內部網路介面 1 位址設定頁面

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-17）

- 選擇【埠號】3，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-17 內部網路介面 2 位址設定頁面

步驟3. 接於 LAN1（隸屬於 192.168.1.x/24 網段）、LAN2（隸屬於 192.168.2.x/24 網段）的使用者電腦透過 MHG-2000 控管，直接以本機 IP 位址經原有閘道器轉換為真實 IP 位址上網；彼此需透過管制條例互通。（如圖 3-18）

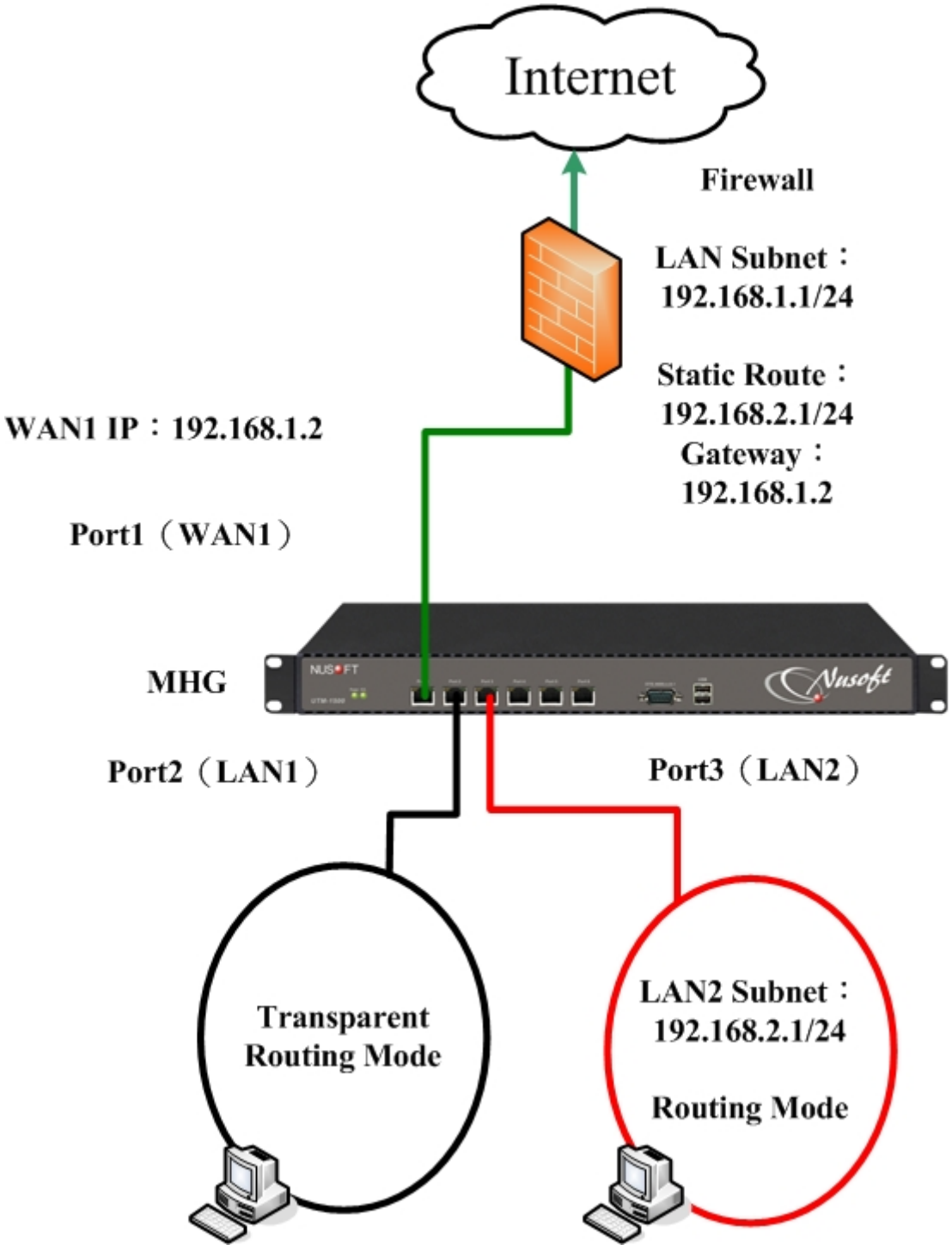


圖 3-18 內部網路透通路由、NAT / 路由模式適用環境

3.1.6 將 MHG-2000 置於原有的閘道器和內部網路之間，於設定為內部（NAT / 路由模式）網路的介面連接使用者電腦、設定為非軍事區（透通橋接模式）網路的介面連接原有內部網路，管理存取網路資源權限

環境設定

原有閘道器之 LAN（172.16.1.1）為 172.16.x.x/16 網段。

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）為 192.168.1.x/24 網段，連接的使用者電腦(網卡的預設閘道皆設為 192.168.1.1)轉址為 WAN1(172.16.1.12)，經原有閘道器轉換為真實 IP 位址存取網際網路資源。

Port2 設為 WAN1（172.16.1.12）和原有閘道器之 LAN 對接。

Port3 設為 DMZ1（透通橋接模式）連接原有內部網路電腦（隸屬於 172.16.x.x/16 網段，網卡的預設閘道皆設為 172.16.1.1)，直接以本機 IP 位址經原有閘道器轉換為真實 IP 位址存取網際網路資源。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-19）

- 選擇【埠號】1，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-19 內部網路介面位址設定頁面

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-20）

- 選擇【埠號】3，按下【修改】鈕。
- 【介面類型】選擇非軍事區網路。
- 【非軍事區介面模式】選擇透通橋接模式。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-20 非軍事區網路透通橋接模式設定頁面

步驟3. 在【網路介面】>【介面分組】頁面中，做下列設定：（如圖 3-21）

- 將【埠號 2（WAN1）】、【埠號 3（DMZ1）】介面設為分組 1。
- 按下【確定】鈕，完成設定。

圖 3-21 介面分組設定

步驟4. 接於非軍事區網路介面的使用者電腦透過 MHG-2000 控管，直接以本機 IP 位址（隸屬於 172.16.x.x/16 網段）經原有閘道器轉換為真實 IP 位址上網。接於內部網路介面的使用者電腦，轉址為 WAN1（172.16.1.12）經原有閘道器轉換為真實 IP 位址上網。（如圖 3-22）

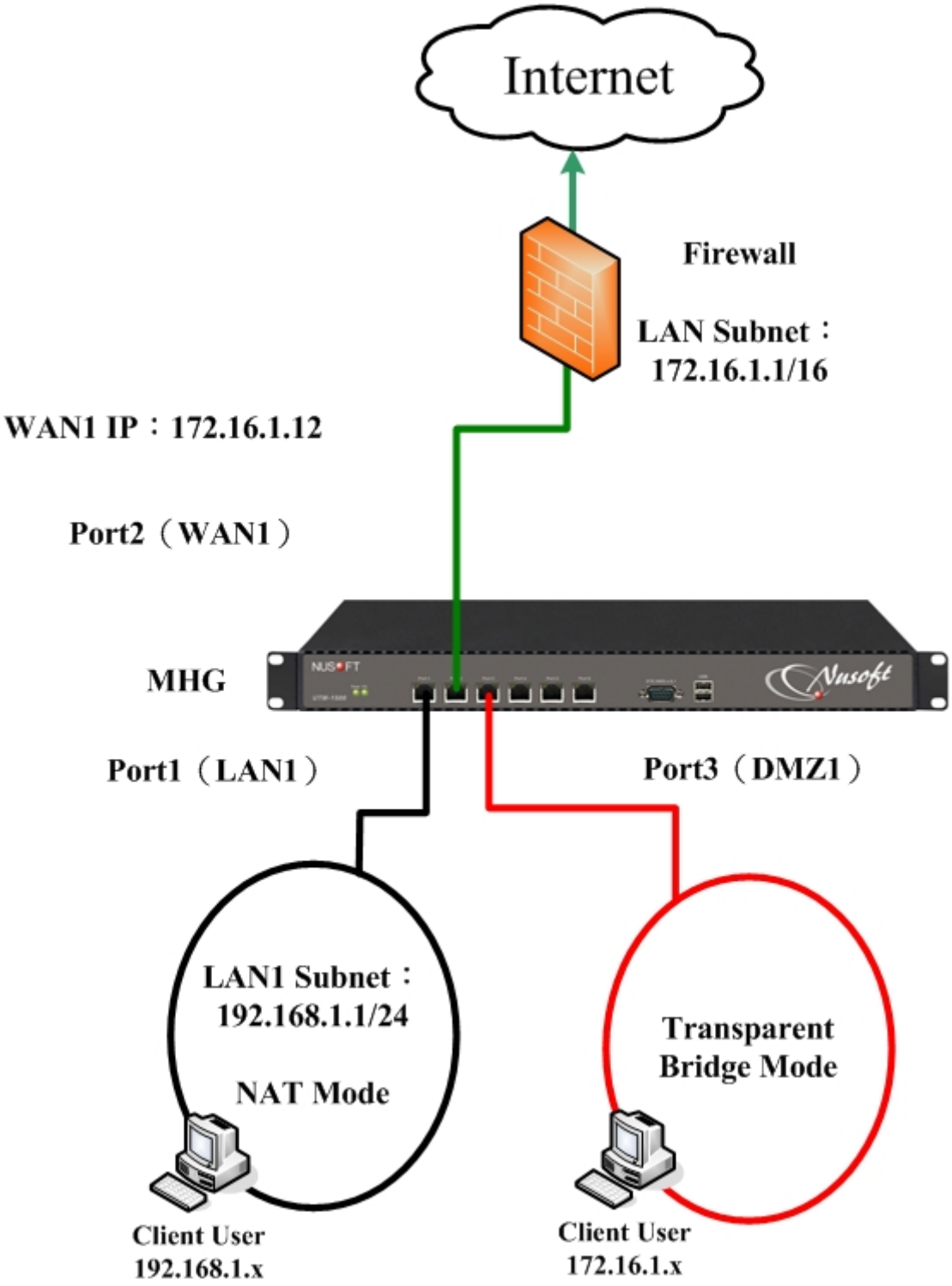


圖 3-22 非軍事區網路透通橋接模式適用環境 01

說明：

1. 位於非軍事區的電腦會直接透過原有閘道器路由上網。
2. 若 Port4 設為 WAN2（211.22.22.22）和 ATU-R 對接，連上網際網路。**（如圖 3-23）**
   - 接於非軍事區網路介面的電腦（隸屬於 172.16.x.x/16 網段）：
     - 網卡的預設閘道設為原有閘道器之 LAN（172.16.1.1），直接透過 MHG-2000 的 WAN1，以本機 IP 位址經原有閘道器轉換為真實 IP 位址上網。（透過原有閘道器路由）
     - 網卡的預設閘道設為 MHG-2000 的 WAN1（172.16.1.12），轉址為 WAN1（172.16.1.12）經原有閘道器轉換為真實 IP 位址、WAN2 真實 IP 位址（211.22.22.22）存取網際網路資源。（透過 MHG-2000 路由，並進行流量負載平衡）
   - 接於內部網路介面的電腦（隸屬於 192.168.1.x/24 網段）：
     - 網卡的預設閘道設為 MHG-2000 的 LAN1（192.168.1.1），轉址為 WAN1（172.16.1.12）經原有閘道器轉換為真實 IP 位址、WAN2 真實 IP 位址（211.22.22.22）存取網際網路資源。（透過 MHG-2000 路由，並進行流量負載平衡）

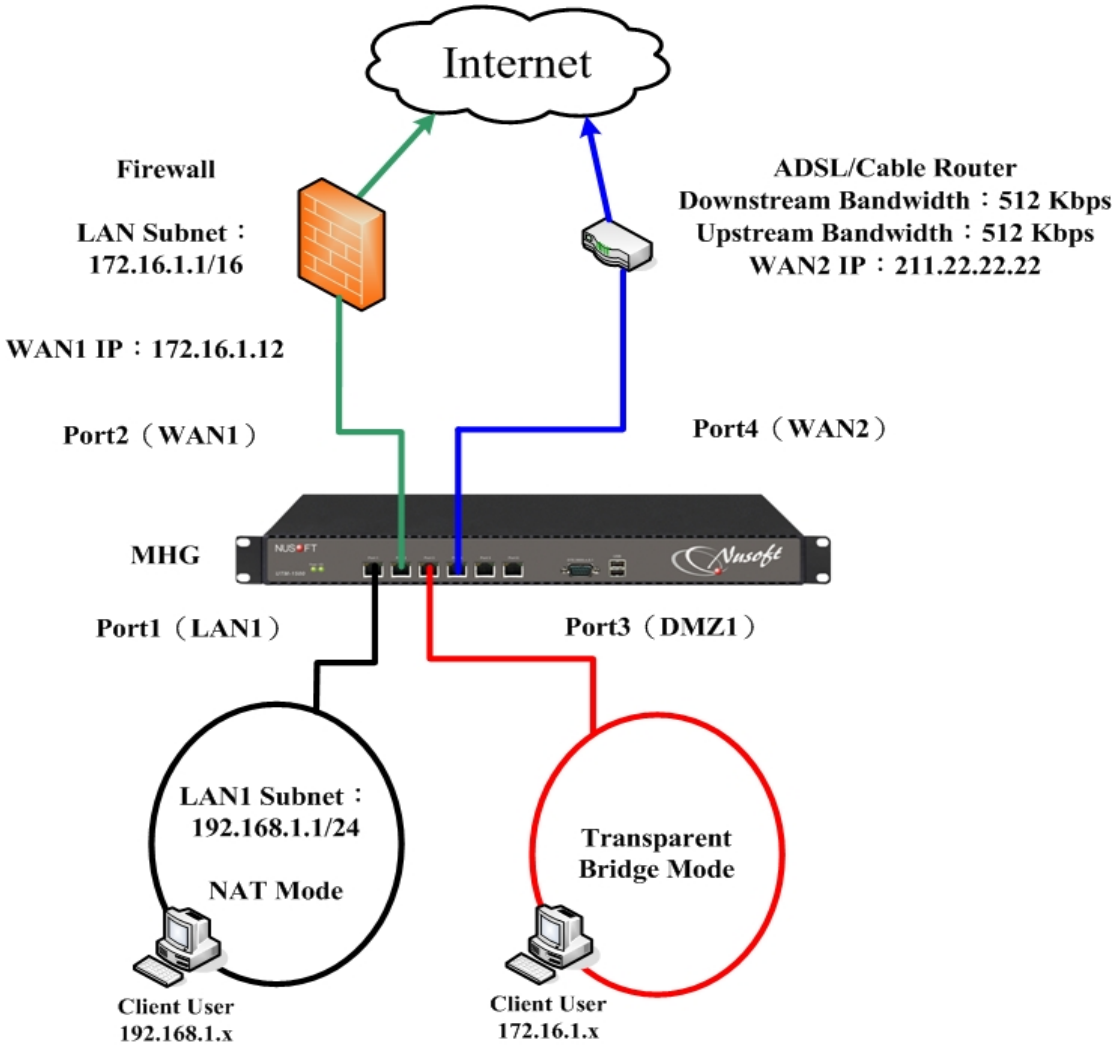


圖 3-23 非軍事區網路透通橋接模式適用環境 02

3. 若原有的內部網路有路由器連接不同的網段，讓它們能透過原有閘道器上網；在置於 MHG-2000 的非軍事區網路介面後，可直接以原網段 IP 位址透過 MHG-2000 的 WAN1 經原有閘道器轉換為真實 IP 位址上網。(透過原有閘道器路由)**(如圖 3-24)**

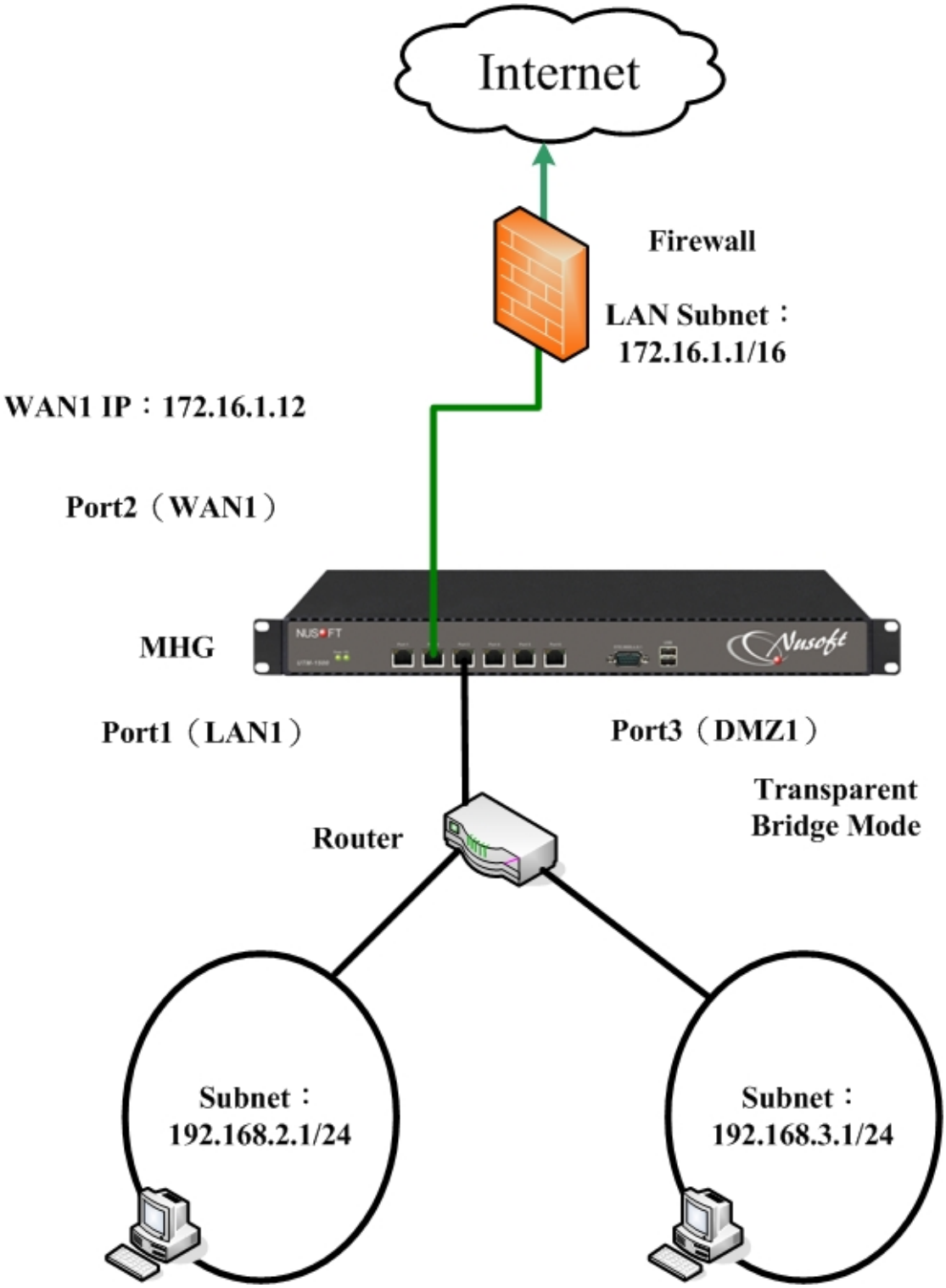


圖 3-24 非軍事區網路透通橋接模式適用環境 03

4. 若 MHG-2000 設有 2 個 WAN 和不同的閘道器或路由器連接、原有內部網路有 2 個網段和非軍事區網路介面連接；其中一網段電腦的預設閘道指向 WAN1 連接的閘道器（路由器），另一網段電腦的預設閘道指向 WAN2 連接的閘道器（路由器）。當 MHG-2000 允許此 2 網段同時存取所有外部網路時，此 2 網段的電腦僅會依所設定的閘道位址向指定的 WAN 傳送封包。**（如圖 3-25）**

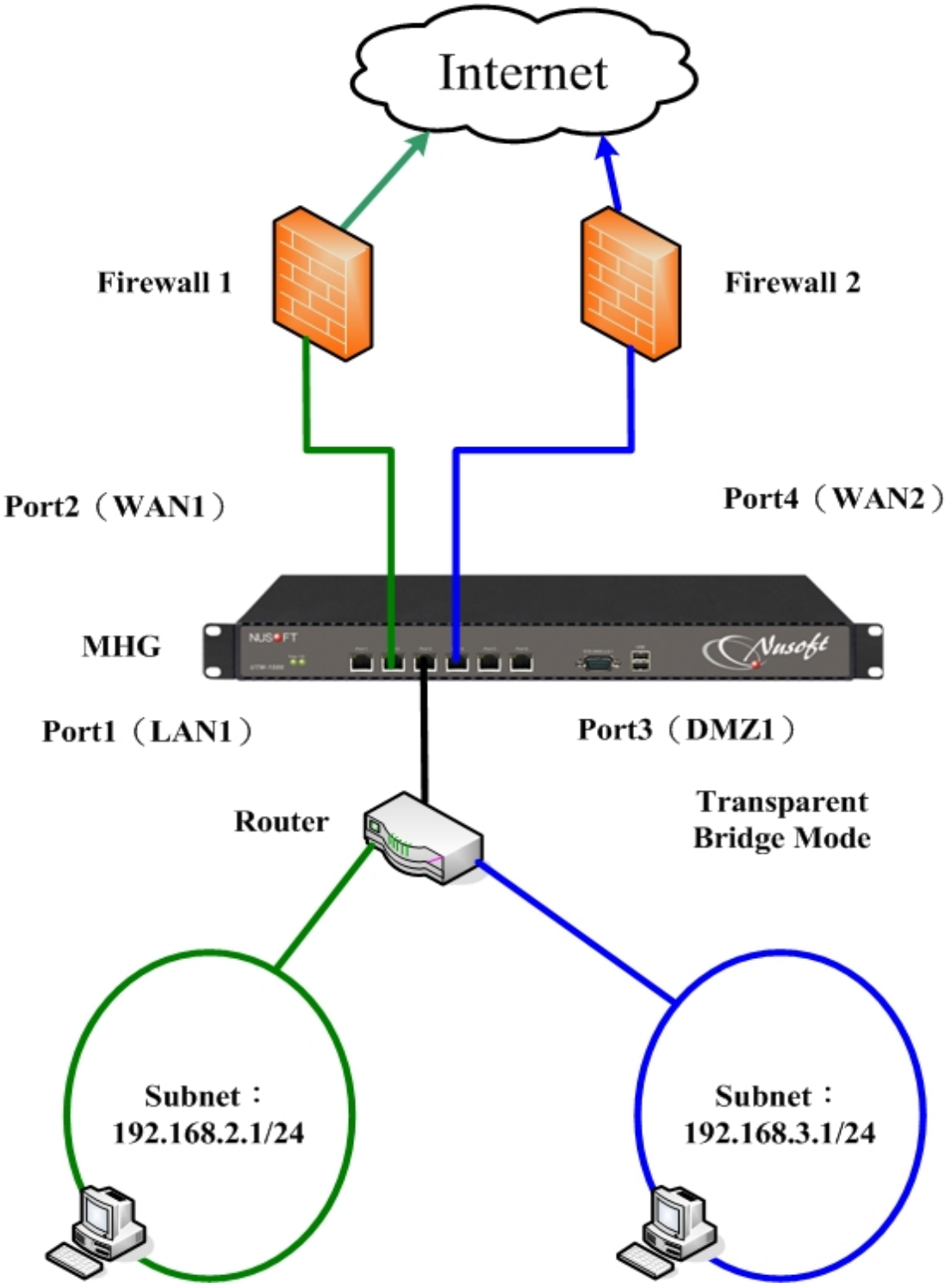


圖 3-25 非軍事區網路透通橋接模式適用環境 04

3.1.7 將 MHG-2000 置於原有的閘道器和內部網路、非軍事區網路之間，分別加強管理原有閘道器內部網路、非軍事區網路存取網路資源權限

環境設定

原有閘道器之 LAN（192.168.1.1）為 192.168.1.x/24 網段。

WAN（61.11.11.11）和 ATU-R 對接，連上網際網路。

DMZ（透通模式）。

Port1 設為 WAN1（192.168.1.2）和原有閘道器之 LAN 對接。

Port2 設為 LAN1（透通橋接模式）連接原有內部網路電腦（隸屬於 192.168.1.x/24 網段，網卡的預設閘道皆設為 192.168.1.1），直接以本機 IP 位址經原有閘道器轉換為真實 IP 位址存取網際網路資源。

Port3 設為 WAN2（61.11.11.12）和原有閘道器之 DMZ 對接。

Port4 設為 DMZ1（透通橋接模式）連接原有非軍事區網路對外服務的伺服器（採用 WAN2 線路 ISP 配發的可用真實 IP 位址），直接以本機 IP 位址經原有閘道器連線網際網路。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-26）

- 選擇【埠號】1，按下【修改】鈕。
- 【介面類型】選擇外部網路。
- 選擇指定的【外部網路連線模式】。
- 輸入指定的連線資訊。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

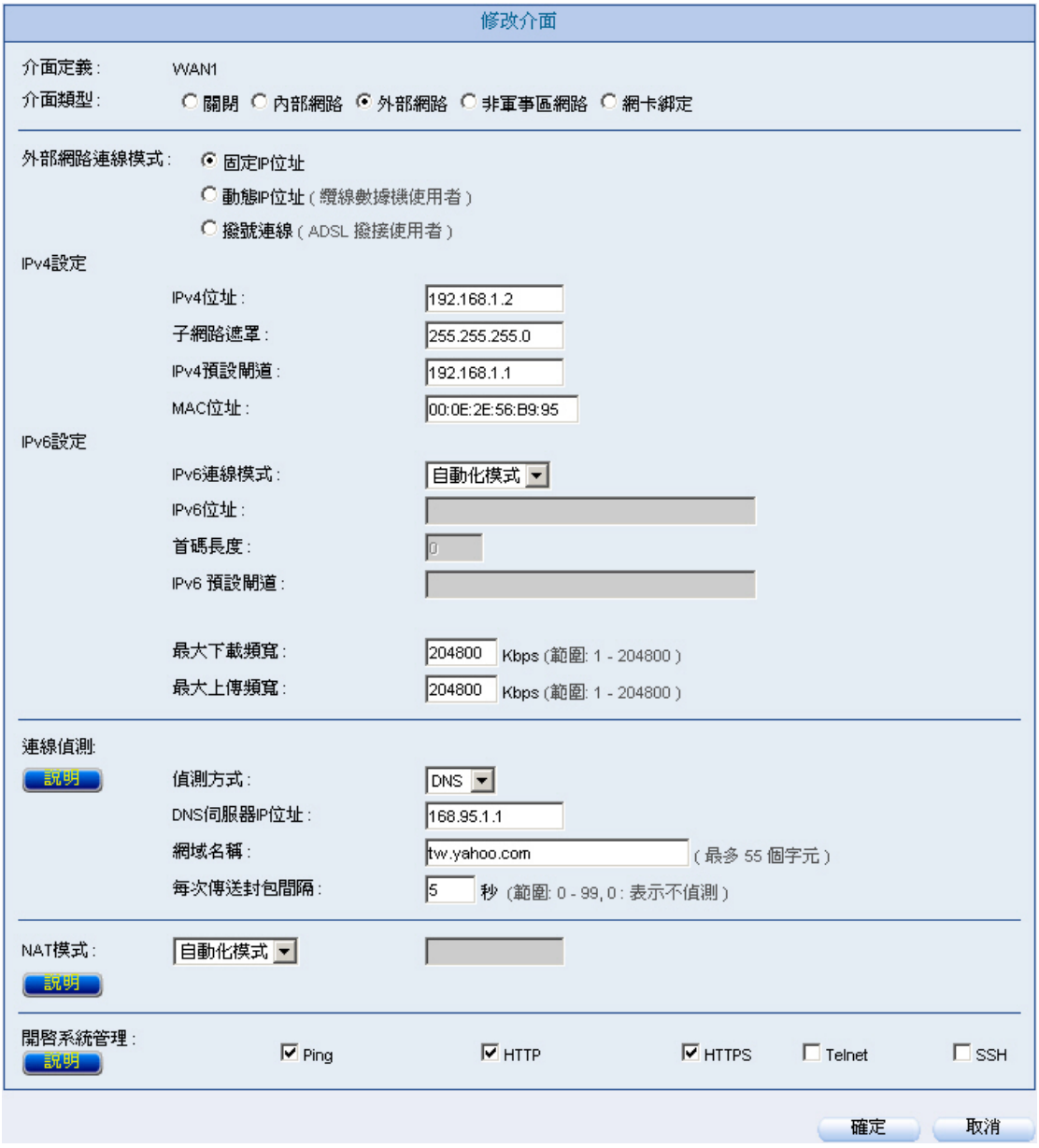


圖 3-26 外部網路介面 1 連線設定頁面

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-27）

- 選擇【埠號】2，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇透通橋接模式。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-27 內部網路透通橋接模式設定頁面

步驟3. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-28）

- 選擇【埠號】3，按下【修改】鈕。
- 【介面類型】選擇外部網路。
- 選擇指定的【外部網路連線模式】。
- 輸入指定的連線資訊。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

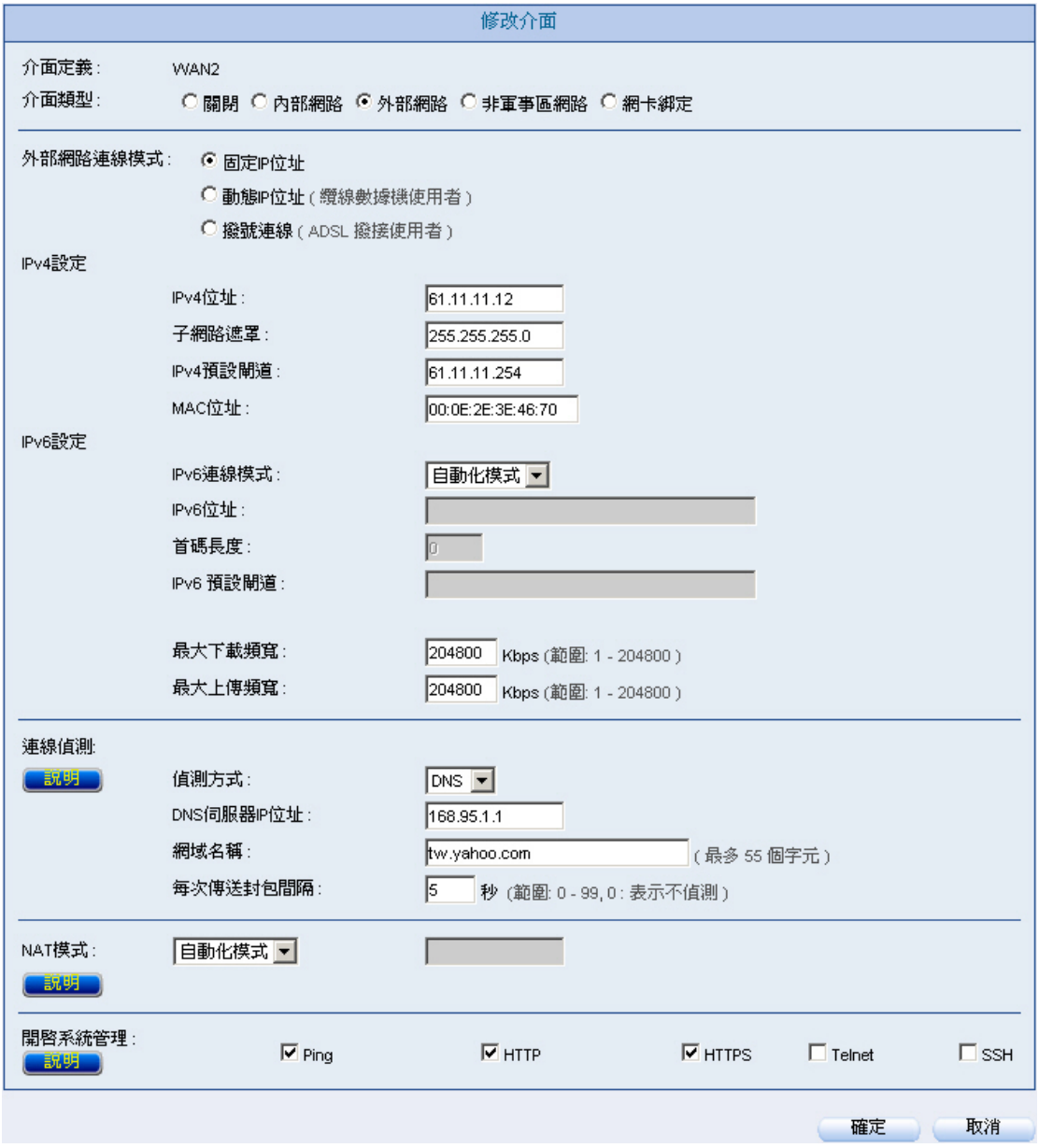


圖 3-28 外部網路介面 2 連線設定頁面

步驟4. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-29）

- 選擇【埠號】4，按下【修改】鈕。
- 【介面類型】選擇非軍事區網路。
- 【非軍事區介面模式】選擇透通橋接模式。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-29 非軍事區網路透通橋接模式設定頁面

步驟5. 在【網路介面】>【介面分組】頁面中，做下列設定：（如圖 3-30）

- 將【埠號 1（WAN1）】、【埠號 2（LAN1）】介面設為分組 1。
- 將【埠號 3（WAN2）】、【埠號 4（DMZ1）】介面設為分組 2。
- 按下【確定】鈕，完成設定。

圖 3-30 介面分組設定

注意：

1. 此時可將 MHG-2000 視為 2 個獨立的交換器，【埠號 1（WAN1）】和【埠號 2（LAN1）】專門用來控管原有內部網路的網路存取權限、【埠號 3（WAN2）】和【埠號 4（DMZ1）】專門用來控管原有非軍事區網路的網路存取權限；隸屬不同群組的介面無法互通。

步驟6. 接於【埠號 2（LAN1）】的使用者電腦透過 MHG-2000 控管，直接以本機 IP 位址（隸屬於 192.168.1.x/24 網段）經原有閘道器轉換為真實 IP 位址上網。接於【埠號 4（DMZ1）】的伺服器，直接以 ISP 配發的真實 IP 位址經原有閘道器對外服務。（如圖 3-31）

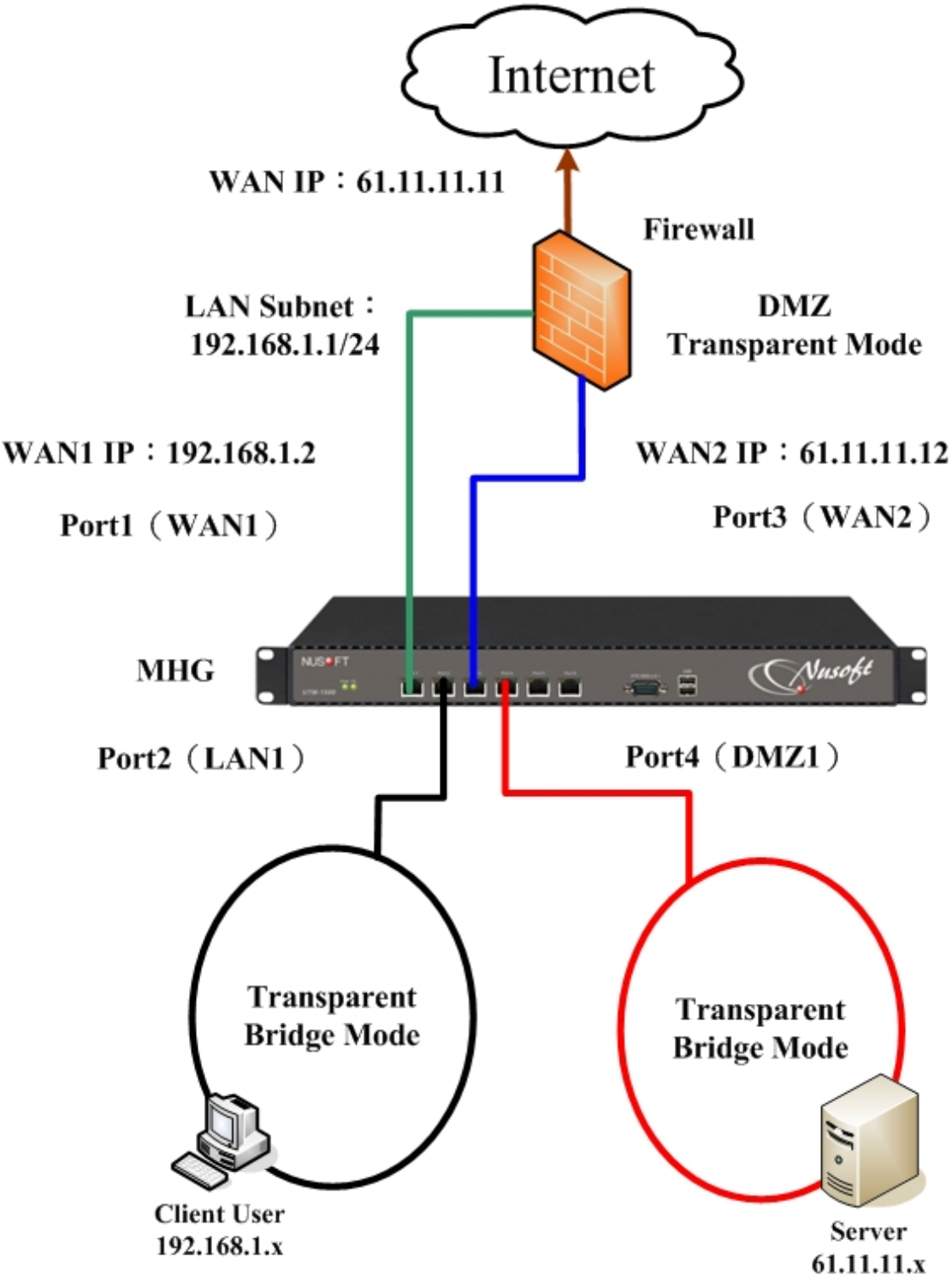


圖 3-31 介面分組適用環境

3.1.8 以 MHG-2000 做為閘道器，設定兩個內部（一個採 NAT / 路由模式，另一個採透通橋接模式）網路介面，分別連接不同部門的使用者電腦，管理存取網路資源權限

環境設定

Port1 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

Port2 設為 LAN1（192.168.1.1，NAT / 路由模式）為 192.168.1.x/24 網段，連接業務部門的使用者電腦（網卡的預設閘道皆設為 192.168.1.1）轉址為 WAN1（61.11.11.11）存取網際網路資源。

Port3 設為 LAN2（透通橋接模式）為 192.168.1.x/24 網段，連接客服部門的使用者電腦（網卡的預設閘道皆設為 192.168.1.1）轉址為 WAN1（61.11.11.11）存取網際網路資源。

接於 LAN1 和 LAN2 的電腦需透過管制條例互通。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-32）

- 選擇【埠號】1，按下【修改】鈕。
- 【介面類型】選擇外部網路。
- 選擇指定的【外部網路連線模式】。
- 輸入指定的連線資訊。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

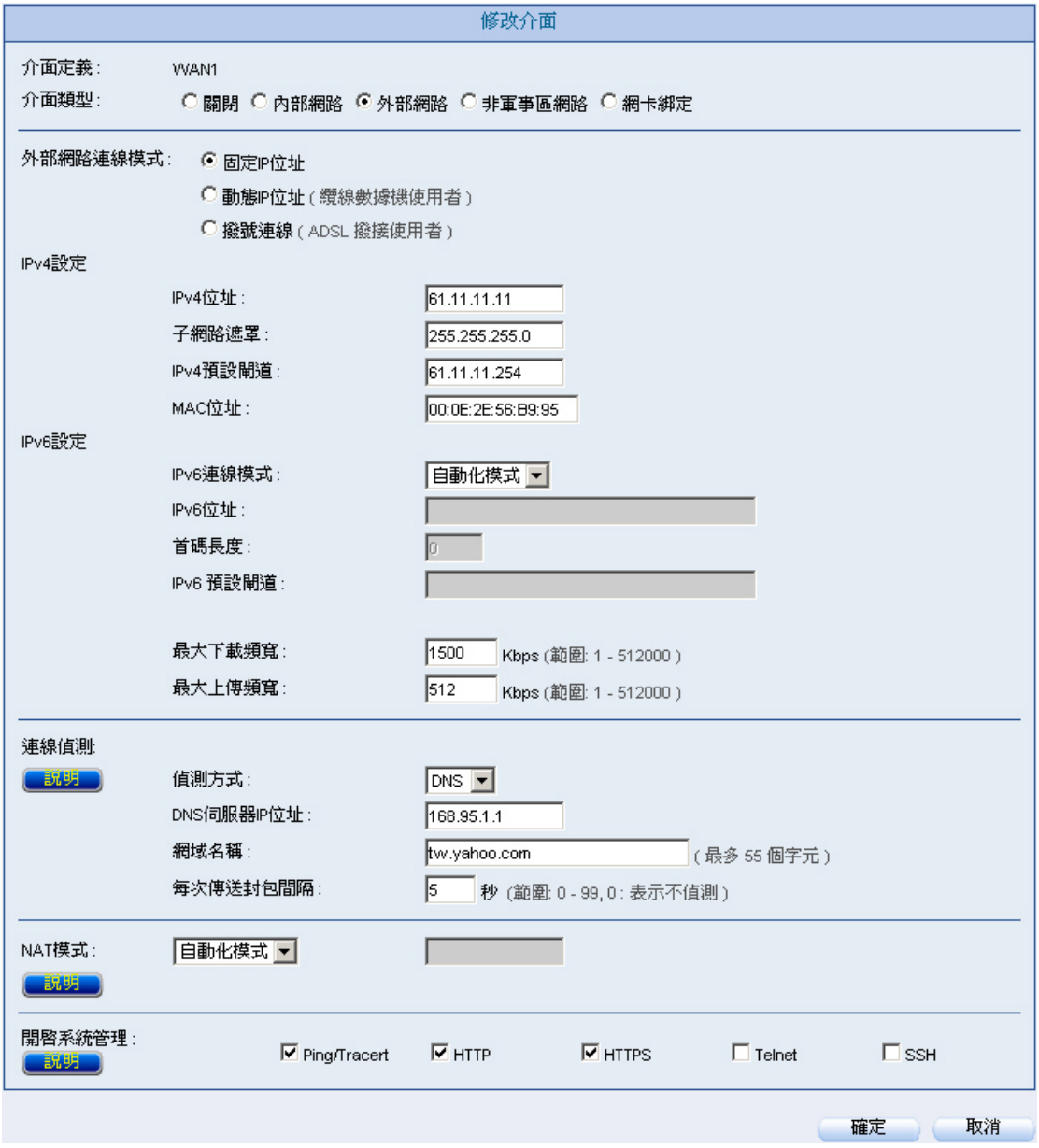


圖 3-32 外部網路介面 1 連線設定頁面

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-33）

- 選擇【埠號】2，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-33 內部網路介面 1 位址設定頁面

步驟3. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-34）

- 選擇【埠號】3，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇透通橋接模式。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-34 內部網路介面 2 位址設定頁面

步驟4. 在【網路介面】>【介面分組】頁面中，做下列設定：（如圖 3-35）

- 將【埠號 1（WAN1）】、【埠號 2（LAN1）】、【埠號 3（LAN2）】介面設為分組 1。
- 按下【確定】鈕，完成設定。

圖 3-35 介面分組設定

說明：

1. 此時可將 MHG-2000 內部相同網段的使用者，以不同的實體介面分隔所屬部門的作業環境，例如：【埠號 2（LAN1）】用來連接業務部門的使用者電腦、【埠號 3（LAN2）】用來連接客服部門的使用者電腦。

步驟5. 接於 LAN1 的業務部、LAN2 的客服部使用者電腦，皆隸屬於 192.168.1.x/24 網段，並轉換成 WAN1 真實 IP 位址（61.11.11.11）存取網際網路資源；彼此需透過管制條例互通。**（如圖 3-36）**

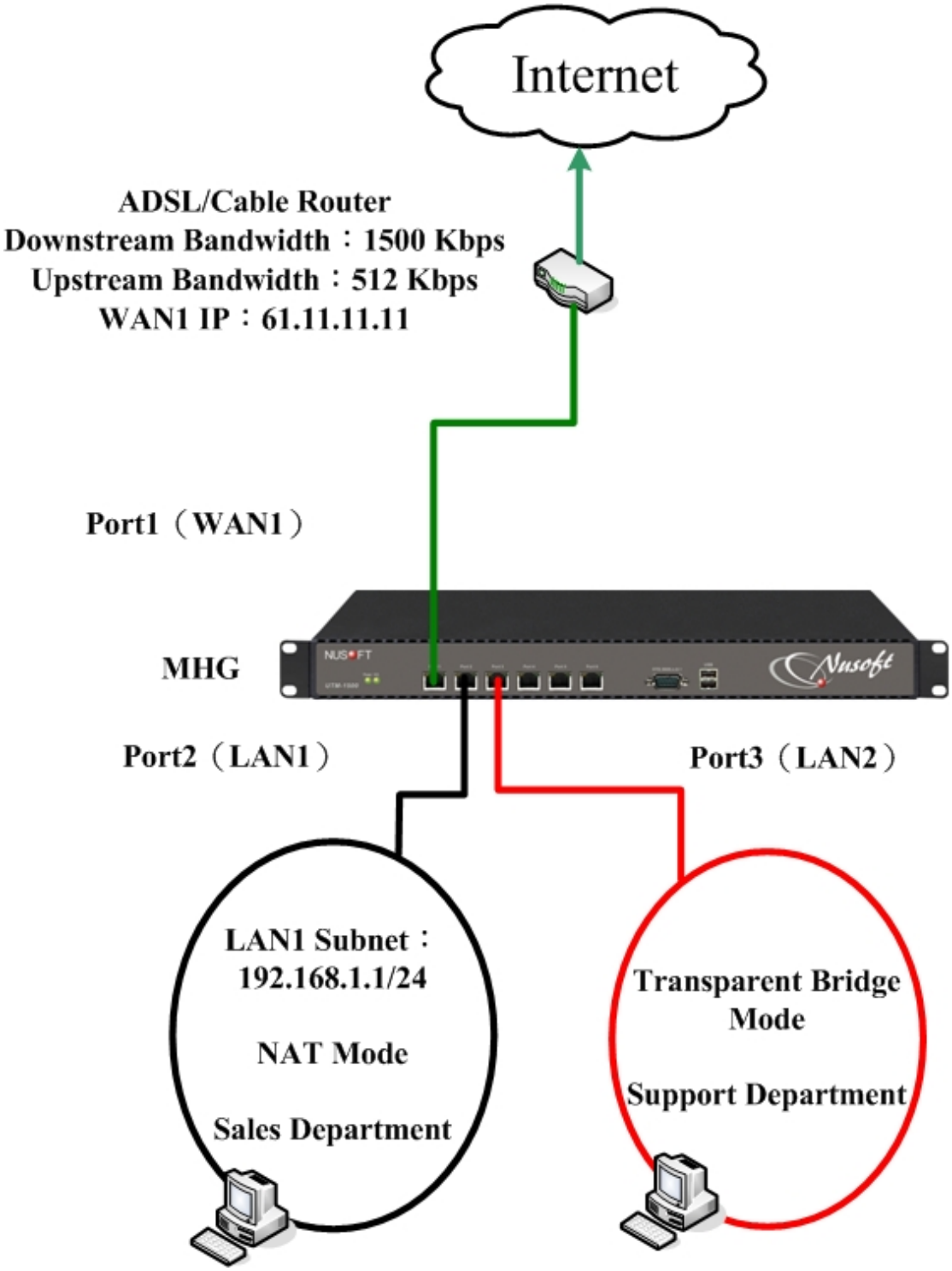


圖 3-36 內部網路透通橋接、NAT / 路由模式適用環境

3.1.9 將 MHG-2000 置於原有的閘道器和內部網路之間，於設定為內部（NAT / 路由模式）網路和所屬綁定的介面連接原有內部網路、設定為外部（固定 IP 位址連線模式）網路和所屬綁定的介面連接使用者電腦，增加彼此資料傳輸量

環境設定

原有閘道器之 LAN 有 192.168.1.x/24（閘道位址為 192.168.1.1）、192.168.2.x/24（閘道位址為 192.168.2.1）網段。

Port1 設為 WAN1（192.168.2.2）。

Port2 和 Port1 綁定並連接到同一交換器（設定 Trunk），藉以銜接原有閘道器之 LAN。

將原有閘道器 192.168.2.x/24 網段和 WAN1 連接到同一交換器。

Port3 設為 LAN1（192.168.1.1，NAT / 路由模式）。

Port4 和 Port3 綁定並連接到同一交換器（設定 Trunk），藉以銜接原有內部網路電腦（隸屬於 192.168.1.x/24 網段，網卡的預設閘道皆設為 192.168.1.1）轉址為 WAN1（192.168.2.2），經原有閘道器轉換為真實 IP 位址存取網際網路資源。

192.168.1.x/24 網段和 192.168.2.x/24 網段，可分別透過整合多個實體網路埠頻寬的 LAN1 和 WAN1 互傳資料。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-37）

- 選擇【埠號】1，按下【修改】鈕。
- 【介面類型】選擇外部網路。
- 選擇指定的【外部網路連線模式】。
- 輸入指定的連線資訊。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

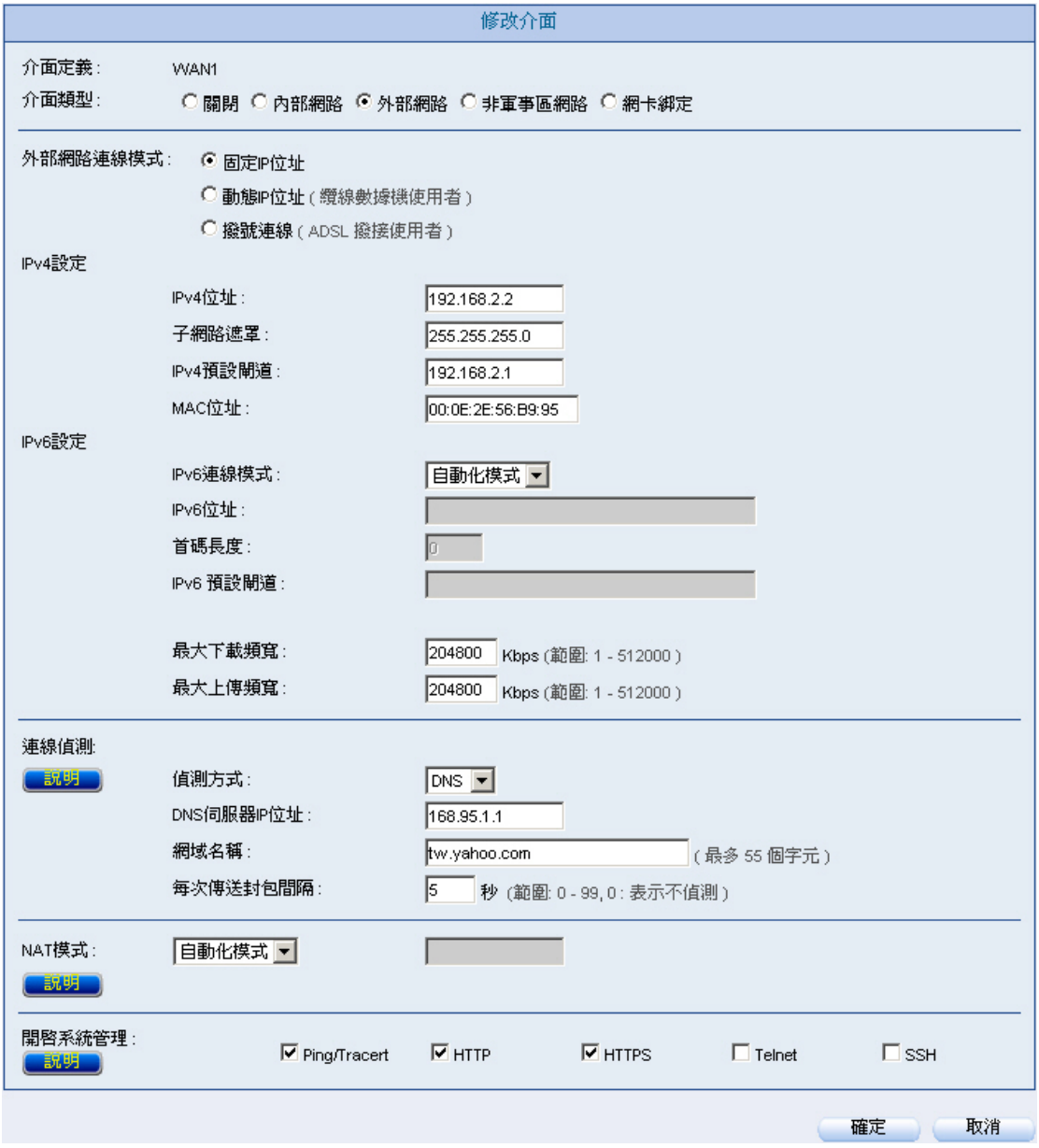


圖 3-37 外部網路介面 1 連線設定頁面

步驟2. 在【網路介面】>【介面位址】頁面中，做下列設定：**（如圖 3-38）**

- 選擇【埠號】2，按下【修改】鈕。
- 【介面類型】選擇網卡綁定。
- 【綁定介面】選擇 Port1（WAN1）。
- 選擇指定的【綁定模式】、【偵測模式】。
- 按下【確定】鈕，完成設定。

圖 3-38Port2 和 Port1 綁定設定頁面

說明：

1. 【外部網路】介面要採用固定 IP 位址連線模式，方可做為【綁定介面】。

步驟3. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-39）

- 選擇【埠號】3，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-39 內部網路介面位址設定頁面

步驟4. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-40）

- 選擇【埠號】4，按下【修改】鈕。
- 【介面類型】選擇網卡綁定。
- 【綁定介面】選擇 Port3（LAN1）。
- 選擇指定的【綁定模式】、【偵測模式】。
- 按下【確定】鈕，完成設定。

圖 3-40Port4 和 Port3 綁定設定頁面

說明：

1. 【內部網路】、【非軍事區網路】介面要採用 NAT / 路由模式，方可做為【綁定介面】。

步驟5. 接於 LAN1（隸屬於 192.168.1.x/24 網段）、WAN1（隸屬於 192.168.2.x/24 網段）的使用者電腦透過 MHG-2000 管制條例彼此互通。（如圖 3-41）

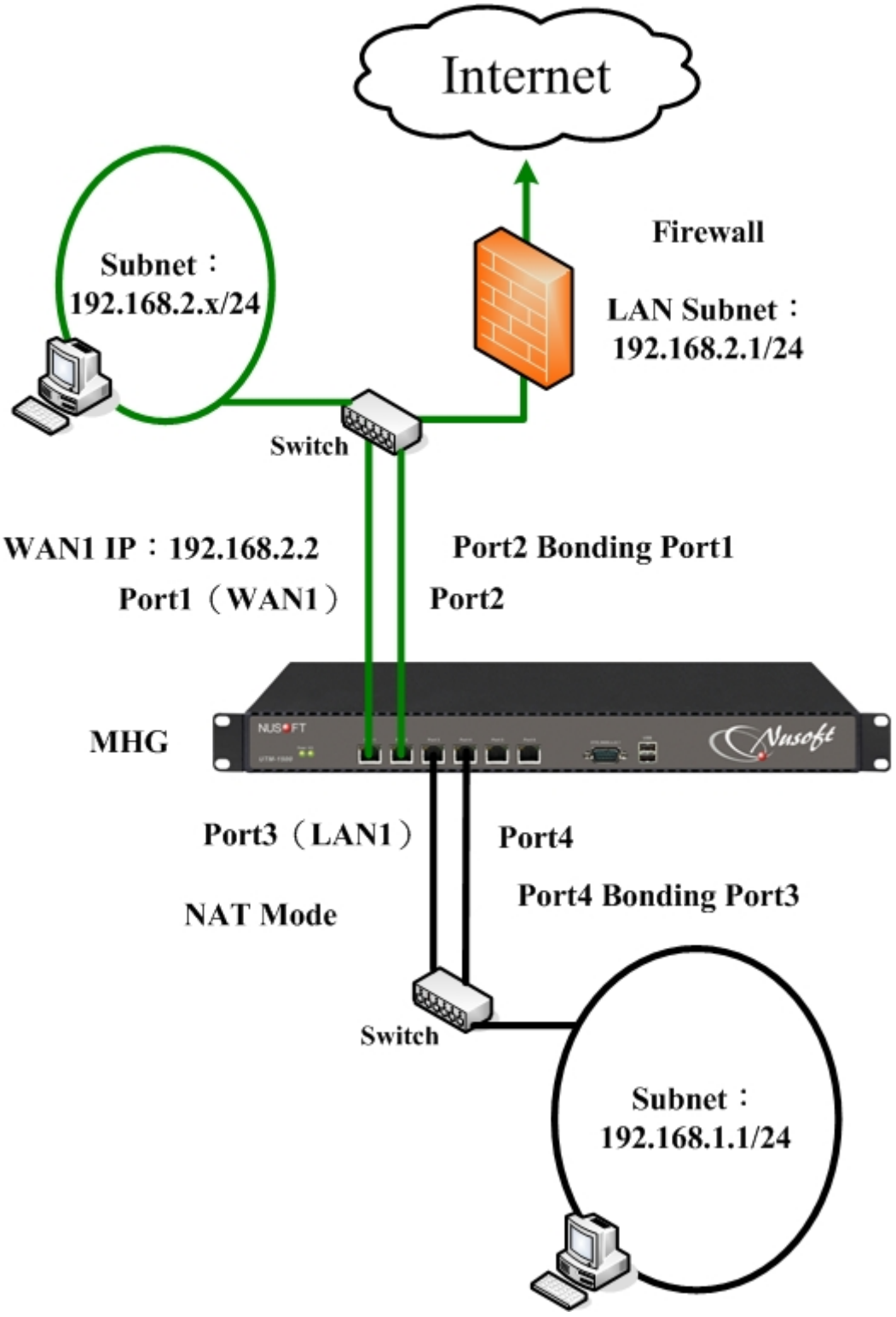


圖 3-41 網卡綁定適用環境

3.1.10 以 MHG-2000 做為閘道器，設定一個外部（固定 IP 位址連線模式）網路介面和所屬虛擬網路介面，將不同的上網線路連接到同一實體網路埠，同時處理網路連線需求

環境設定

申請兩條固接 IP 線路（有各自 ATU-R，ATU-R1、ATU-R2）。

Port1 設為 WAN1（61.11.11.11）。

設定隸屬於 WAN1 的虛擬網路介面 Virtual_WAN1（211.22.22.22）。

將 ATU-R1、ATU-R2 和 WAN1（包含所屬虛擬網路介面 Virtual_WAN1）連接到同一交換器。

Port2 設為 LAN1（192.168.1.1，NAT / 路由模式）為 192.168.1.x/24 網段，連接的使用者電腦轉址為 WAN1（61.11.11.11）或 Virtual_WAN1（211.22.22.22）存取網際網路資源。。

步驟1. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-42）

- 選擇【埠號】1，按下【修改】鈕。
- 【介面類型】選擇外部網路。
- 選擇指定的【外部網路連線模式】。
- 輸入指定的連線資訊。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

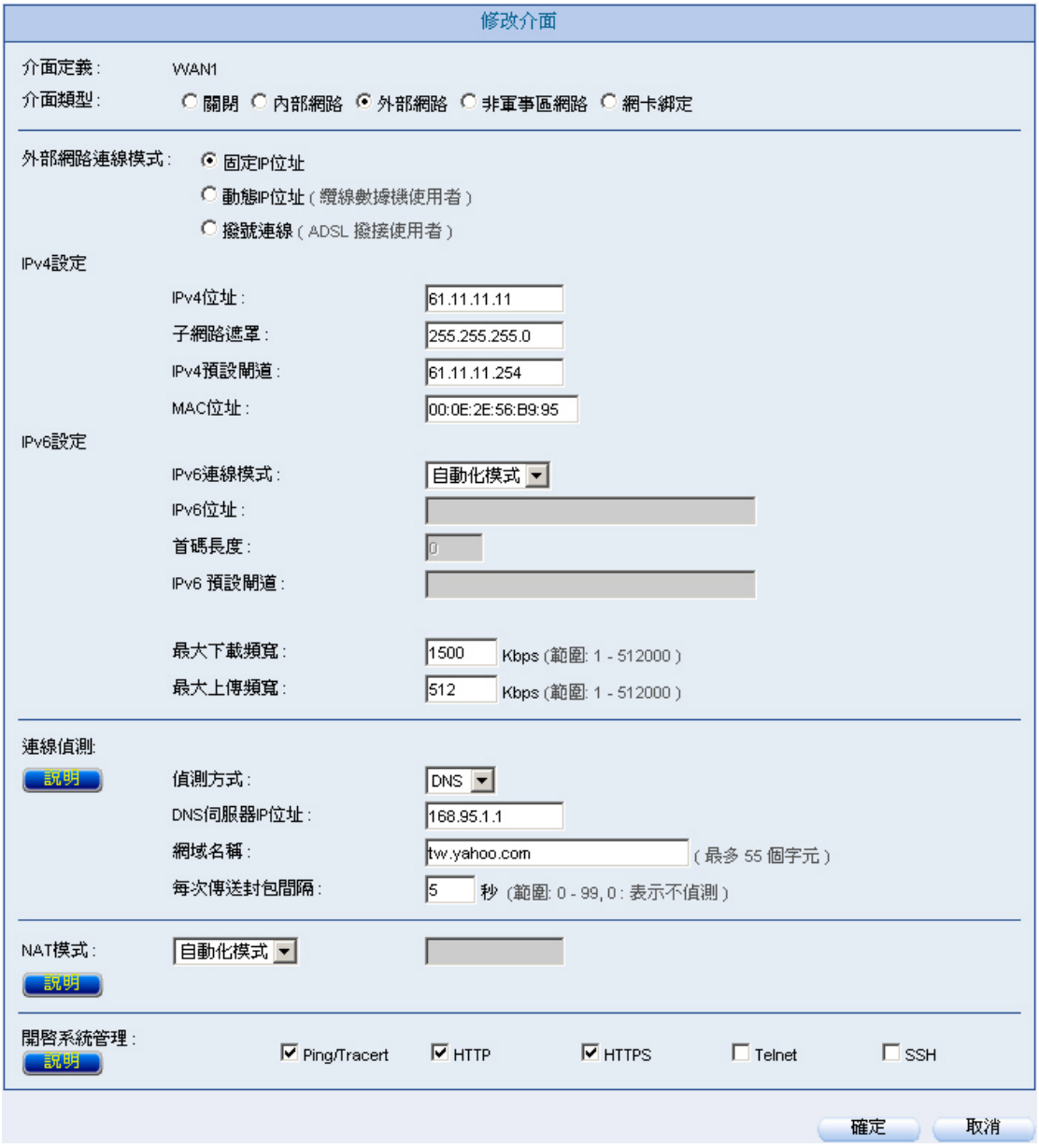


圖 3-42 外部網路介面 1 連線設定頁面

步驟2. 在【網路介面】>【虛擬外部網路】頁面中，做下列設定：（如圖 3-43）

- 輸入指定的虛擬外部網路【名稱】。
- 【介面】選擇 Port1（WAN1）。
- 輸入指定的連線資訊。
- 按下【確定】鈕，完成設定。（如圖 3-44）

圖 3-43 設定外部網路介面 1 的虛擬網路介面

圖 3-44 完成外部網路介面 1 的虛擬網路介面設定

步驟3. 在【網路介面】>【介面位址】頁面中，做下列設定：（如圖 3-45）

- 選擇【埠號】2，按下【修改】鈕。
- 【介面類型】選擇內部網路。
- 【內部網路介面模式】選擇 NAT / 路由模式。
- 輸入指定的【IPv4 位址】、【子網路遮罩】。
- 【開啟系統管理】的 Ping/Tracert、HTTP 和 HTTPS 功能。
- 按下【確定】鈕，完成設定。

圖 3-45 內部網路介面位址設定頁面

步驟4. 接於內部網路介面的使用者電腦，轉換成 WAN1 真實 IP 位址（61.11.11.11）、Virtual_WAN1 真實 IP 位址（211.22.22.22）存取網際網路資源。（如圖 3-46）

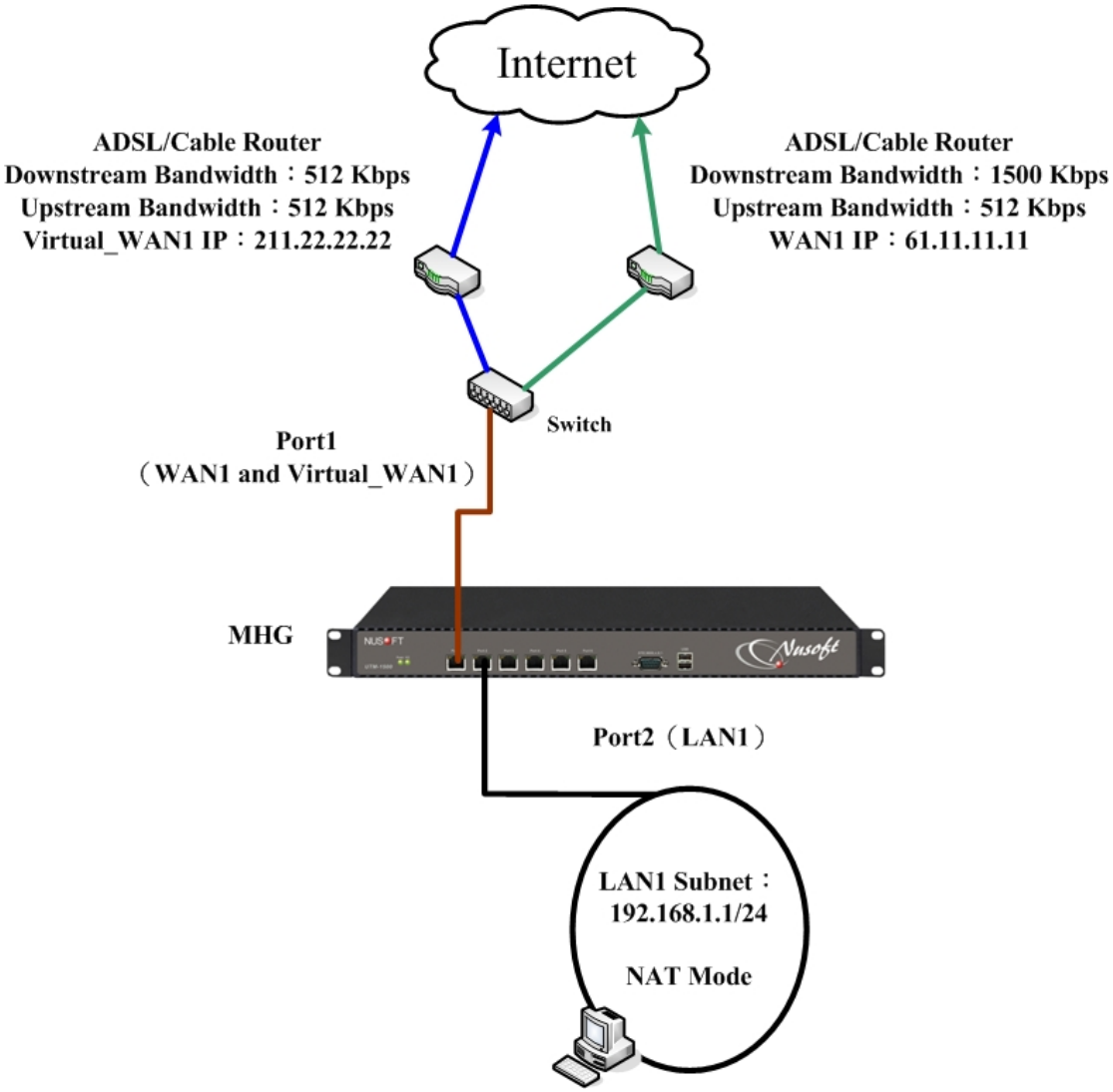


圖 3-46 虛擬外部網路適用環境

說明：

1. 可在【管制條例】>【內部至外部】、【非軍事區至外部】頁面中，設定透過指定【虛擬外部網路】介面上網的規則。（如圖 3-47，圖 3-48）

圖 3-47 設定透過虛擬外部網路上網管制條例

圖 3-48 完成透過虛擬外部網路上網管制條例設定

2. 可在【管制條例選項】>【虛擬伺服器】>【IP 對應】頁面中，設定透過指定虛擬外部網路介面連線內部特定主機。（如圖 3-49，圖 3-50）

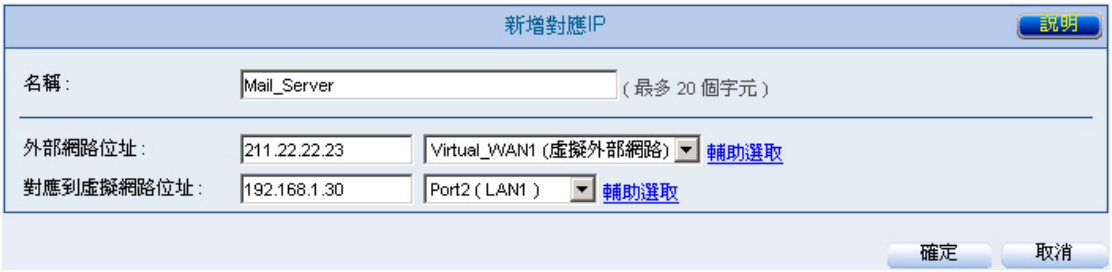


圖 3-49 設定虛擬外部網路 IP 對應

圖 3-50 完成虛擬外部網路 IP 對應設定

3. 可在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，設定內部特定主機透過指定虛擬外部網路介面提供服務。（如圖 3-51，圖 3-52）

圖 3-51 設定虛擬外部網路連接埠對應

圖 3-52 完成虛擬外部網路連接埠對應設定

管制條例選項

第4章　位址表

用來設定位於 MHG-2000 內部網路、外部網路、非軍事區網路的 IP 位址列表，並視需求將特定 IP 位址進行群組、劃分。

這些 IP 位址可能是一個主機 IP 位址，也可能是一個網段。系統管理員可以自行設定一個易辨識的名字代表此一 IP 位址。基本上 IP 位址根據不同的網路區可分為三種：內部網路 IP 位址(Internal IP Address)、外部網路 IP 位址(External IP Address) 和非軍事區網路 IP 位址(DMZ IP Address)。當系統管理員欲將不同 IP 位址封包的過濾規則，加入相同管制條例時，可先將這些 IP 位址建立一個「內部網路群組」、「外部網路群組」或是「非軍事區群組」，以簡化設立管制條例工作程序。

說明：

1. 當位址表設定完成後，系統管理員在設定管制條例時，就可選用此位址表名稱，套用在管制條例的來源位址(Source Address)或目的位址(Destination Address)。所以位址表的設定應該在管制條例的設定之前，如此在設定管制條例時，才可在位址表中挑出正確的 IP 位址名稱。

【位址表】功能概述：

名稱 說明如下：

- 用於指定一個易辨識的名字代表所設定之 IP 位址。

IP 位址範圍 說明如下：

- 可以 IPv4 子網路遮罩指定、IPv6 首碼長度指定、直接輸入 IP 範圍、輸入特定 FQDN。

說明：

1. FQDN（Fully Qualified Domain Name）是由主機名稱（Hostname）和網域名稱（Domain Name）兩部份所組成。以 www.nusoft.com.tw 為例，主機名稱就是 www，網域名稱就是 nusoft.com.tw。
2. 以往在封鎖同時對應多個 IP 的網站（例如：Facebook、Yahoo、...）時，只能逐一輸入人工查詢網站對應的 IP、網段，容易會有所遺漏，若採以 FQDN 設定外部網路位址表，系統會自動查詢網站使用的所有 IP 位址。
3. FQDN 功能可以運用在網站黑/白名單功能鞭長莫及的地方（網站黑/白名單功能僅可管制 HTTP），例如：HTTPS、FTP。只要於外部網路位址表設定網站的 FQDN，再於管制條例中套用並封鎖之即可。

網際協定 說明如下：

- 位址表採用的網際網路協定，可為 IPv4 或 IPv6。

IP 位址 說明如下：

- 可以是一個主機 IP 位址，也可以是一個網段。可分為三種不同的網路區段：內部網路 IP 位址(Internal IP Address)、外部網路 IP 位址(External IP Address)和非軍事區網路 IP 位址(DMZ IP Address)。

子網路遮罩 說明如下：

- 對應 IPv4 單一特定 IP 時，應設定為 255.255.255.255。
- 對應 IPv4 一特定網段時（例如：192.168.100.x 之 C Class 網段的 IP），應設定為 255.255.255.0。

首碼長度 說明如下：

- 對應 IPv6 單一特定 IP 時，應設定為 128。
- 對應 IPv6 一特定網段時（例如：21DA:D3:0:2F3B:2AA:FF:FE28:9C5A，前置字元是 21DA:D3:0:2F3B），應設定為 64，衍生的子網路識別碼為 21DA:D3:0:2F3B::/64。

MAC 位址 說明如下：

- 將特定單一主機之網卡 MAC 位址與其 IP 位址對應，可防止使用者更改 IP 位址，透過它條管制條例，存取非授權之網路服務。

網路介面 說明如下：

- 用於指定所設定之 IP 位址隸屬的網路介面。

說明：

1. 在【管制條例選項】>【位址表】>【外部網路群組】頁面中，*CHU、 *CHINA_TELECOM、*CHINA_EDU 與*CHINA_MOBILE 分別代表中國聯通(China Unicom, CHU)、中國電信(China Telecom)、中國教育網與中國移動(China Mobile)所擁有的網路區段。可於對外連線時，依封包傳送目的位址，透過管制條例指定適當的傳輸線路，達到策略路由(PBR)的效果。
2. 可利用【輔助新增】方式，自動取得【監控報告】>【系統狀態】>【ARP 表】和【連線狀態】的資料，迅速完成【管制條例選項】>【位址表】>【內部網路】和【非軍事區網路】位址表設定。

4.1 位址表功能使用範例

編碼	適用範圍	範例環境	頁碼
4.1.1	**內部網路**	將特定IP位址指定給固定使用者使用，並限制其僅能透過管制條例以FTP協定存取網路資源	**136**
4.1.2	**內部網路群組** **外部網路**	設定一條只有部分使用者能與遠端特定IP連線之管制條例	**139**

4.1.1 將特定 IP 位址指定給固定使用者使用，並限制其僅能透過管

制條例以 FTP 協定存取網路資源

步驟1. 在【管制條例選項】>【位址表】>【內部網路】頁面中，做下列設定：（如圖 4-1）

- 輸入使用者的【名稱】。
- 【IP 位址範圍】選擇以 IPv4 位址 / 子網路遮罩定義。
- 【網際協定】選擇 IPv4。
- 輸入使用者的【IP 位址】。
- 【子網路遮罩】輸入 255.255.255.255。(代表 1 個 IP 位址)
- 輸入使用者的【MAC 位址】。
- 選擇所屬【網路介面】。
- 按下【確定】鈕，完成設定。（如圖 4-2）

圖 4-1 設定內部網路位址表

圖 4-2 完成內部網路位址表設定

說明：

1. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 MHG-2000【內部網路】、【內部網路群組】、【外部網路】、【外部網路群組】、【非軍事區網路】、【非軍事區群組】位址表錯亂時，可清除規則表重新【匯入】。
2. 系統管理員在設定位址表時，可利用點選

的方式，讓 MHG-2000 自動填入指定 IP 位址對應的 MAC 位址。
3. 若要透過 MHG-2000 將設定的 IP 位址自動配發給指定的 MAC 位址，在【系統管理】>【組態】>【DHCP】頁面中，可進行【配發指定 IP 至用戶端】設定。
4. 在【管制條例選項】>【位址表】>【內部網路】頁面中，MHG-2000 會自動預設一條 Inside Any 的位址表，此位址表代表了整個內部網路。其他如【外部網路】、【非軍事區網路】一樣有代表整個網域的 Outside Any 與 DMZ Any 預設位址表設定。
5. 【管制條例選項】>【位址表】>【外部網路】與【非軍事區網路】其設定模式與【內部網路】相同；唯一的不同是【外部網路】無法設定 MAC 位址和所屬網路介面。

步驟2. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 4-3）

- 【來源網路位址】選擇所設定的內部網路位址表規則。
- 【服務名稱】選擇 FTP。
- 按下【確定】鈕，完成設定。（如圖 4-4）

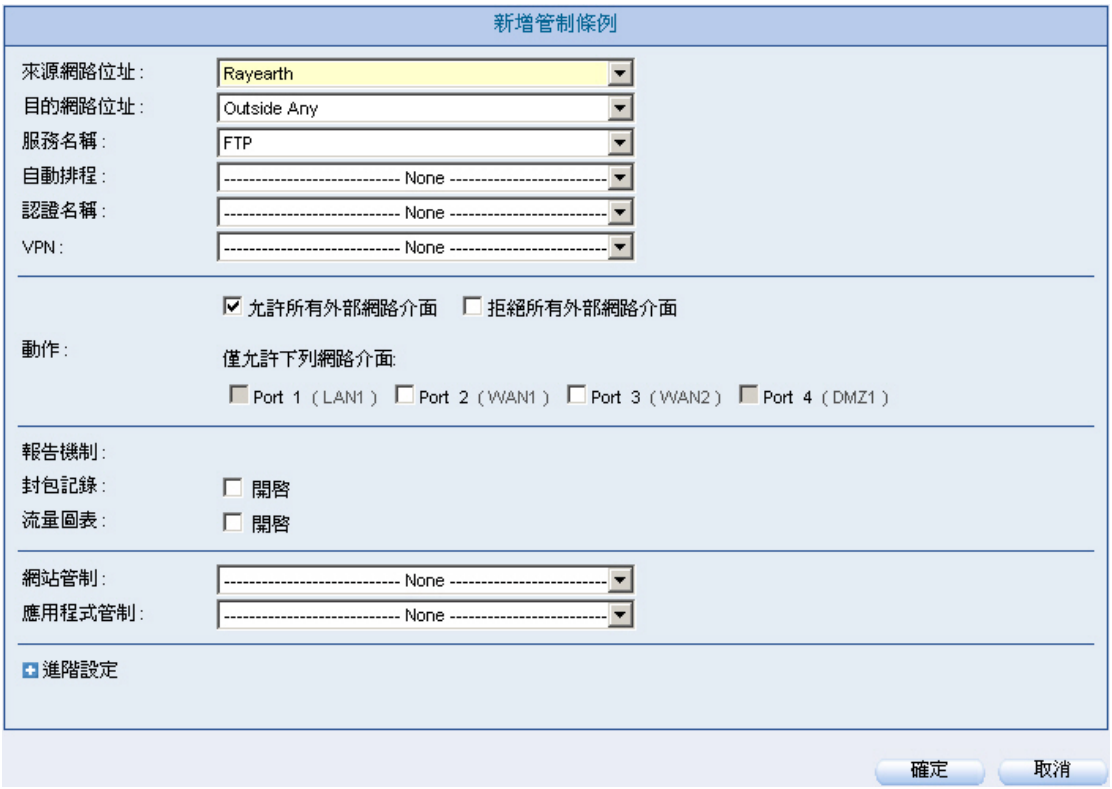


圖 4-3 設定限制單一使用者透過特定服務存取網路資源之管制條例

圖 4-4 完成管制條例設定

4.1.2 設定一條只有部分使用者能與遠端特定 IP 連線之管制條例

步驟1. 於【管制條例選項】>【位址表】>【內部網路】頁面中，做下列設定：（如圖 4-5）

圖 4-5 內部網路位址設定

步驟2. 於【管制條例選項】>【位址表】>【內部網路群組】頁面中，做下列設定：（如圖 4-6）

- 輸入群組【名稱】。
- 將指定【可選取的位址】新增至【被選取的位址】清單中。
- 按下【確定】鈕，完成設定。（如圖 4-7）

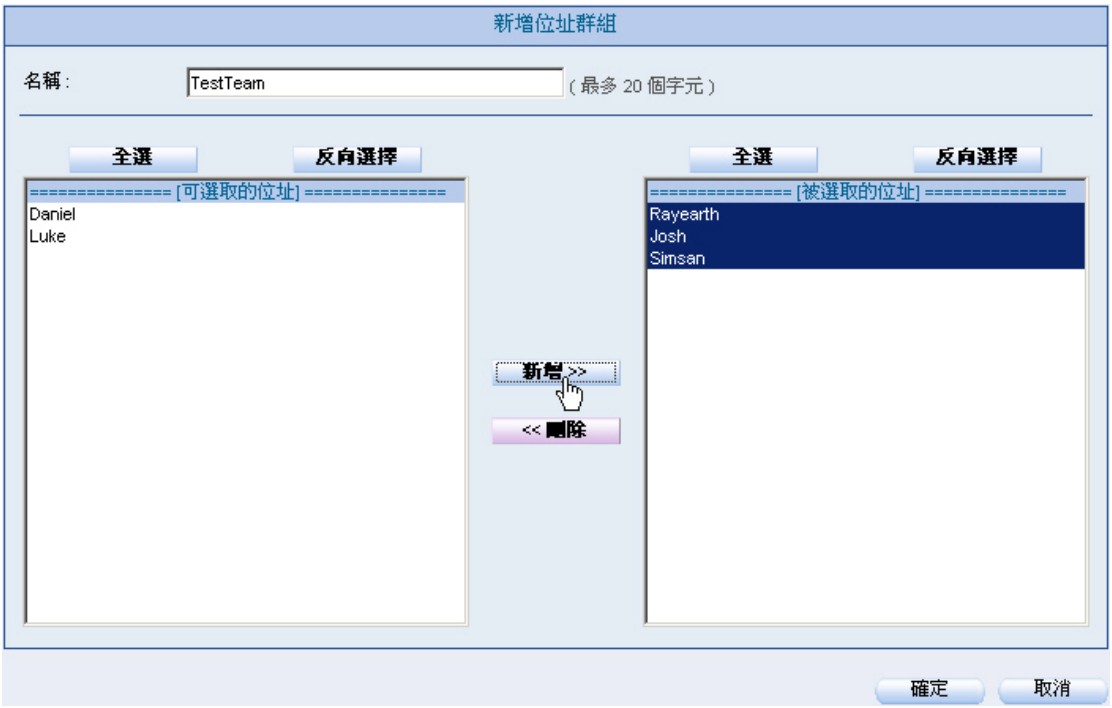


圖 4-6 設定內部網路位址群組

圖 4-7 完成內部網路位址群組設定

說明：

1. 【管制條例選項】>【位址表】>【外部網路群組】與【非軍事區群組】其設定模式與【內部網路群組】相同。

步驟3. 於【管制條例選項】>【位址表】>【外部網路】頁面中，做下列設定：（如圖 4-8）

- 輸入辨識【名稱】。
- 【IP 位址範圍】選擇以 IPv4 位址 / 子網路遮罩定義。
- 【網際協定】選擇 IPv4。
- 輸入特定的外部【IP 位址】。
- 【子網路遮罩】輸入 255.255.255.255。(代表 1 個 IP 位址)
- 按下【確定】鈕，完成設定。（如圖 4-9）

圖 4-8 設定外部網路位址表

圖 4-9 完成外部網路位址表設定

說明：

1. FQDN 查詢網址對應的 IP 位址之模式：

- 比對關鍵字：舉例來說，當 FQDN 設為 google，則會在使用者透過瀏覽器存取包含 google 字串的網址時，查詢其相映 IP 位址。
- 比對特定開頭網址：舉例來說，當 FQDN 設為^mail.google，則會在使用者透過瀏覽器存取以 mail.google 字串開頭的網址時，查詢其相映 IP 位址。
- 比對特定結尾網址：舉例來說，當 FQDN 設為 google.com$，則會在使用者透過瀏覽器存取以 google.com 字串結尾的網址時，查詢其相映 IP 位址。
- 比對與特定字串相符網址：舉例來說，當 FQDN 設為^mail.google.com$，則會在使用者透過瀏覽器存取完全符合 mail.google.com 字串的網址時，查詢其相映 IP 位址。

步驟4. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 4-10）

- 【來源網路位址】選擇所設定的內部網路位址群組規則。
- 【目的網路位址】選擇所設定的外部網路位址表規則。
- 按下【確定】鈕，完成設定。（如圖 4-11）

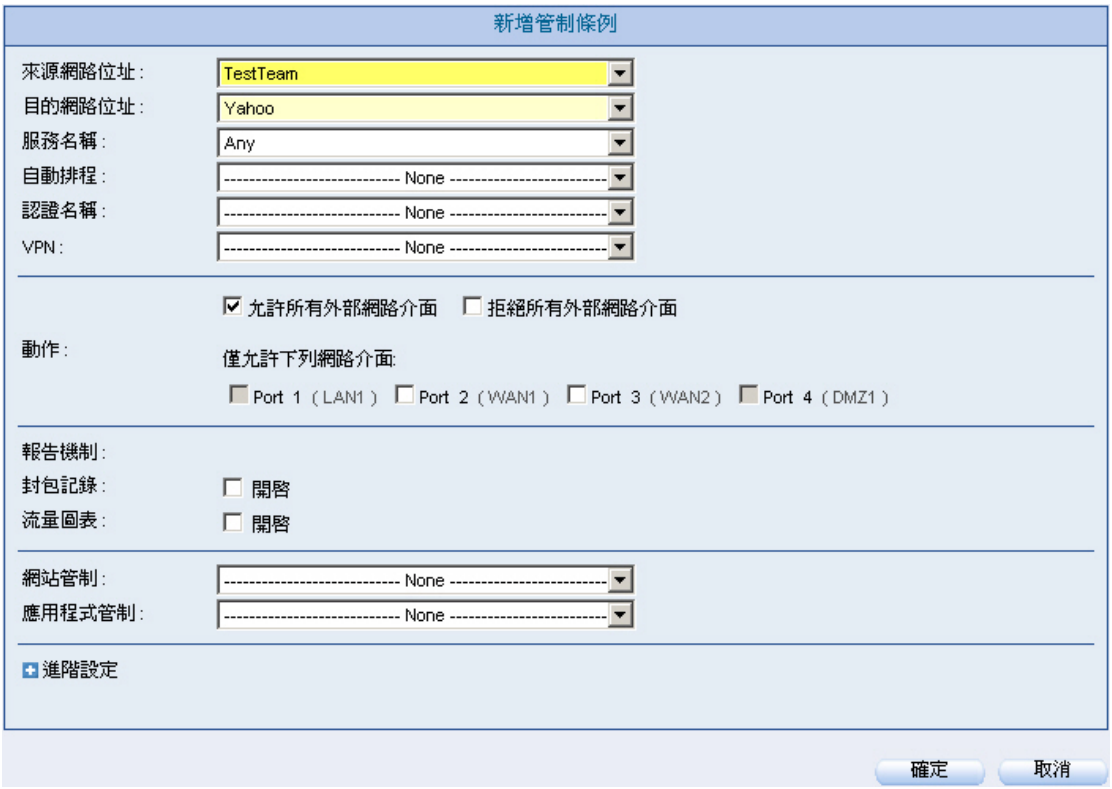


圖 4-10 管制條例套用位址表規則

圖 4-11 完成管制條例設定

說明：

1. 【位址表】規則必須套用至【管制條例】才會有實際作用。

第5章　服務表

TCP 協定和 UDP 協定提供各種不同的服務，每一個服務都有對應的 TCP 或 UDP 埠號，例如：TELNET(TCP 埠 23)、SMTP(TCP 埠 25)、POP3(TCP 埠 110)、…。MHG-2000 內建基本服務表和自訂服務表，以規範允許存取的網路資源。

- 【基本服務】：定義了常用的 TCP 或 UDP 服務，不能修改也不可刪除。
- 【自訂服務】：讓使用者可設定欲使用的特定 TCP 埠和 UDP 埠。

說明：

1. 在【管制條例選項】>【服務表】>【服務群組】頁面中，可將要允許或控管的服務整合為單一規則，以便於套用至管制條例。例如：有 1 個 IP 位址可以對伺服器存取 5 個不同的服務（HTTP、FTP、SMTP、POP3 和 TELNET），如果不使用服務群組功能，總共需制定 1x5=5 條管制條例；反之，則只需一條管制條例即可達到 5 條管制條例的作用。

【基本服務】功能概述：

基本服務 說明如下：

圖示	說明
ANY	任何 TCP、UDP 服務，如：Any。
ICMP	ICMP 協定，如：PING、Traceroute。
TCP	TCP 服務，如：AFPoverTCP、AOL、BGP、FINGER、FTP、GOPHER、HTTP、HTTPS、InterLocator、IRC、L2TP、LDAP、MSN、NetMeeting、NNTP、POP3、PPTP、Real-Media、RLOGIN、SMTP、SSH、TCP-Any、TELNET、VDO-Live、WAIS、WINFRAME、X-Windows。
UDP	UDP 服務，如：DNS、IKE、IMAP、NFS、NTP、PC-Anywhere、RIP、SNMP、SYSLOG、TALK、TFTP、UDP-Any、UUCP。

【自訂服務】功能概述：

名稱 說明如下：

- 系統管理員可在此為自訂的服務命名。

通訊協定 說明如下：

- 設備彼此之間溝通所需求之協定，一般常用為 TCP 和 UDP。

用戶端 說明如下：

- 用戶端電腦之網卡使用的埠號，建議使用預設範圍。

伺服器端 說明如下：

- 可在此輸入所要自訂服務之埠號。

5.1 自訂服務功能使用範例

5.1.1 透過管制條例允許外部使用者，經由網路電話設備和內部使用者彼此溝通。(VoIP 埠號：TCP 1720、TCP 15323-15333、UDP 15323-15333)

步驟1. 在【管制條例選項】>【位址表】>【內部網路】和【內部網路群組】頁面中，做下列設定：(如圖 5-1, 圖 5-2)

圖 5-1 內部網路位址表設定

圖 5-2 內部網路位址群組設定

步驟2. 在【管制條例選項】>【服務表】>【自訂服務】頁面中，做下列設定：（如圖 5-3）

- 輸入指定服務【名稱】。
- 【通訊協定#1】選擇 TCP，【用戶端】不變，【伺服器端】輸入 1720：1720。
- 【通訊協定#2】選擇 TCP，【用戶端】不變，【伺服器端】輸入 15328：15333。
- 【通訊協定#3】選擇 UDP，【用戶端】不變，【伺服器端】輸入 15328：15333
- 按下【確定】鈕，完成設定。（如圖 5-4）

圖 5-3 設定自訂服務

圖 5-4 完成自訂服務設定

說明：

1. 在一般的情況下，用戶端電腦之網路卡的埠號，其範圍為 0-65535。建議不要修改【自訂服務】的【用戶端】範圍。
2. 在界定埠號範圍的兩個空格內輸入不同數值，代表開啟此一區間埠號（如 15328：15333）；若兩個空格內輸入相同數值，代表開啟單一埠號（如 1720：1720）。

步驟3. 將完成的【管制條例選項】>【服務表】>【自訂服務】設定，套用至【管制條例選項】>【虛擬伺服器】>【連接埠對應】。（如圖 5-5）

圖 5-5 虛擬伺服器套用自訂服務項目

步驟4. 在【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 5-6）

- 【目的網路位址】選擇所設定的虛擬伺服器規則。
- 【服務名稱】選擇所設定的自訂服務規則。
- 按下【確定】鈕，完成設定。（如圖 5-7）

圖 5-6 設定外部對內部 VoIP 溝通之管制條例

圖 5-7 完成管制條例設定

步驟5. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 5-8）

- 【來源網路位址】選擇所設定的內部網路位址群組規則。
- 【服務名稱】選擇所設定的自訂服務規則。
- 【動作】勾選 Port2（WAN1）。
- 按下【確定】鈕，完成設定。（如圖 5-9）

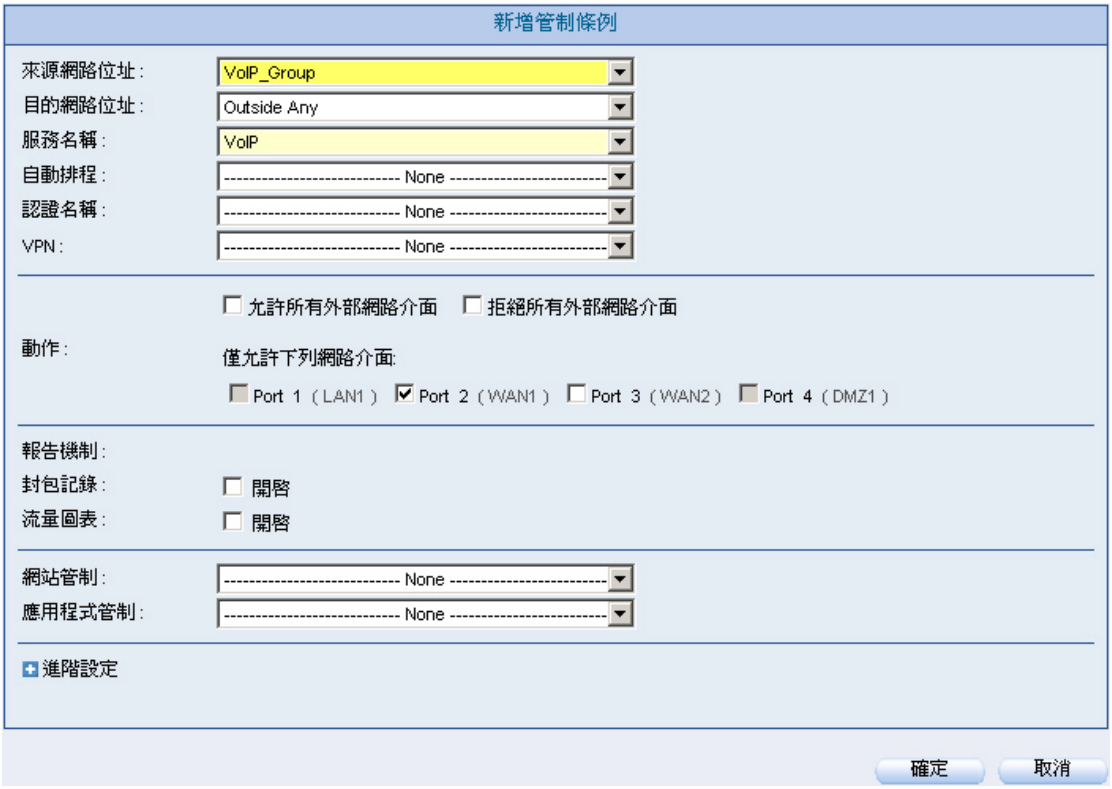


圖 5-8 設定內部對外部 VoIP 溝通之管制條例

圖 5-9 完成管制條例設定

說明：

1. 【服務表】必須配合【管制條例】與【管制條例選項】>【虛擬伺服器】使用才有實際作用。

5.2 服務群組功能使用範例

5.2.1 將所需的服務群組化，並限制特定使用者僅能透過管制條例上網存取此群組提供之服務資源。（群組：HTTP、POP3、SMTP、DNS）

步驟1. 在【管制條例選項】>【服務表】>【服務群組】頁面中，做下列設定：（如圖 5-10）

- 輸入指定服務【群組名稱】。
- 將【可選取的服務】（HTTP、POP3、SMTP、DNS）新增至【被選取的服務】清單中。
- 按下【確定】鈕，完成設定。（如圖 5-11）

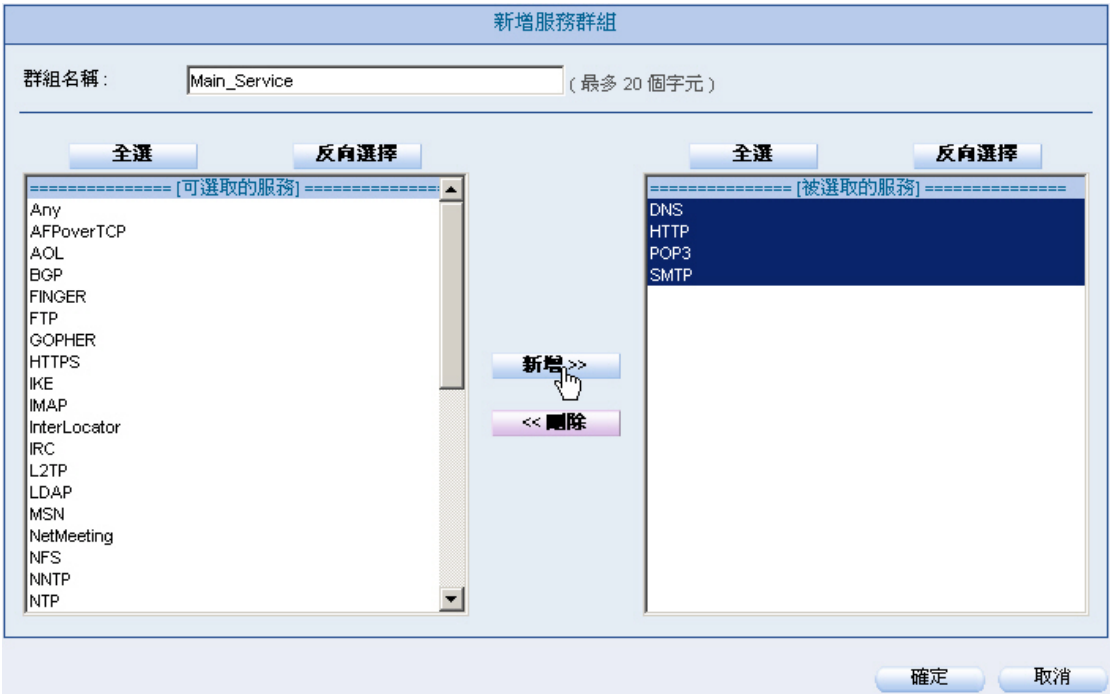


圖 5-10 設定服務群組

圖 5-11 完成服務群組設定

步驟2. 在【管制條例選項】>【位址表】>【內部網路群組】頁面中，設定一僅能上網存取特定服務之位址群組。（如圖 5-12）

圖 5-12 位址表群組設定

步驟3. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 5-13）

- 【來源網路位址】選擇所設定的內部網路位址群組規則。
- 【服務名稱】選擇所設定的服務群組規則。
- 按下【確定】鈕，完成設定。（如圖 5-14）

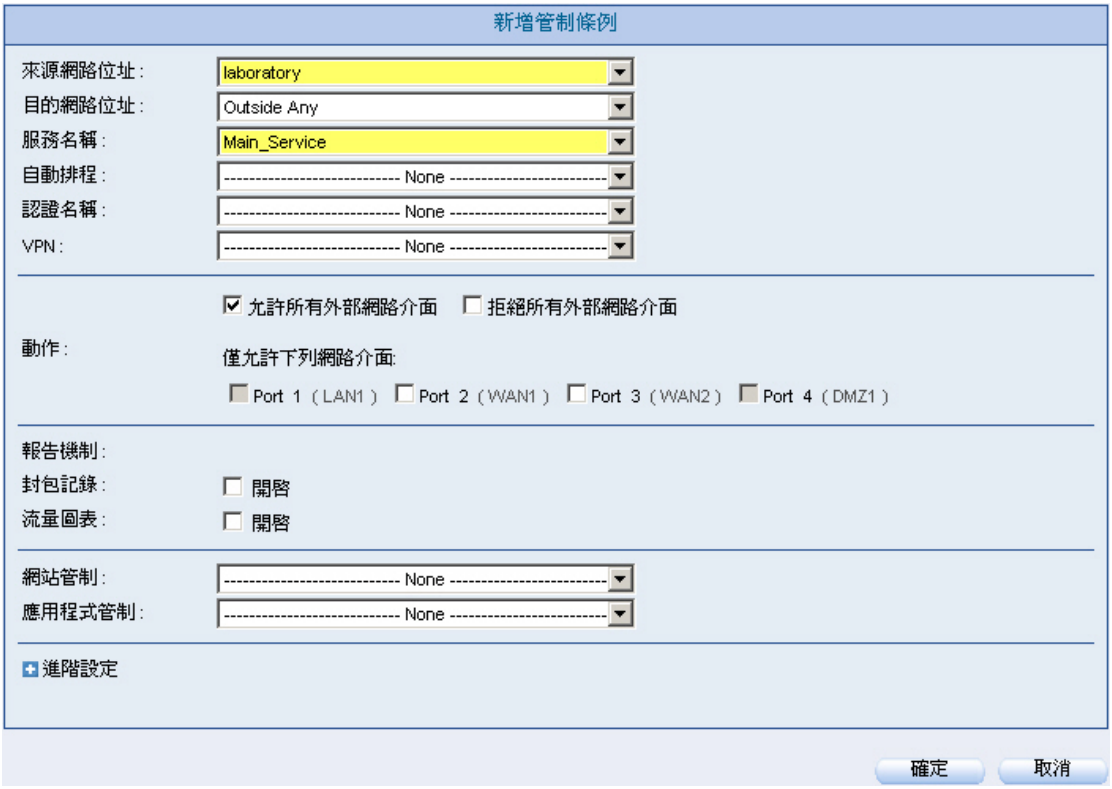


圖 5-13 設定特定使用者存取指定網路服務之管制條例

圖 5-14 完成管制條例設定

第6章　排程表

用來安排 MHG-2000 管制條例的執行時段，以便於管理網路來發揮其最大效能。

【設定】功能概述：

名稱 說明如下：

- 排程規則的辨識名稱。

排程模式 說明如下：

- 排程規則的運作模式可為：
  - 循環：以一週為基準，個別定義星期一～星期日每天的時段，讓套用此排程的管制條例持續按時管理上網權限。
  - 一次：依照年、月、日、時、分定義一期限，讓套用此排程的管制條例僅在此期限內管理上網權限。

6.1 排程表功能使用範例

6.1.1 規劃內部使用者一週中每天透過管制條例，存取網路資料的有效時段

步驟1. 在【管制條例選項】>【排程表】>【設定】頁面中，做下列設定：

- 按下【新增】鈕。
- 輸入指定的第一段排程【名稱】。
- 選擇指定的第一段【排程模式】。
- 使用下拉式選單安排每天的第一運作時段。
- 按下【確定】鈕。（如圖 6-1）
- 再次按下【新增】鈕。
- 輸入指定的第二段排程【名稱】。
- 選擇指定的第二段【排程模式】。
- 使用下拉式選單安排每天的第二運作時段。
- 按下【確定】鈕，完成設定。（如圖 6-2, 圖 6-3）

圖 6-1 設定第一條排程表規則

圖 6-2 設定第二條排程表規則

圖 6-3 完成排程表設定

步驟2. 在【管制條例選項】>【排程表】>【排程群組】頁面中，做下列設定：（如圖 6-4）

- 輸入指定排程【群組名稱】
- 將【可選取的排程】（Rest_01、Rest_02）新增至【被選取的排程】清單中。
- 按下【確定】鈕，完成設定。（如圖 6-5）

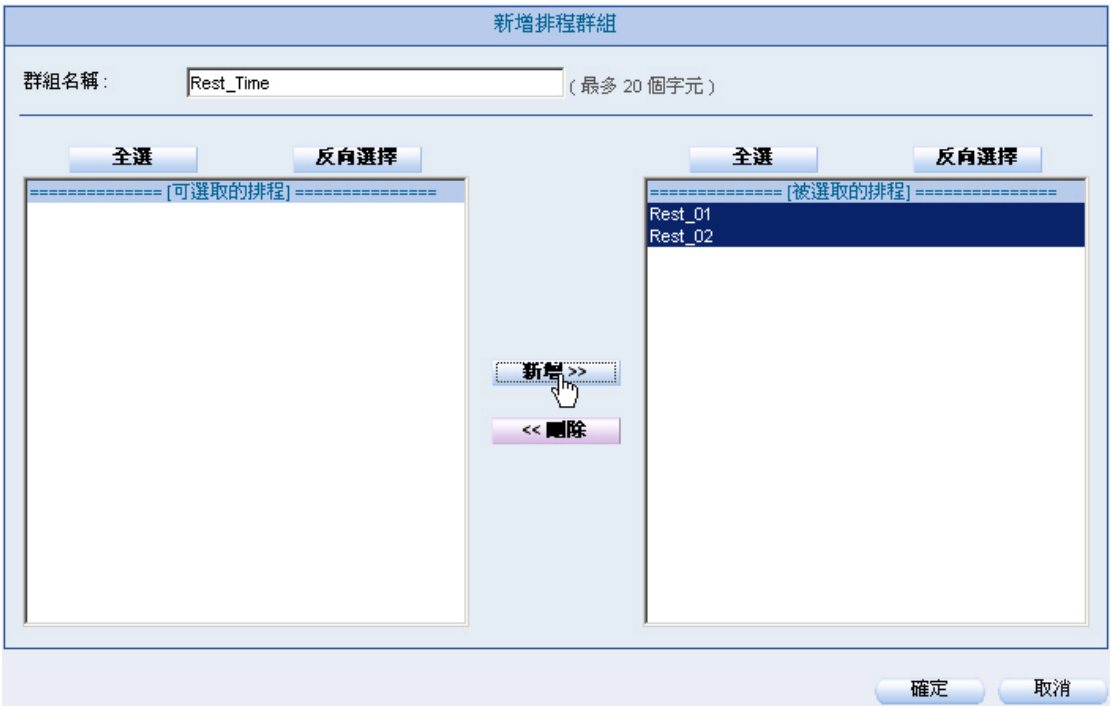


圖 6-4 設定排程群組

圖 6-5 完成排程群組設定

步驟3. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 6-6）

- 【自動排程】選擇所設定的排程表規則。
- 按下【確定】鈕，完成設定。（如圖 6-7）

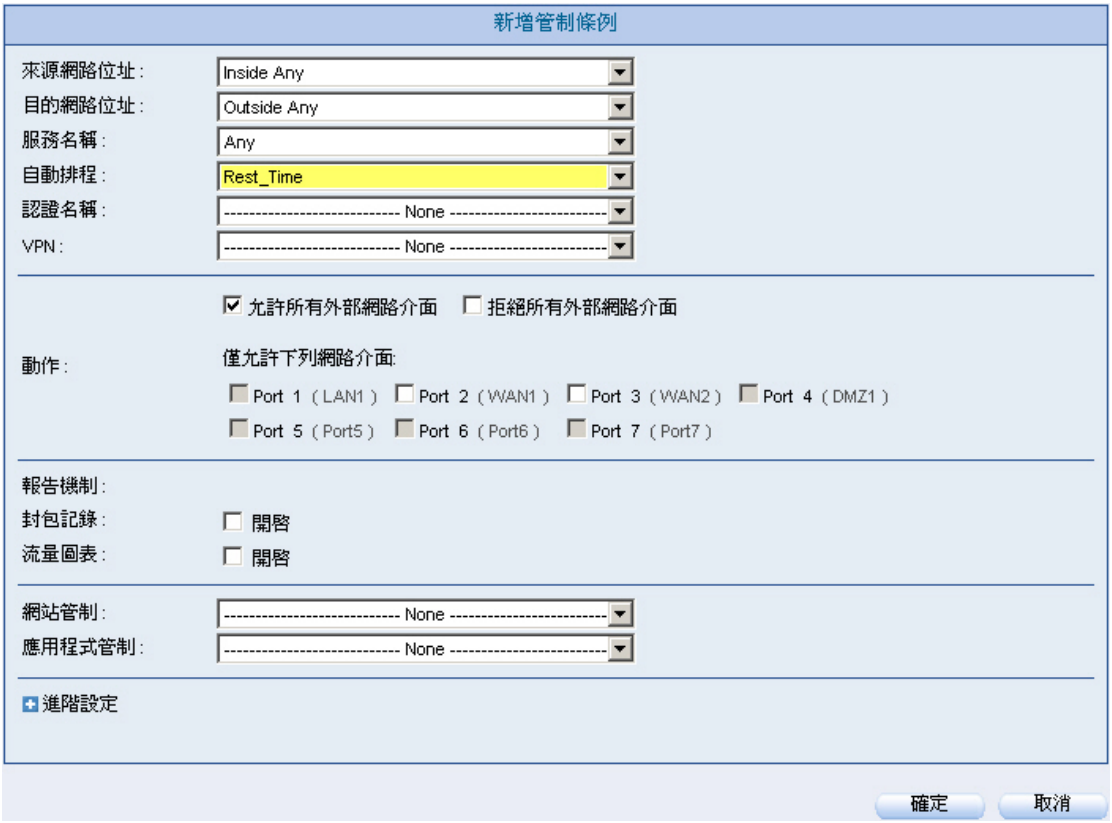


圖 6-6 管制條例套用排程規則

圖 6-7 完成管制條例設定

第7章　頻寬表

用來控管透過 MHG-2000 存取網路資源所使用的頻寬。可藉由管制條例運用適合的頻寬管理規則，有效分配、充分利用所能使用的頻寬。**（如圖 7-1, 圖 7-2）**

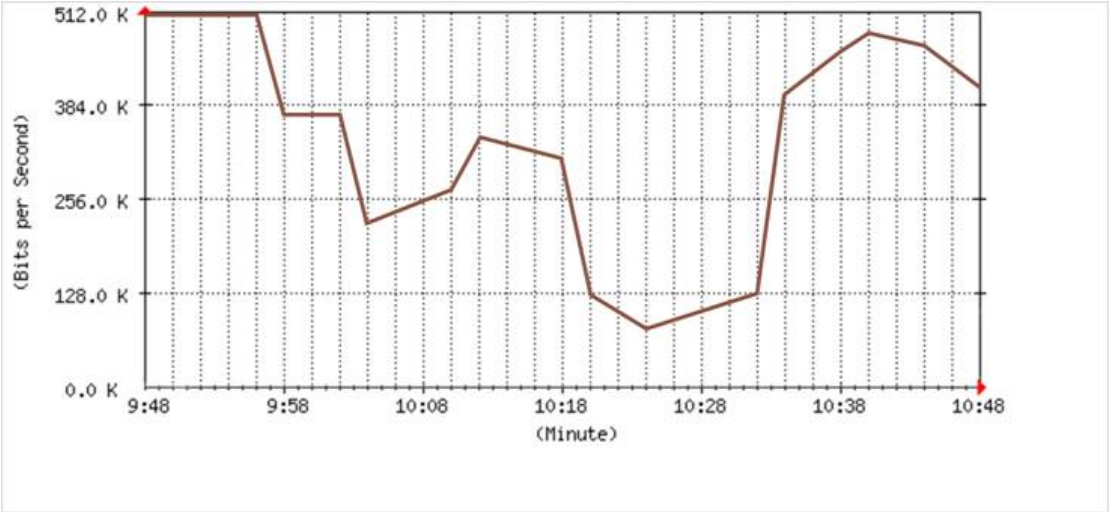


圖 7-1 未經頻寬管理的網路流量

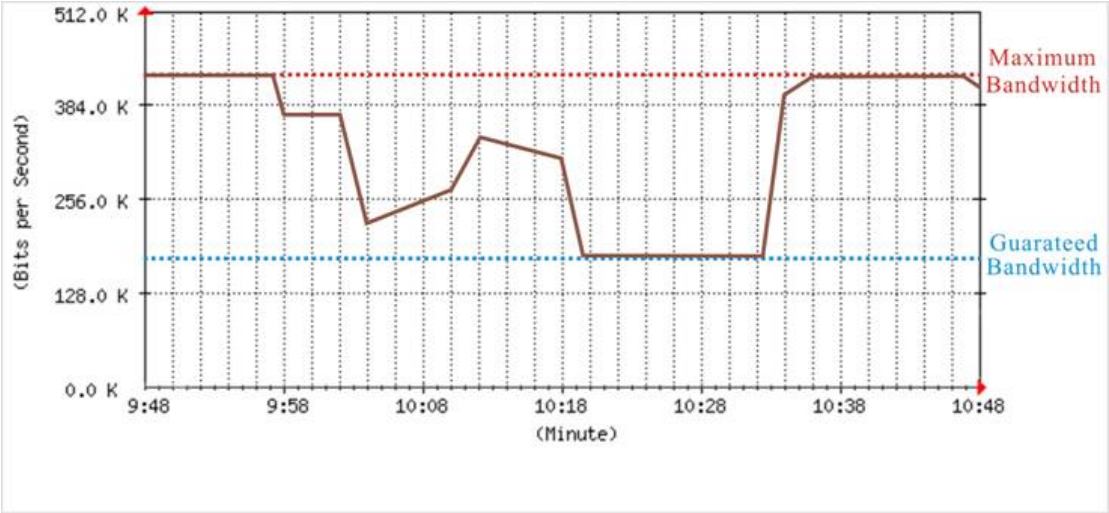


圖 7-2 經頻寬管理後的網路流量（最大頻寬：400 Kbps, 保證頻寬：200Kbps）

【設定】功能概述：

名稱 說明如下：

- 頻寬管制規則的辨識名稱。

網路介面 說明如下：

- 指設定為外部網路介面的網路埠。

下載頻寬 說明如下：

- 設定可運用的線路保證及最大下載頻寬。

上傳頻寬 說明如下：

- 設定可運用的線路保證及最大上傳頻寬。

優先權 說明如下：

- 設定未使用的下載和上傳頻寬分配優先權。

保證頻寬 說明如下：

- 在管制規則中，可使用的線路基本頻寬。

最大頻寬 說明如下：

- 在管制規則中，可使用的線路最大頻寬。

7.1 頻寬表功能使用範例

7.1.1 設定一條能限定使用者上傳與下載頻寬之管制條例

步驟1. 在【管制條例選項】>【頻寬表】>【設定】頁面中，做下列設定：（如圖 7-3）

- 輸入頻寬表【名稱】。
- 在【網路介面】2（WAN1）、3（WAN2）中，輸入所要限定之頻寬大小。
- 選擇頻寬表之【優先權】。
- 按下【確定】鈕，完成設定。（如圖 7-4）

圖 7-3 設定頻寬表

1 / 1 移至
名稱
網路介面
下載頻寬
上傳頻寬
優先權
變更
Policy_QoS
1 (LAN1)
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
2 (WAN1)
保證頻寬 = 200 Kbps
最大頻寬 = 400 Kbps
保證頻寬 = 200 Kbps
最大頻寬 = 400 Kbps
3 (WAN2)
保證頻寬 = 300 Kbps
最大頻寬 = 400 Kbps
保證頻寬 = 50 Kbps
最大頻寬 = 64 Kbps
4 (DMZ1)
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
中
修改
刪除
5 (Port5)
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
6 (Port6)
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
7 (Port7)
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
保證頻寬 = 0 Kbps
最大頻寬 = 0 Kbps
1 / 1 移至
新增

圖 7-4 完成頻寬表設定

步驟2. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 7-5）

- 【頻寬管理】選擇所設定的頻寬表規則。
- 按下【確定】鈕，完成設定。（如圖 7-6）

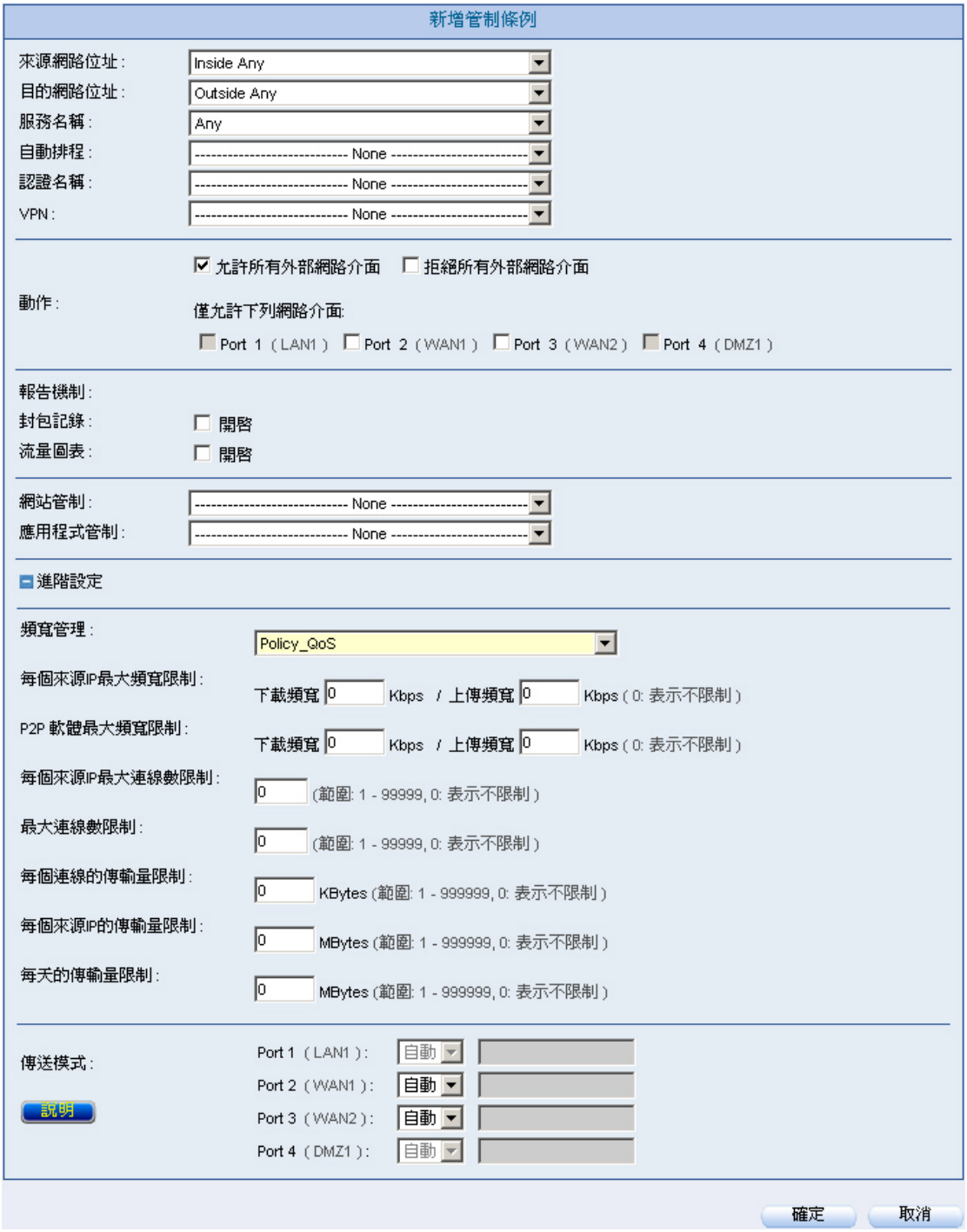


圖 7-5 管制條例套用頻寬管理規則

圖 7-6 完成管制條例設定

說明：

1. 系統管理員設定【頻寬表】的根據，即【網路介面】>【介面位址】頁面中，設定為外部網路介面的【下載頻寬】與【上傳頻寬】，故系統管理員務必準確設定其上傳、下載頻寬。

第8章　認證表

採用內建認證帳戶、群組，和外部 RADIUS、POP3、LDAP 伺服器等驗證機制，來控管透過 MHG-2000 存取網路資源的權限。

【認證設定】功能概述：

認證管理 說明如下：

- 提供系統管理員進行 MHG-2000 認證機制的基本設定：
  - 【認證埠號】：當 MHG-2000 啟用認證機制時，內部使用者需透過指定的埠號進行認證，預設為 82。
  - 【允許連線閒置時間】：當內部使用者經認證連到外部網路時，可設定其認證後的連線閒置時間，超過設定的時間，認證即會自動失效，預設為 30 分鐘。
  - 【認證成功後可使用時間】：當內部使用者經認證連到外部網路時，可由此限制其認證連線的可用時間，超過設定的時間，認證即會自動失效。
  - 【關閉自動導向認證畫面】：當內部使用者欲認證連到外部網路時，需自行開啟指定認證頁面（於瀏覽器網址列輸入 http://MHG-2000 內部網路介面 IP 位址:所設定的認證埠號），進行授權驗證作業。
  - 【使用者可以進行密碼變更】：當啟用此功能時，允許透過【認證帳戶】進行認證的使用者，自行變更認證登入的密碼。
  - 【不允許相同帳號重複認證】：當啟用此功能並透過用戶、群組、RADIUS、POP3 或 LDAP 來進行認證動作時，已經被使用的認證帳號不可再被他人使用。
  - 【啟動記錄 / 報告以認證名稱取代來源位址顯示】：用來將認證使用者上網行為，以其認證名稱來辨識、儲存。（例如：網站管制報告、封包記錄、應用程式管制記錄、…）
  - 【顯示認證介面前，所重新連結的網站】：將欲連線認證頁面的內部使用者，直接導向指定的網站（建置的網頁有內嵌連回 MHG-2000 進行認證的介面）。
  - 【認證成功後，所重新連結的網站】：將通過認證的內部使用者，直接導向指定的網站，預設為空值（會直接連到使用者所要登入的網站）。
  - 【請上傳認證介面背景圖檔】：用來更改認證頁面的背景圖示。
  - 【認證介面顯示訊息】：可在開啟認證頁面時，顯示指定訊息（支援 HTML 語法），預設為空值（顯示系統預設的訊息）。
  - 【認證成功顯示訊息】：可在認證成功時，於認證頁面中顯示指定訊息（支援 HTML 語法），預設為空值（顯示系統預設的訊息）。
  - 【認證失敗顯示訊息】：可在認證失敗時，於認證頁面中顯示指定訊息（支援 HTML 語法），預設為空值（顯示系統預設的訊息）。
    - 在【管制條例選項】>【認證表】>【認證設定】頁面中，做下列設定：**（如圖 8-1）**

圖 8-1 認證管理設定頁面

- 當使用者透過認證連到外部網路時，會出現如下之畫面：**（如圖 8-2）**

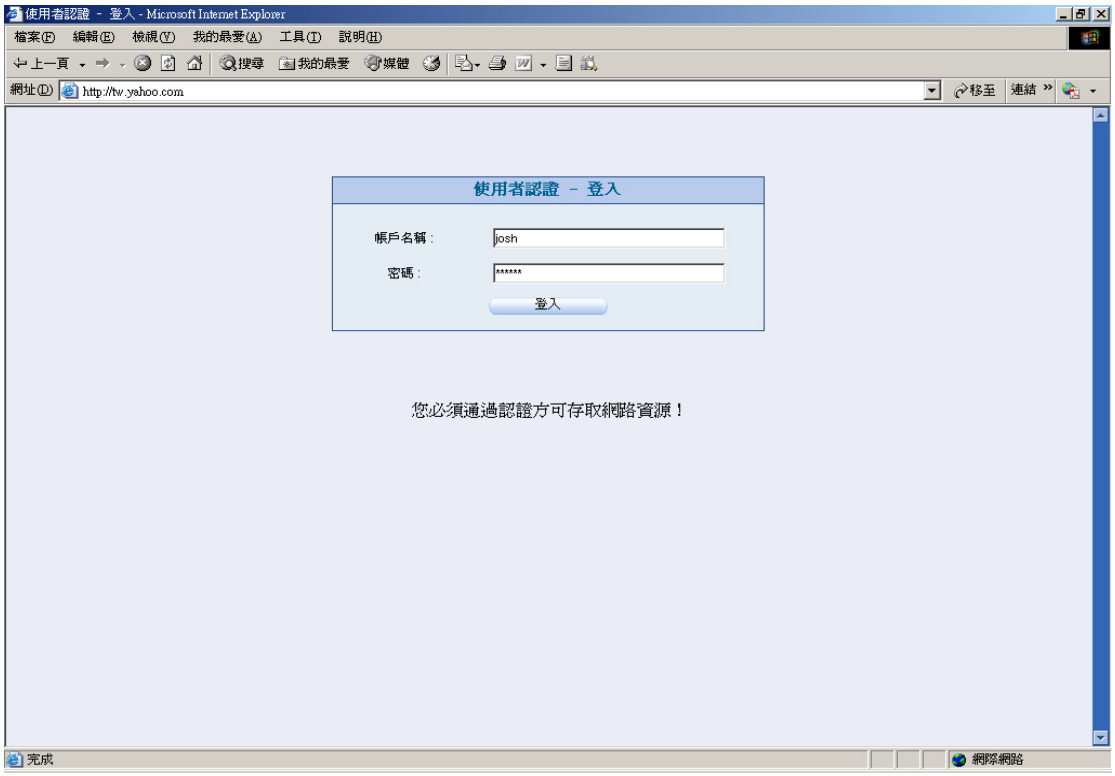


圖 8-2 認證登入頁面

- 經過認證後，會連到指定網站：**（如圖 8-3）**

圖 8-3 認證後連結的指定網站

說明：

1. 密碼變更功能只適用於變更【認證帳戶】密碼。
2. 使用者如欲直接進行認證動作，可於瀏覽器網址列輸入 http://MHG-2000 內部網路介面 IP 位址:所設定的認證埠號，即可連線認證頁面。
3. 網站管制報告要於【啟動記錄 / 報告以認證名稱取代來源位址顯示】機制後的隔天，才會以使用者認證名稱來辨識、儲存相關記錄。
4. 如需透過外部網頁連回 MHG-2000 進行認證上網授權，並顯示自訂認證訊息，必須做下列設定：
   - 【顯示認證介面前，所重新連結的網站】輸入指定網頁（包含導向內嵌 MHG-2000 認證介面的網頁連結，例如：http://指定外部伺服器 IP/auth_to.html）的 URL（例如：http://指定外部伺服器 IP/auth.html）。
   - 輸入指定【認證介面顯示訊息】、【認證成功顯示訊息】(必須複製一份系統預設訊息再加以修改)、【認證失敗顯示訊息】(必須複製一份系統預設訊息再加以修改)。**(如圖 8-4)**
   - 當使用者連線認證頁面時，會被直接導向指定網頁，再透過其開啟內嵌 MHG-2000 認證介面的網頁（以系統預設認證頁面加以修改）。**(如圖 8-5)**
     - 輸入正確的認證【帳戶名稱】和【密碼】，會顯示自訂認證成功訊息。**(如圖 8-6, 圖 8-7)**
     - 輸入錯誤的認證【帳戶名稱】或【密碼】，會顯示自訂認證失敗訊息。**(如圖 8-8, 圖 8-9)**

圖 8-4 認證管理設定頁面

圖 8-5 開啟外部伺服器特定網頁

圖 8-6 輸入正確認證資料

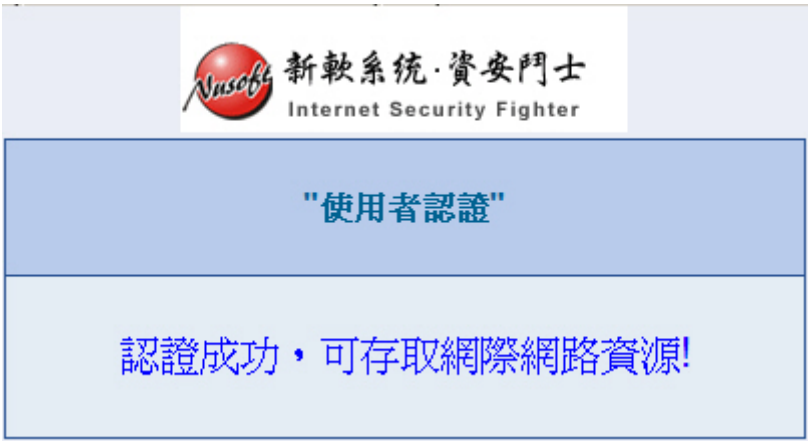


圖 8-7 顯示認證成功訊息

圖 8-8 輸入錯誤認證資料

圖 8-9 顯示認證失敗訊息

【認證帳戶】功能概述：

帳戶名稱 說明如下：

- 用於設定系統內建之認證使用者帳號。

密碼 說明如下：

- 建立認證時所需要的密碼。

確認密碼 說明如下：

- 輸入與密碼欄一致的字串。

使用者必須在下次登入時變更密碼 說明如下：

- 於啟用此後能後，內建認證帳戶進行首次認證時，會強制其變更認證密碼。

認證帳號有效日期 說明如下：

- 設定內建認證帳戶的使用期限。

【外部 RADIUS】功能概述：

共用密碼 說明如下：

- MHG-2000 進行認證時連線 RADIUS 伺服器所需要的密碼。

802.1x RADIUS 說明如下：

- 讓 MHG-2000 透過 RADIUS 進行 802.1x（連接埠架構式網路存取控制）驗證。

RADIUS 帳號 說明如下：

- MHG-2000 連線 RADIUS 伺服器所取得的帳戶清單，可將各帳戶依需求進行群組來提供授權認證。

【外部 LDAP】功能概述：

搜尋依據 說明如下：

- LDAP 伺服器的識別名稱。

篩選條件 說明如下：

- 用來指定 LDAP 伺服器中特定類別的帳號。

帳戶名稱 說明如下：

- MHG-2000 進行認證時連線 LDAP 伺服器所需要的帳號。

LDAP 使用者名稱 說明如下：

- MHG-2000 連線 LDAP 伺服器所取得的帳戶清單，可將各帳戶依需求進行群組來提供授權認證。

【動態密碼】功能概述：

動態密碼設定 說明如下：

- 動態密碼又稱一次性密碼（One Time Password，簡稱 OTP），是指只能使用一次的密碼。一般的靜態密碼容易因為木馬、鍵盤側錄程式、...而被竊取，為了解決此狀況而產生此機制和應用。
- 動態密碼的產生方式，主要是以時間差做為伺服器與密碼產生器的同步條件。在需要登錄的時候，就利用密碼產生器產生一次性密碼，動態密碼一般分為：
  - 計次制：由用戶端系統計數器決定的動態數值（Token）搭配 PIN 或 KEY，以特殊公式演算並擷取出 6~8 字元的密碼，沒有時間限制，但經使用後立即失效。
  - 計時制：由用戶端系統時間決定的動態數值（Token）搭配 PIN 或 KEY，以特殊公式演算並擷取出 6~8 字元的密碼，超過設定的有效使用時間就立即失效。
- 於行動裝置（例如：搭載 iOS、Android 系統的手機）可安裝搭配 MHG-2000 的專屬動態密碼客戶端 APP（NUSOFT OTP），並利用下列資訊產生認證所需的計時制一次性密碼：
  - 【PIN】：用來產生、驗證動態密碼的個人識別碼（Personal Identification Number，簡稱 PIN）。
  - 【KEY】：用來產生、驗證動態密碼的金鑰（Authentication Key）。
- 可結合 MHG-2000 認證、SSL Web VPN 連線機制，在存取網路資源時除了輸入驗證帳號、密碼外，還需要再輸入第二組驗證碼（動態密碼），以提高授權帳號的安全性。
  - 在【管制條例選項】>【認證表】>【動態密碼】頁面中，做下列設定：（如圖 8-10）
    - 輸入指定的【PIN】、【KEY】。
    - 選擇指定的【登入有效時間】。
    - 勾選【認證機制使用動態密碼】、【SSL Web VPN 連線使用動態密碼】。
    - 按下【確定】鈕，完成設定。

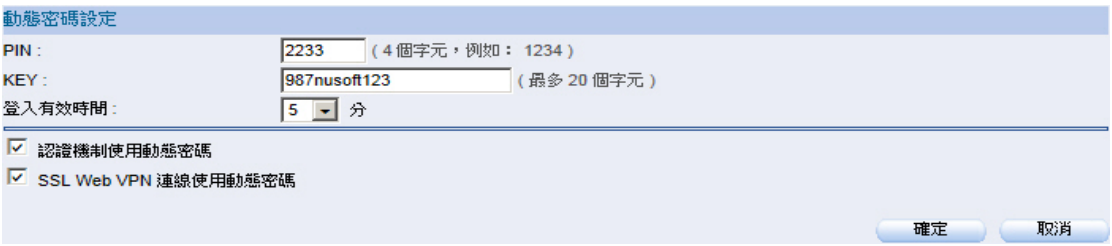


圖 8-10 動態密碼設定頁面

◆ 在行動裝置安裝 NUSOFT OTP APP 後，輸入在 MHG-2000 設定的【PIN】、【KEY】，以產生動態密碼（每分鐘自動產生新密碼）。**（如圖 8-11, 圖 8-12, 圖 8-13）**

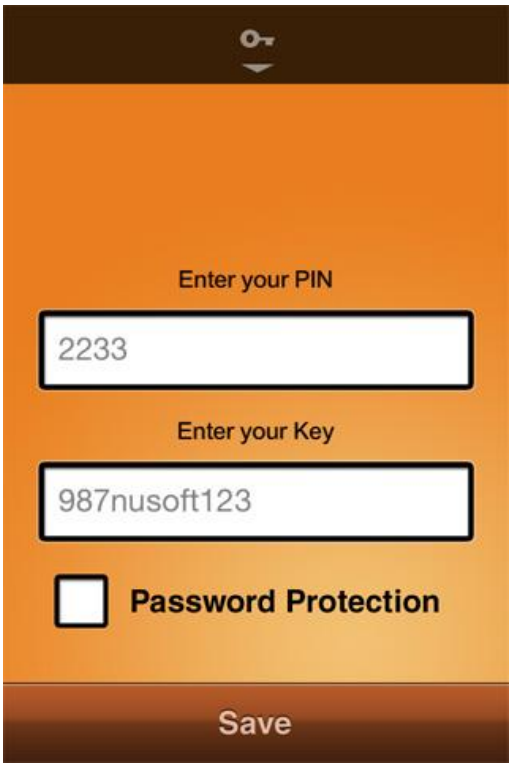


圖 8-11 於 NUSOFT OTP APP 輸入 PIN 和 KEY

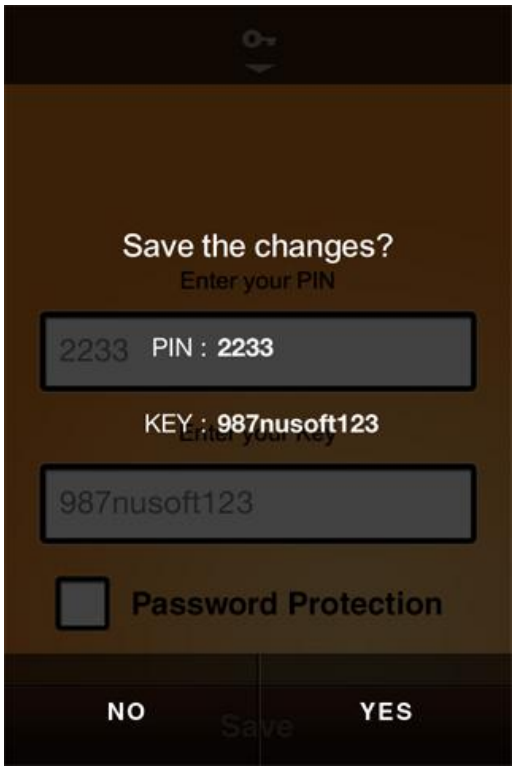


圖 8-12 儲存輸入 NUSOFT OTP APP 的 PIN 和 KEY

圖 8-13 透過 NUSOFT OTP APP 產生動態密碼

◆ 當使用者透過認證連到外部網路時，會出現如下之畫面：（如圖 8-14）

圖 8-14 認證登入頁面

◆ 當使用者和 MHG-2000 建立 SSL Web VPN 連線時，會出現如下之畫面：（如圖 8-15）

圖 8-15SSL Web VPN 連線驗證頁面

注意：

1. 使用動態密碼機制時，MHG-2000（伺服器端）和行動裝置（客戶端）務必先連線同一網路時間伺服器，來同步系統時間。

8.1 認證帳戶和群組功能使用範例

8.1.1 規劃內部使用者必須通過管制條例之認證機制，方可連線至外部網路。(採用內建的認證帳戶和認證群組)

步驟1. 在【管制條例選項】>【認證表】>【認證帳戶】頁面中，建立多筆認證帳戶。(如圖 8-16)

圖 8-16 認證帳戶設定

說明：

1. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 MHG-2000【認證帳戶】名單錯亂時，可清除名單表重新【匯入】。
2. 建議使用者將電腦網卡的慣用 DNS 伺服器設定，指向 MHG-2000 的內部網路介面位址，以便於使用認證機制。

步驟2. 在【管制條例選項】>【認證表】>【認證群組】頁面中，做下列設定：（如圖 8-17）

- 輸入認證群組【名稱】。
- 將指定【可選取的帳戶】新增至【被選取的帳戶】清單中。
- 按下【確定】鈕，完成設定。

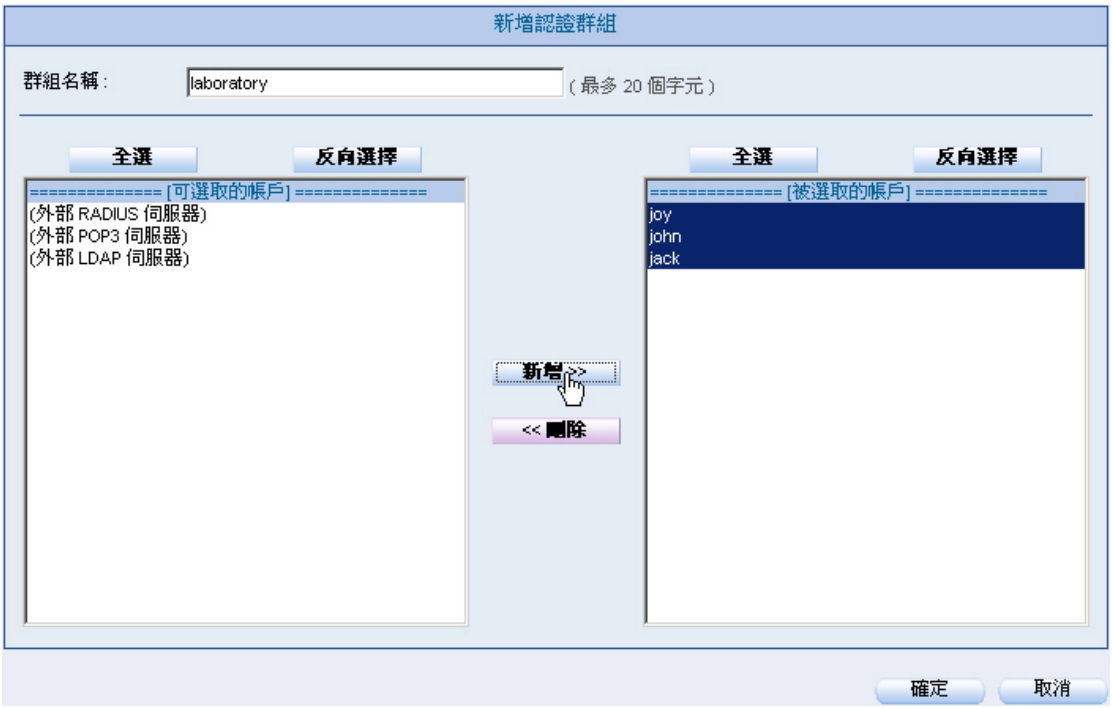


圖 8-17 認證群組設定頁面

步驟3. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 8-18）

- 【認證名稱】選擇所設定的認證群組規則。
- 按下【確定】鈕，完成設定。（如圖 8-19）

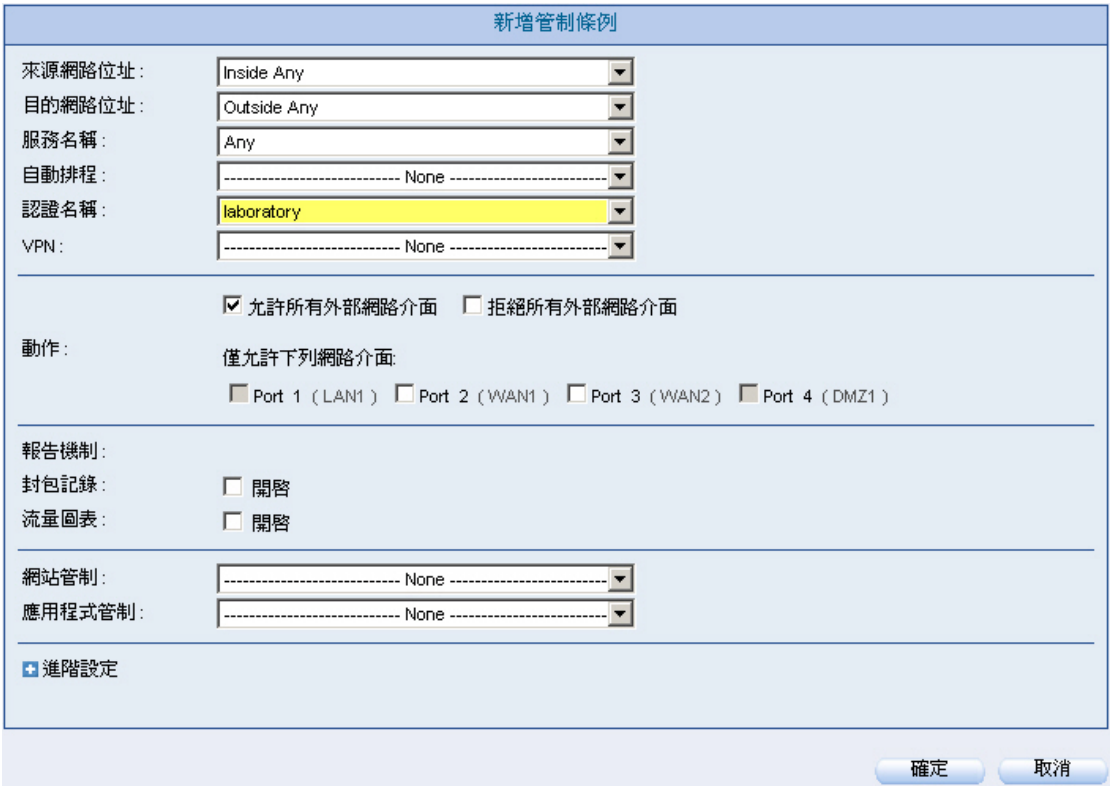


圖 8-18 管制條例套用認證規則

圖 8-19 完成管制條例設定

步驟4. 當內部使用者欲透過設定的認證管制條例瀏覽網頁時，即會先行連線認證頁面。在輸入正確的認證【帳戶名稱】和【密碼】後，按下【登入】鈕即可透過 MHG-2000 上網。（如圖 8-20）

圖 8-20 認證登入頁面

步驟5. 如使用者欲登出認證時，可於【使用者認證-登出】視窗（通過認證時會跳出），或於【使用者認證-登出】頁面（http:// 內部介面位址：認證埠號 / logout.html），按下【登出】鈕。（如圖 8-21）

圖 8-21 登出認證視窗

8.2 RADIUS 認證功能使用範例

8.2.1 規劃使用者必須通過管制條例之認證機制，方可連線至外部網路。【採用外部 RADIUS Server（Windows 2008 Server 內建）認證】

※ Windows 2008 RADIUS Server 設置方法

步驟1. 在【開始】>【程式集】>【系統管理工具】>【伺服器管理員】視窗中，點選【角色】項目，以確定安裝【網路原則伺服器】。（如圖 8-22，圖 8-23）

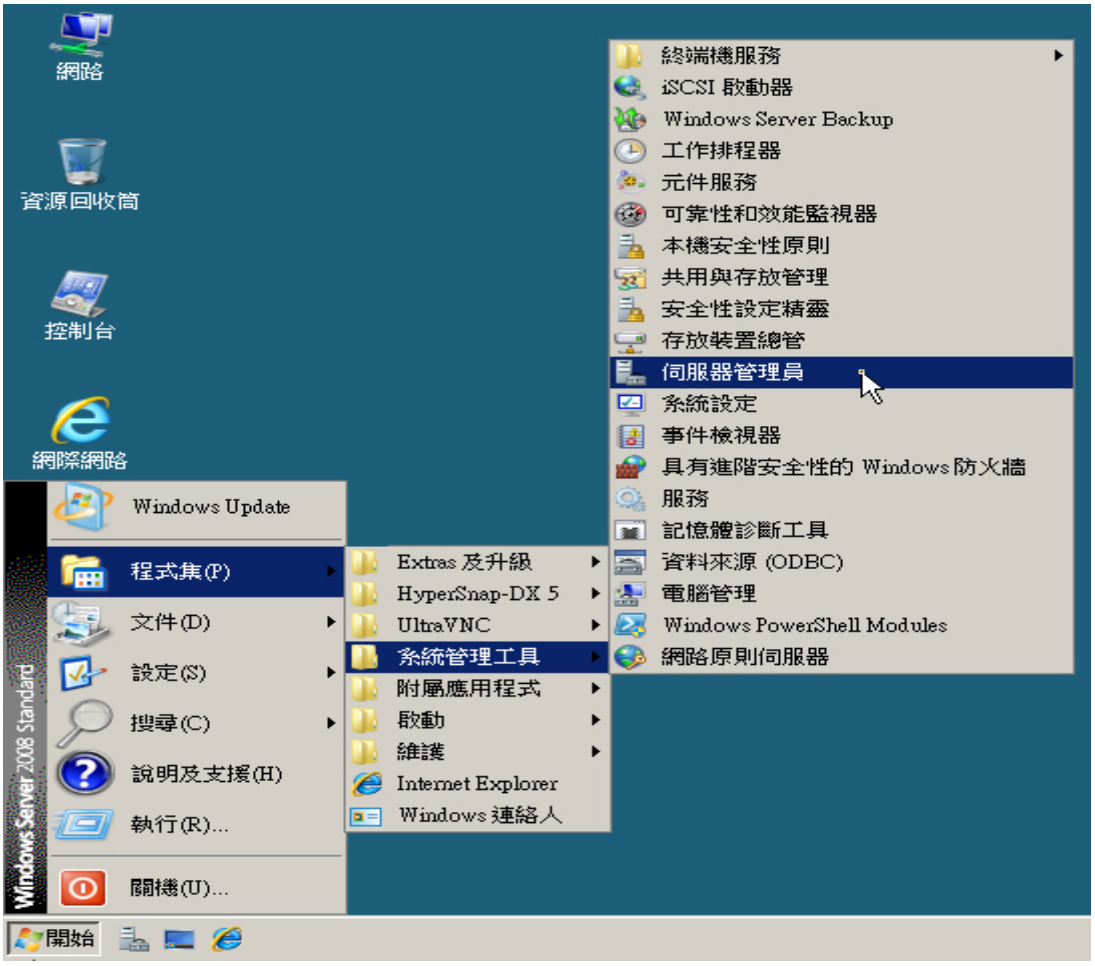


圖 8-22 開啟伺服器管理員視窗

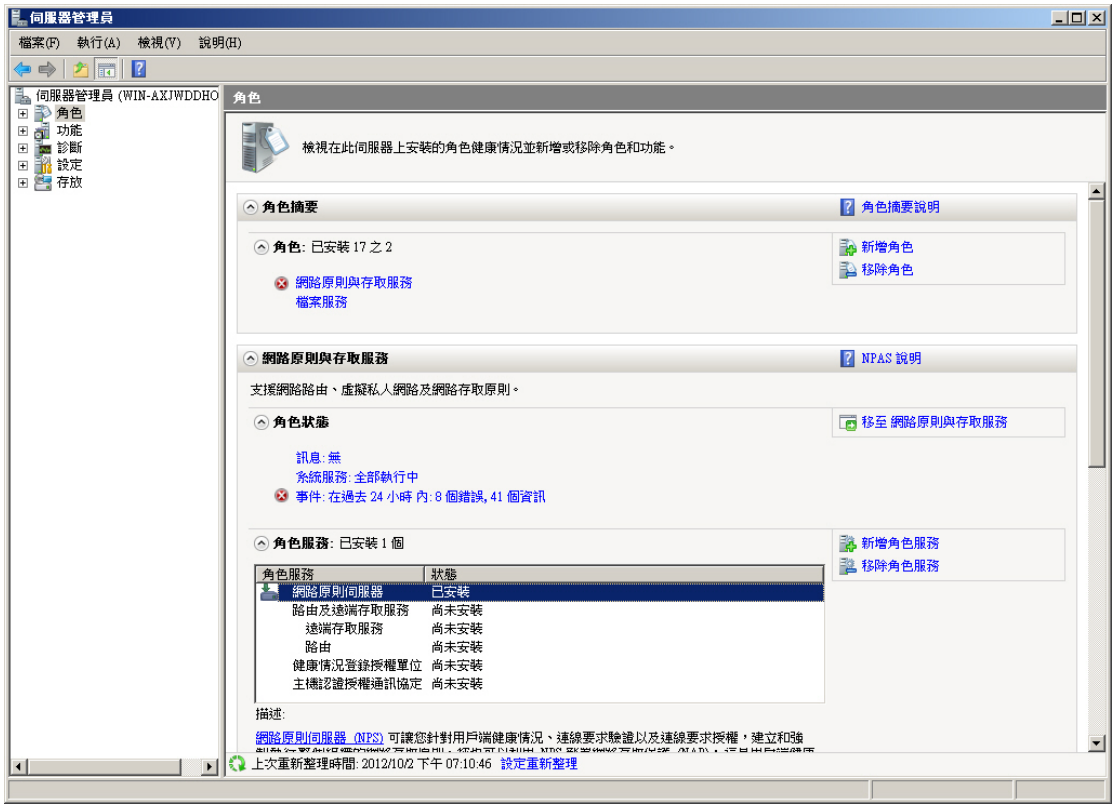


圖 8-23 確認已安裝網路原則伺服器

步驟2. 在【開始】>【程式集】>【系統管理工具】>【網路原則伺服器】視窗中，做下列設定：**（如圖 8-24）**

- 在【NPS（本機）】>【RADIUS 用戶端及伺服器】>【RADIUS 用戶端】項目上，按下滑鼠右鍵並選擇【新增 RADIUS 用戶端】。**（如圖 8-25）**
- 在【新增 RADIUS 用戶端】視窗中：**（如圖 8-26）**
  - 勾選【啟用此 RADIUS 用戶端】。
  - 輸入指定【好記的名稱】。
  - 輸入 MHG-2000【位址（IP 或 DNS）】。
  - 【廠商名稱】選擇 RADIUS Standard。
  - 【手動】輸入指定【共用密碼】、【確認共用密碼】。
  - 按下【確定】鈕，完成設定。**（如圖 8-27）**
- 在【NPS（本機）】>【原則】>【網路原則】項目上，按下滑鼠右鍵並選擇【新增】。**（如圖 8-28）**
- 在【新增網路原則】視窗中：
  - 輸入指定【原則名稱】。
  - 【網路連線方法】選擇未指定網路存取伺服器類型。
  - 按【下一步】鈕。**（如圖 8-29）**
  - 按下【新增】鈕。**（如圖 8-30）**
  - 在【選取條件】視窗中，選擇【服務類型】並按下【新增】鈕：**（如圖 8-31）**
    - 在【服務類型】視窗中，勾選【Framed】、【Authenticate Only】並按下【確定】鈕，完成設定。**（如圖 8-32）**
  - 按【下一步】鈕。**（如圖 8-33）**
  - 選擇【授與存取權】。
  - 按【下一步】鈕。**（如圖 8-34）**
  - 勾選【Microsoft 加密驗證版本 2（MS-CHAP-v2）】、【Microsoft 加密驗證（MS-CHAP）】、【加密驗證（CHAP）】、【未加密驗證（PAP，SPAP）】。
  - 按【下一步】鈕。**（如圖 8-35）**
  - 按【下一步】鈕。**（如圖 8-36）**
  - 檢視 RADIUS 標準屬性，Framed-Protocol【屬性質】選擇 PPP 用於撥號或 VPN、Service-Type【屬性質】選擇 Framed 用於撥號或 VPN。**（如圖 8-37）**
  - 按【下一步】鈕。**（如圖 8-38）**
  - 按下【完成】鈕，完成設定。**（如圖 8-39, 圖 8-40）**

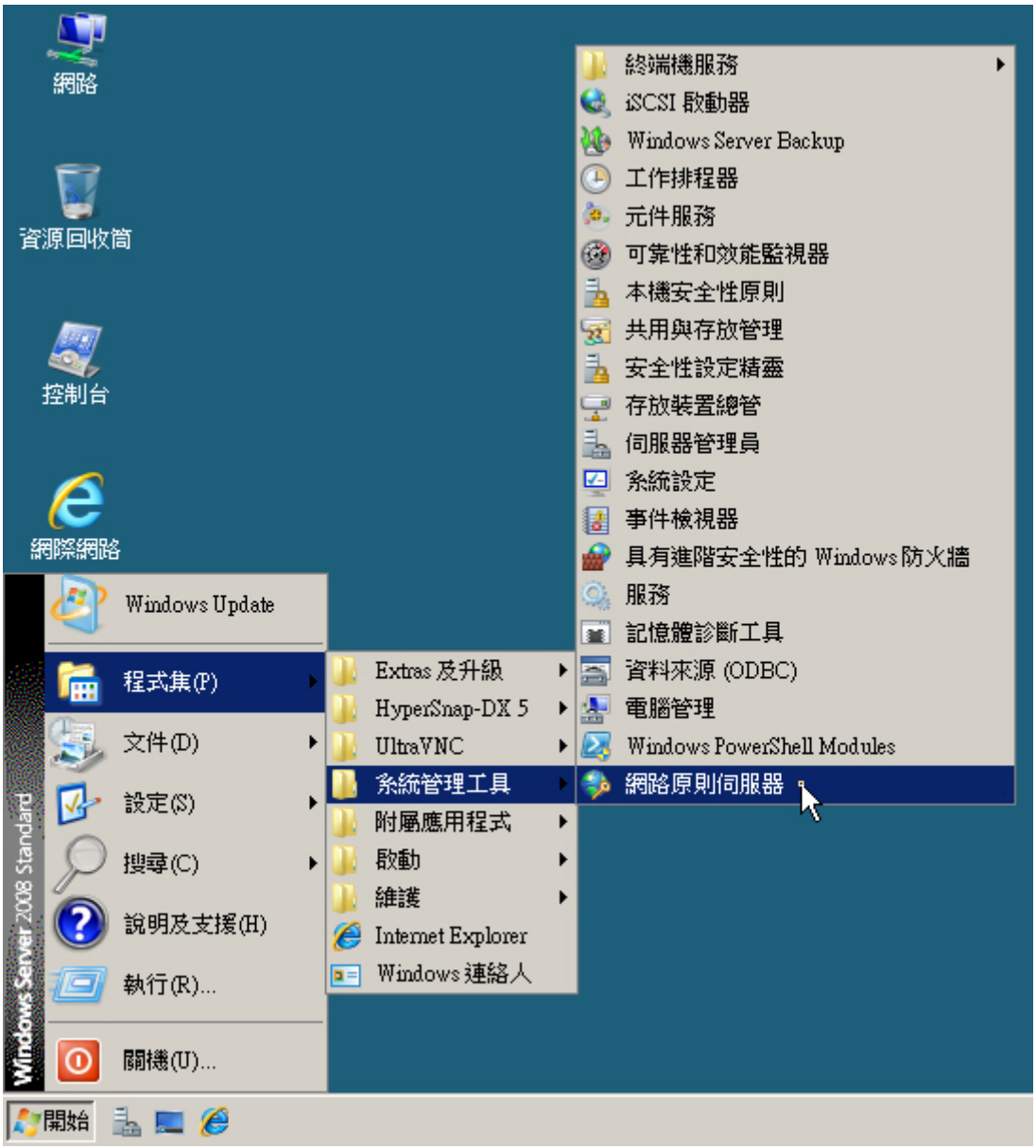


圖 8-24 開啟網路原則伺服器視窗

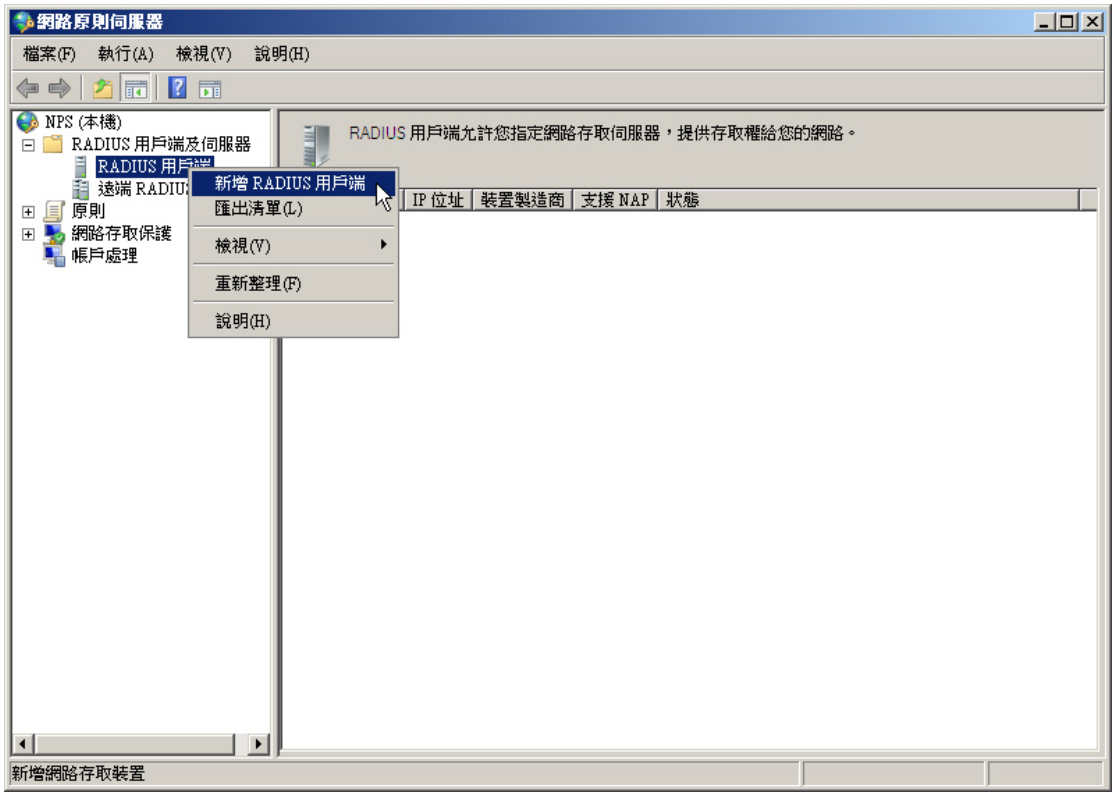


圖 8-25 開啟新增 RADIUS 用戶端視窗

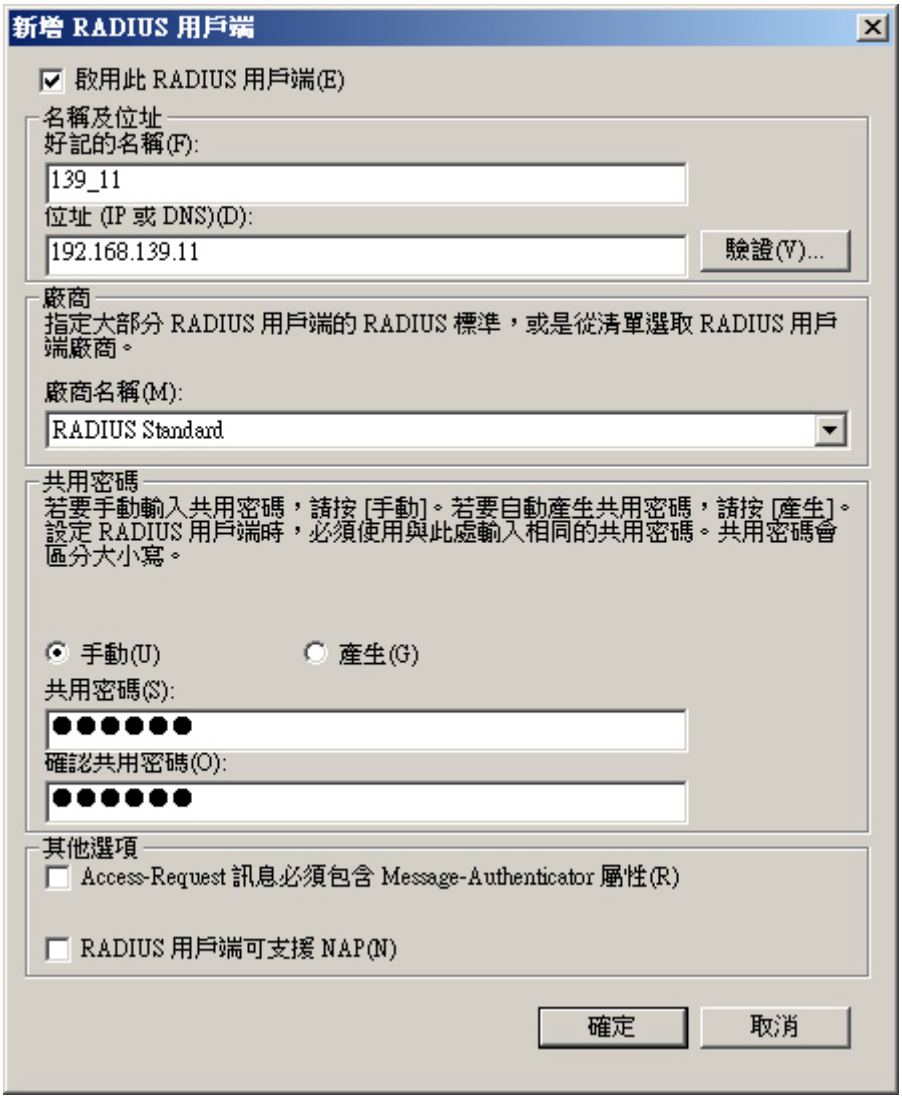


圖 8-26 設定 RADIUS 用戶端

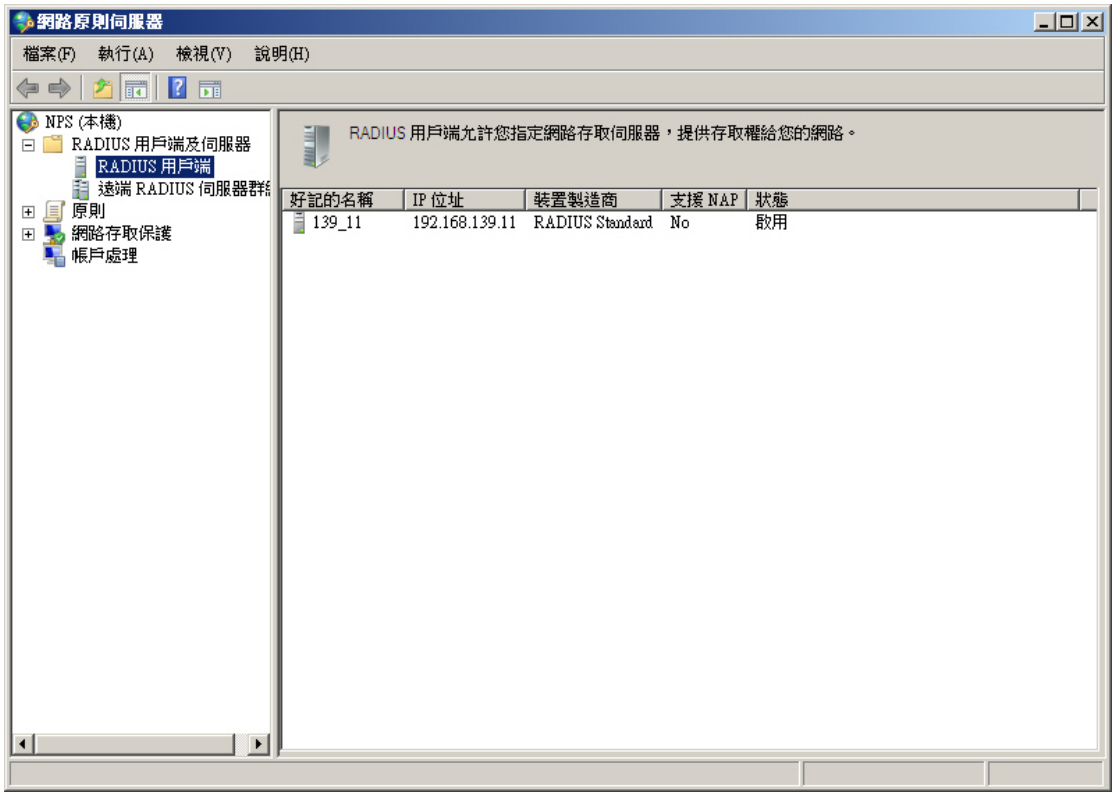


圖 8-27 完成 RADIUS 用戶端設定

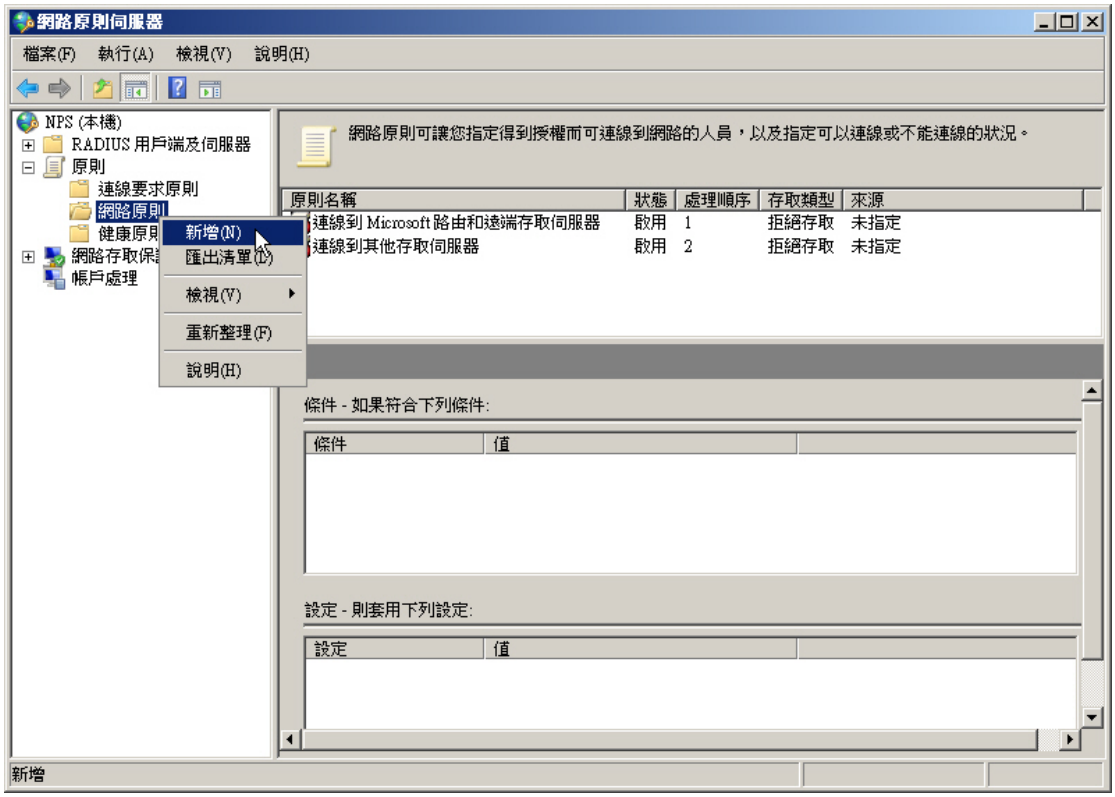


圖 8-28 開啟新增網路原則視窗

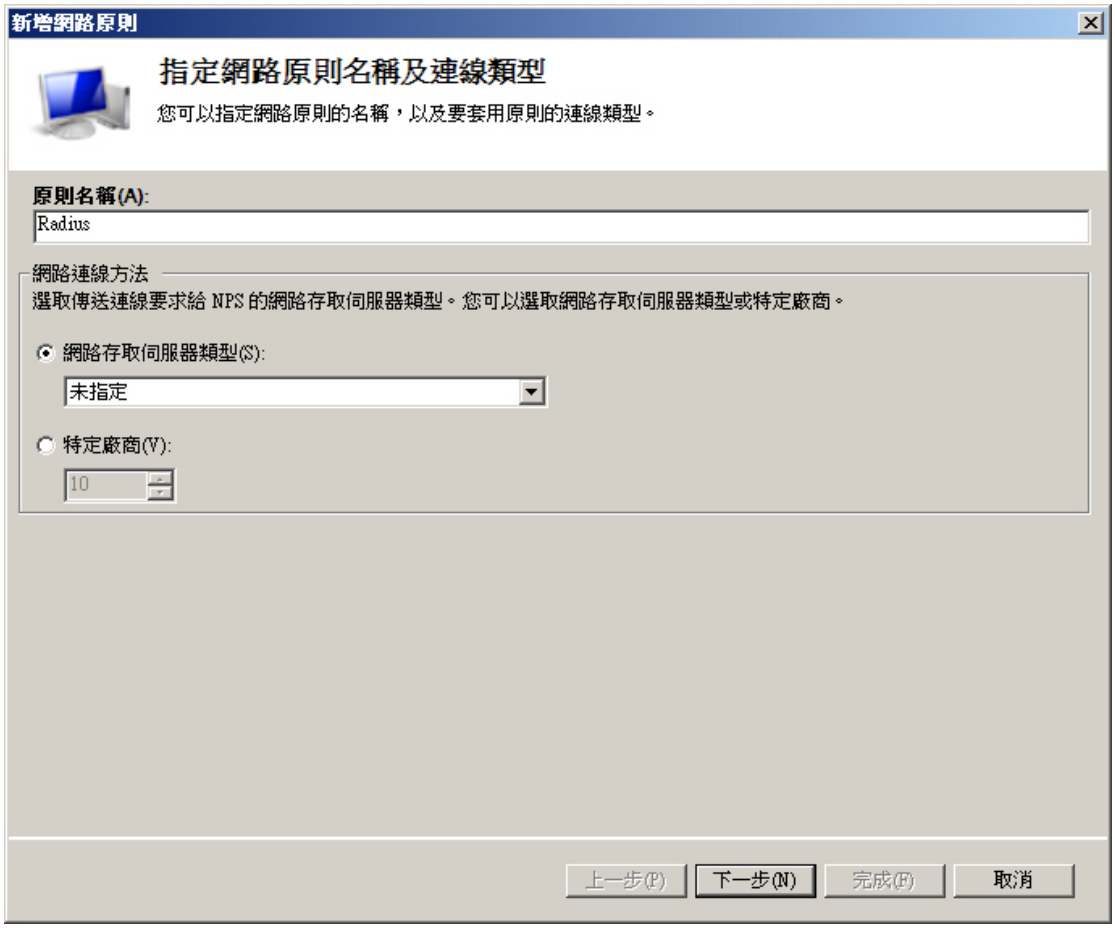


圖 8-29 指定網路原則名稱及連線類型設定

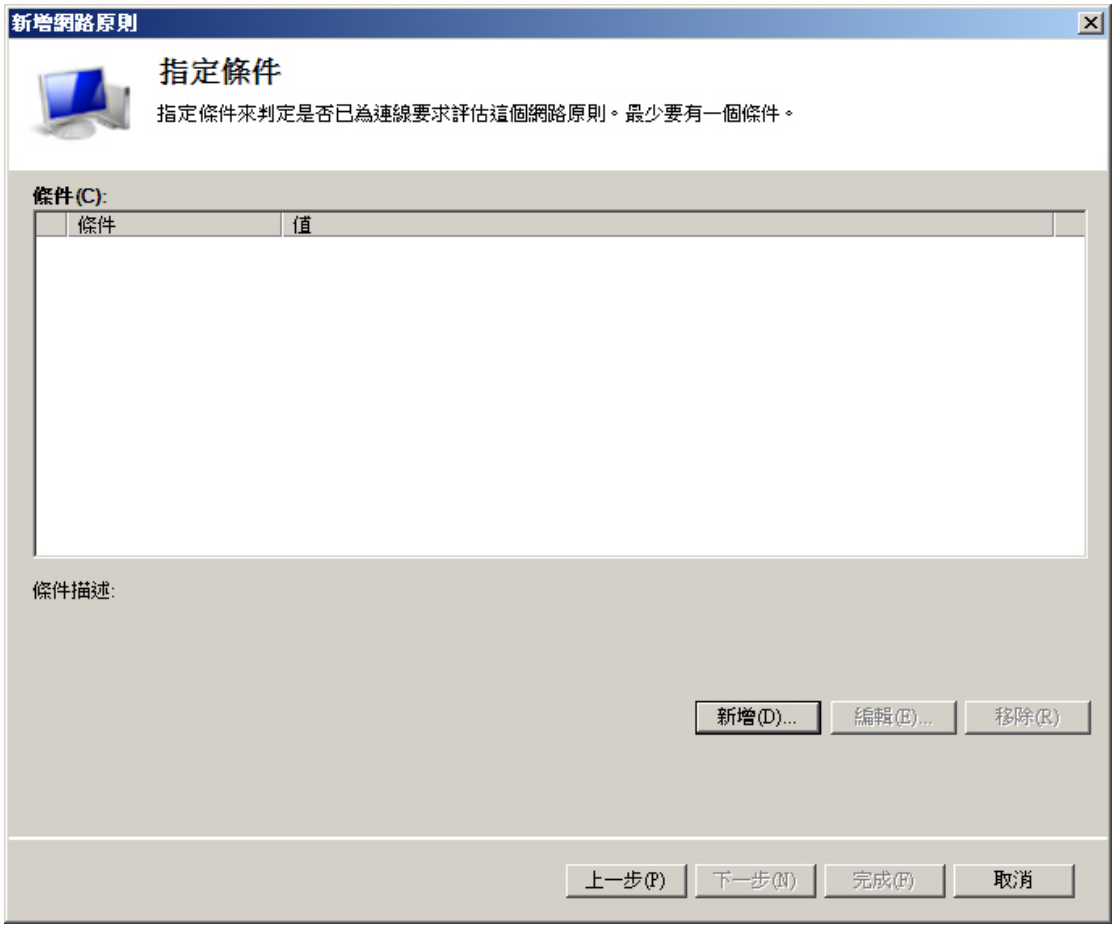


圖 8-30 新增指定條件

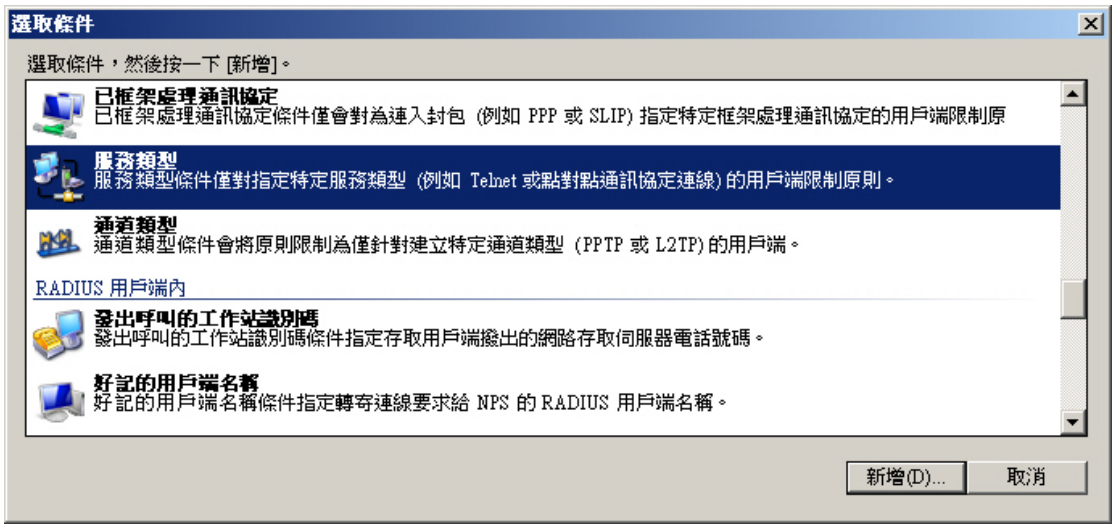


圖 8-31 新增服務類型條件

圖 8-32 服務類型條件設定

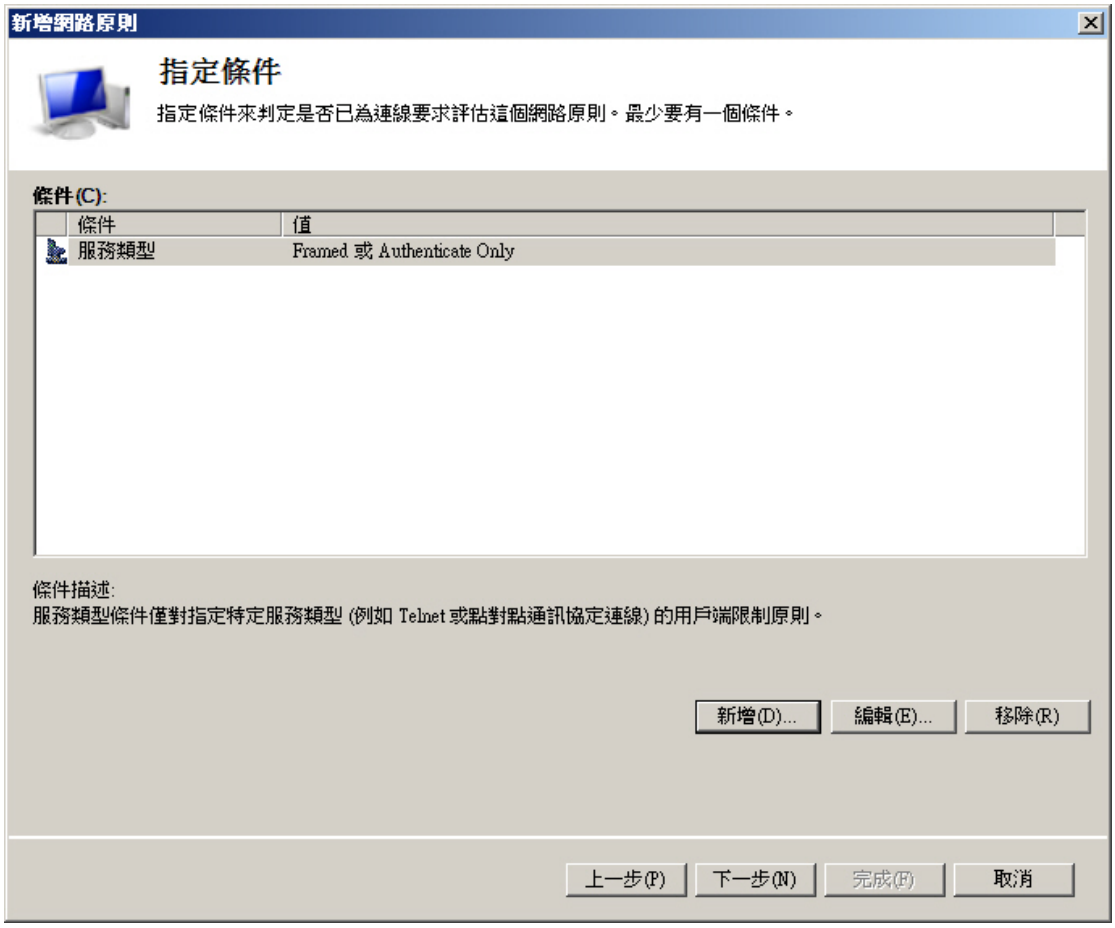


圖 8-33 完成指定條件設定

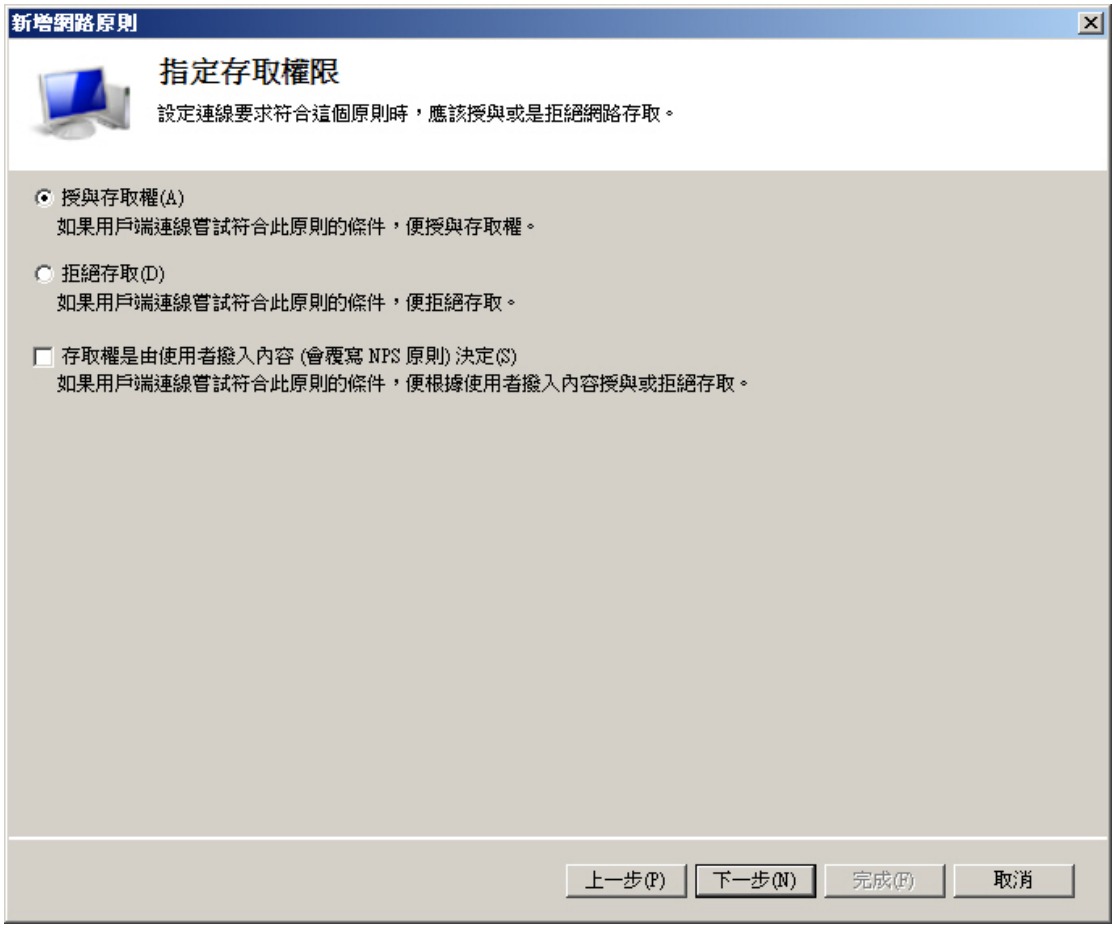


圖 8-34 指定存取權限設定

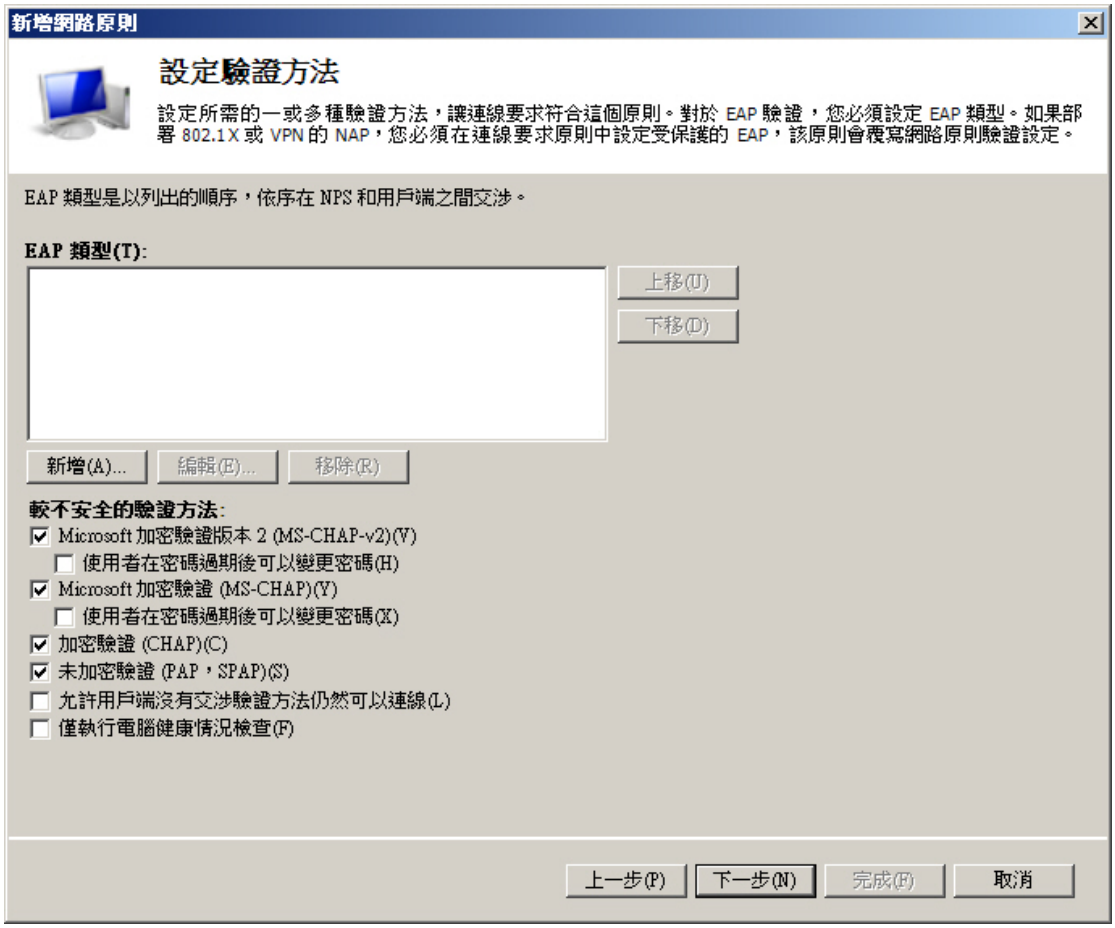

新增網路原則
設定驗證方法
設定所需的一或多種驗證方法，讓連線要求符合這個原則。對於 EAP 驗證，您必須設定 EAP 類型。如果部署 802.1X 或 VPN 的 NAP，您必須在連線要求原則中設定受保護的 EAP，該原則會覆寫網路原則驗證設定。
EAP 類型是以列出的順序，依序在 NPS 和用戶端之間交涉。
EAP 類型(T):
上移(U)
下移(D)
新增(A)...
編輯(E)...
移除(R)
較不安全的驗證方法:
Microsoft 加密驗證版本 2 (MS-CHAP-v2)(V)
使用者在密碼過期後可以變更密碼(H)
Microsoft 加密驗證 (MS-CHAP)(Y)
使用者在密碼過期後可以變更密碼(X)
加密驗證 (CHAP)(C)
未加密驗證 (PAP，SPAP)(S)
允許用戶端沒有交涉驗證方法仍然可以連線(L)
僅執行電腦健康情況檢查(F)
上一步(P)
下一步(N)
完成(F)
取消

圖 8-35 驗證方法設定

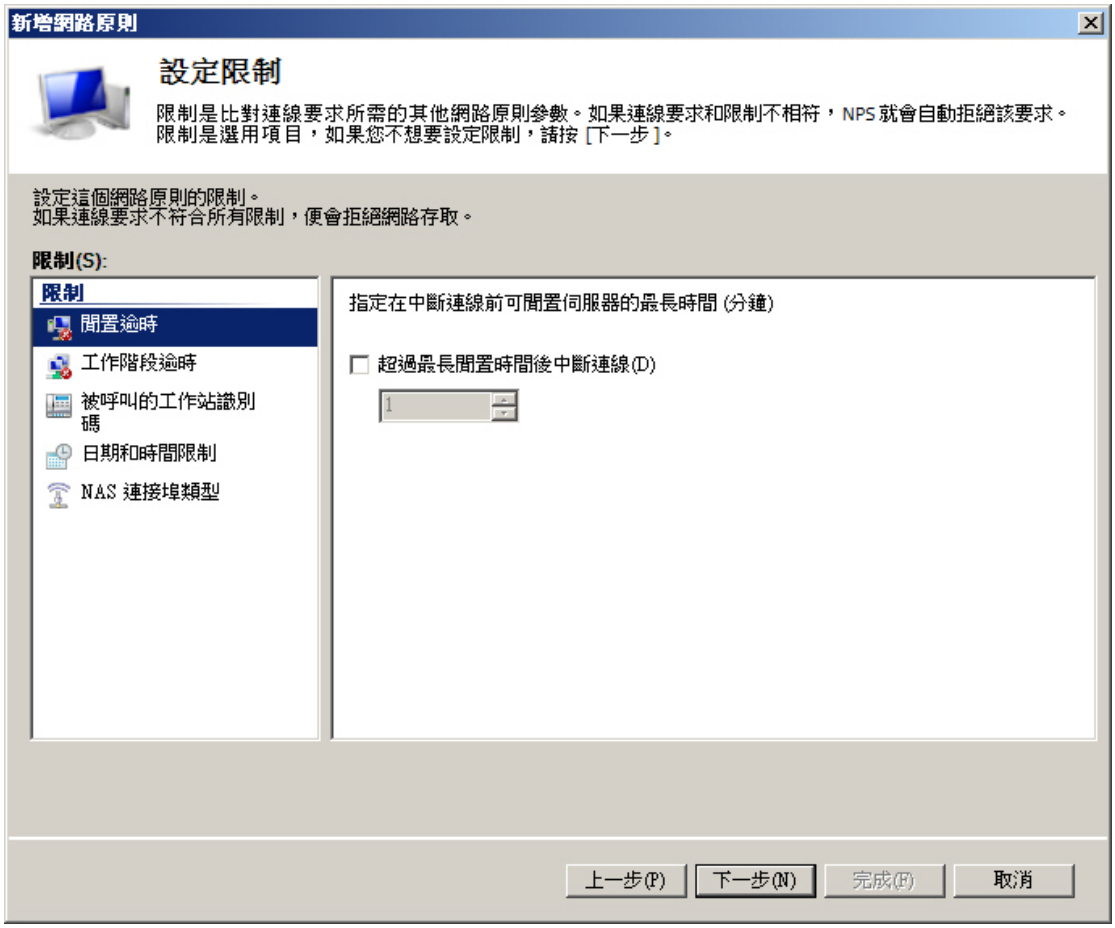


圖 8-36 限制設定

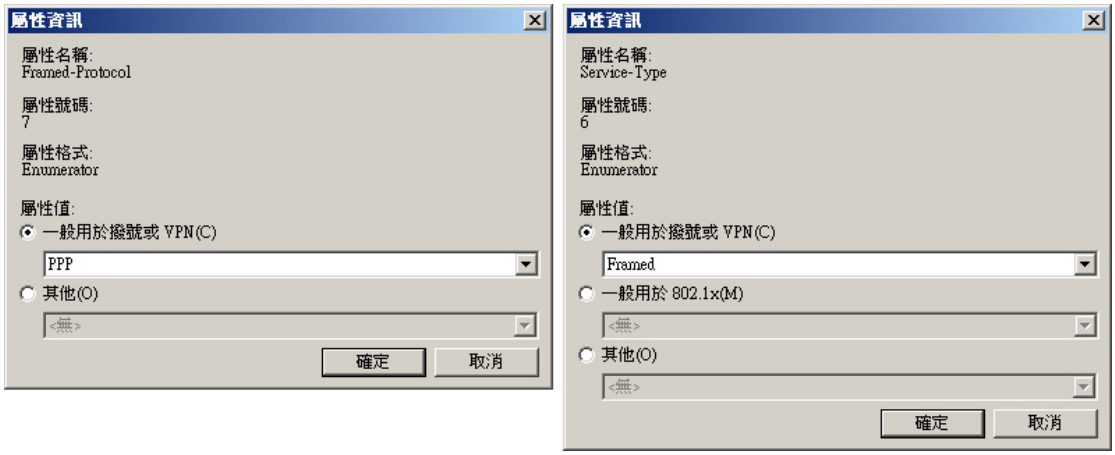


圖 8-37 檢視 RADIUS 標準屬性

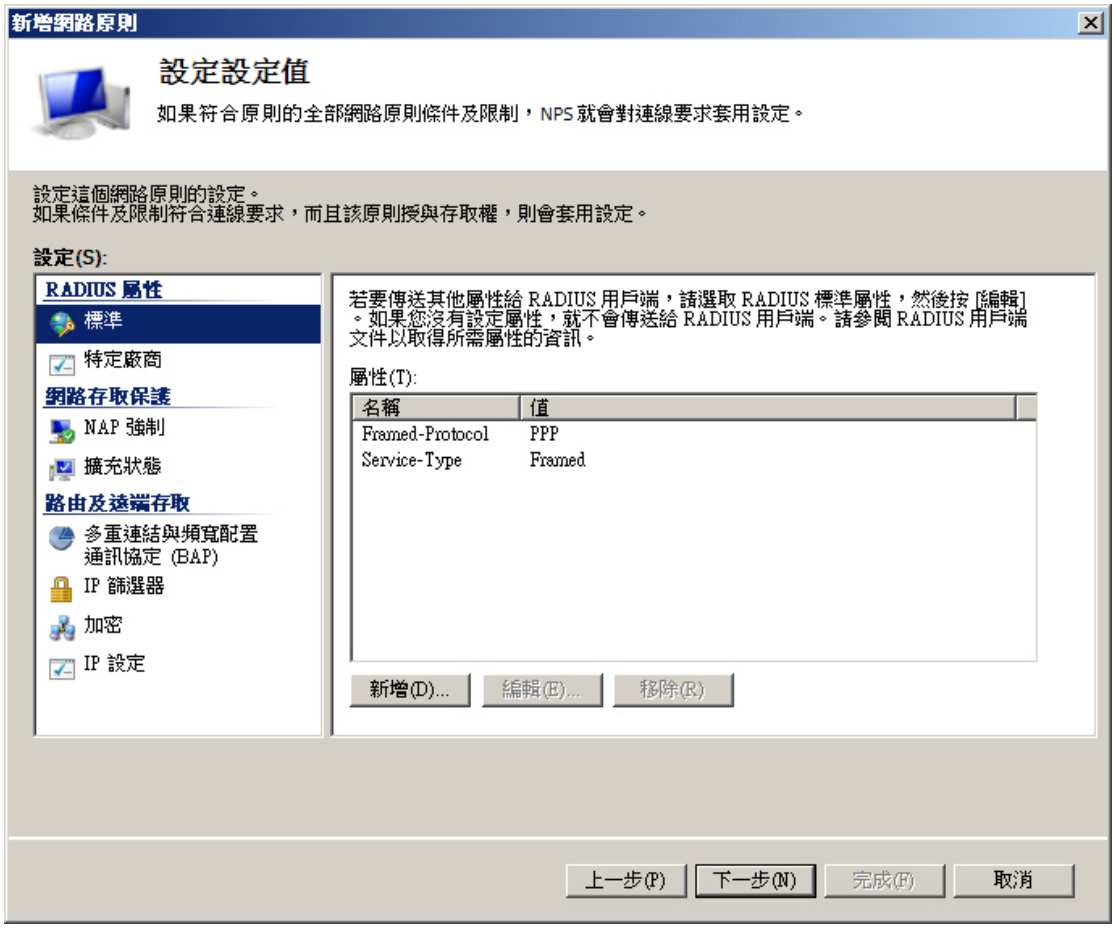


圖 8-38 完成 RADIUS 標準屬性確認

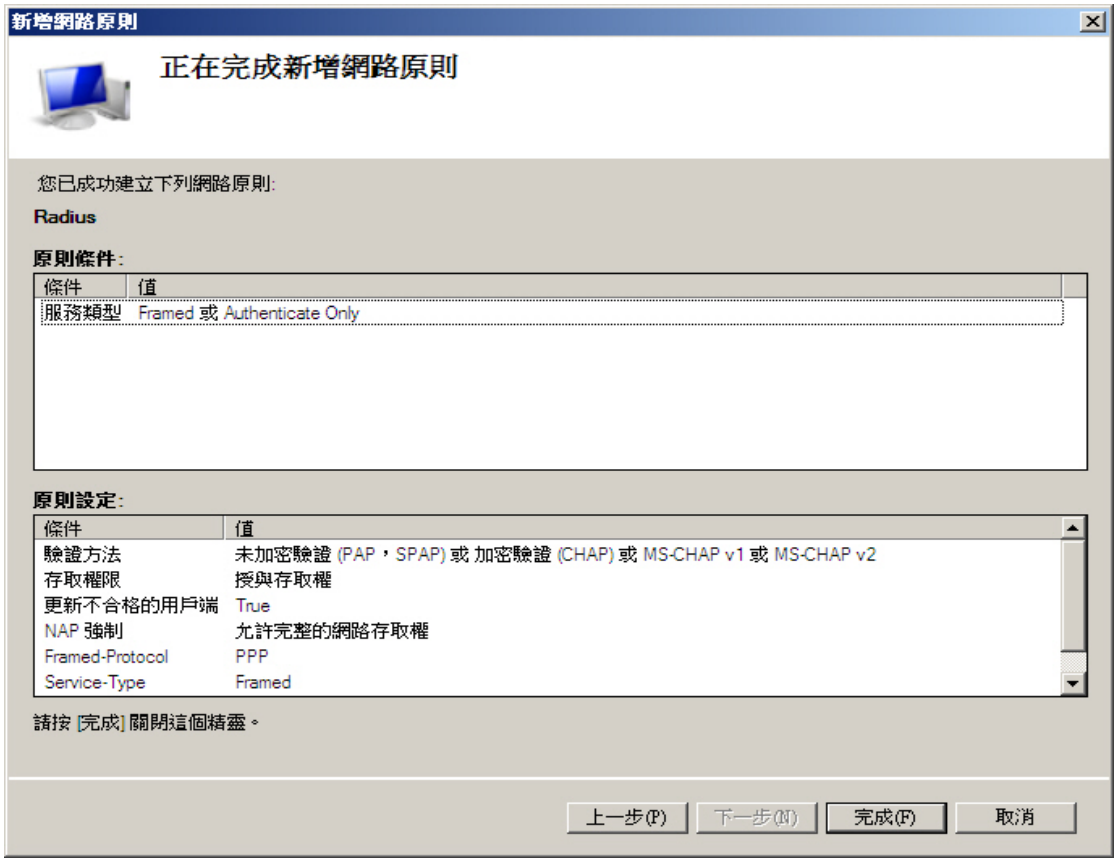


圖 8-39 檢視網路原則設定

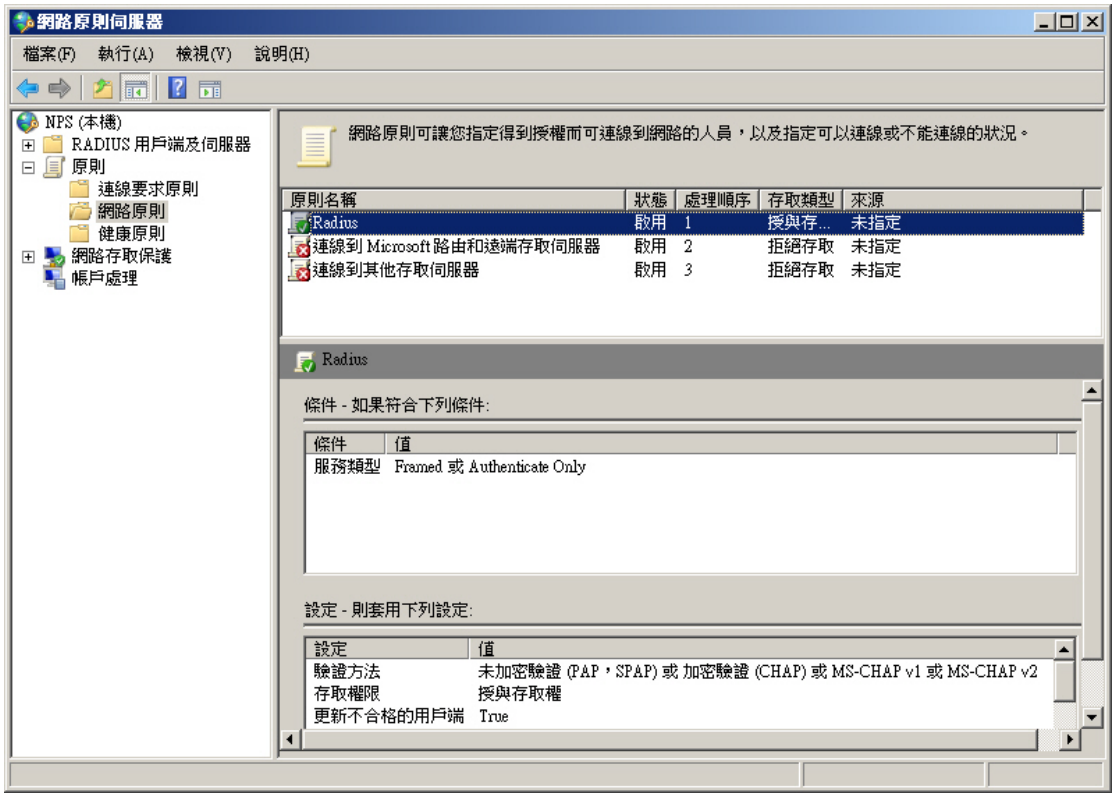


圖 8-40 完成網路原則設定

步驟3. 在【開始】>【程式集】>【系統管理工具】>【電腦管理】視窗中，做下列設定：（如圖 8-41）

- 在【電腦管理（本機）】>【系統工具】>【本機使用者和群組】>【使用者】項目上，按下滑鼠右鍵並選擇【新使用者】。（如圖 8-42）
- 在【新使用者】視窗中：（如圖 8-43）
  - 輸入指定【使用者名稱】、【密碼】、【確認密碼】。
  - 勾選【密碼永久有效】。
  - 按下【建立】鈕，再按下【關閉】鈕，完成設定。（如圖 8-44）

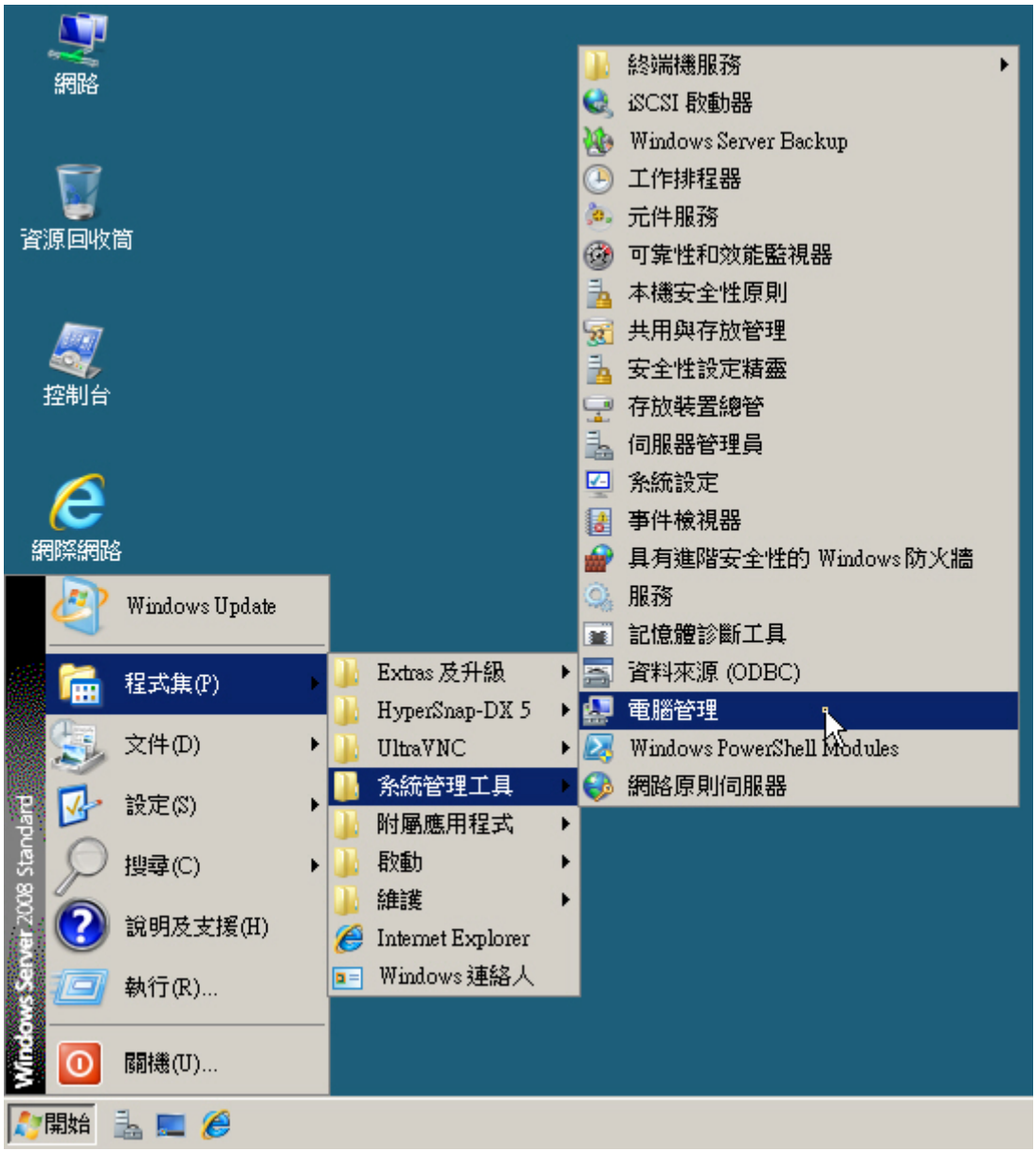


圖 8-41 開啟電腦管理視窗

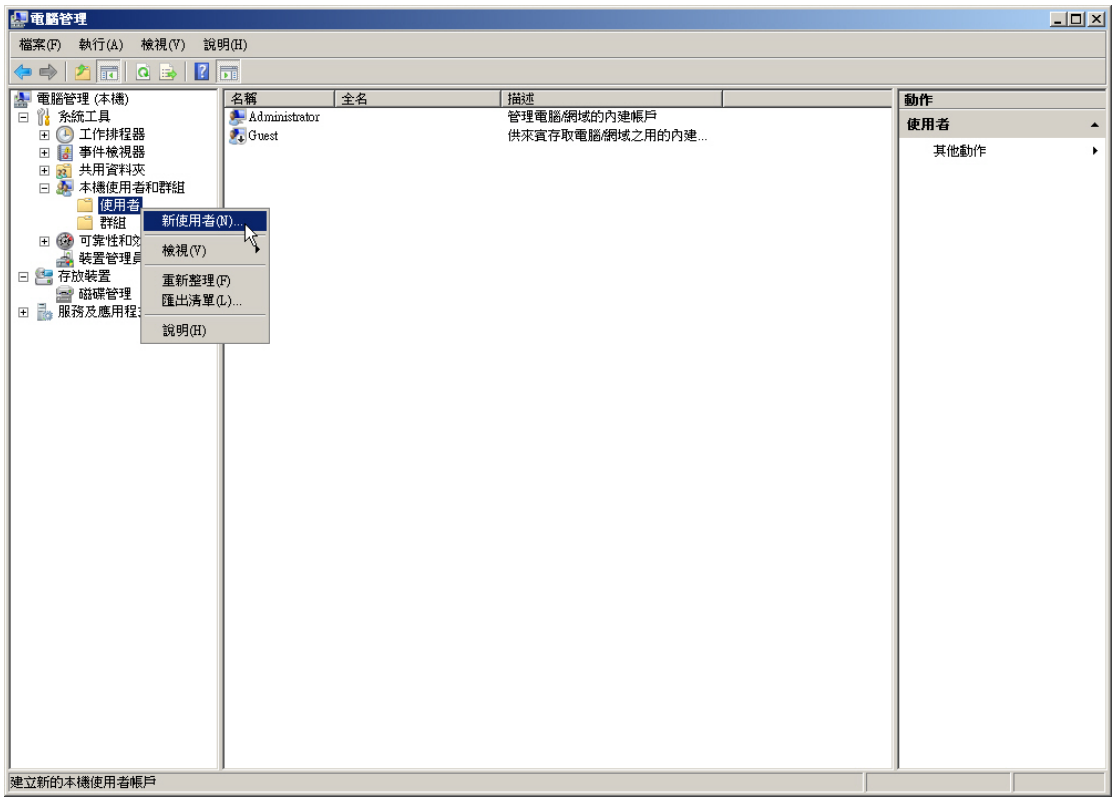


圖 8-42 開啟新使用者視窗

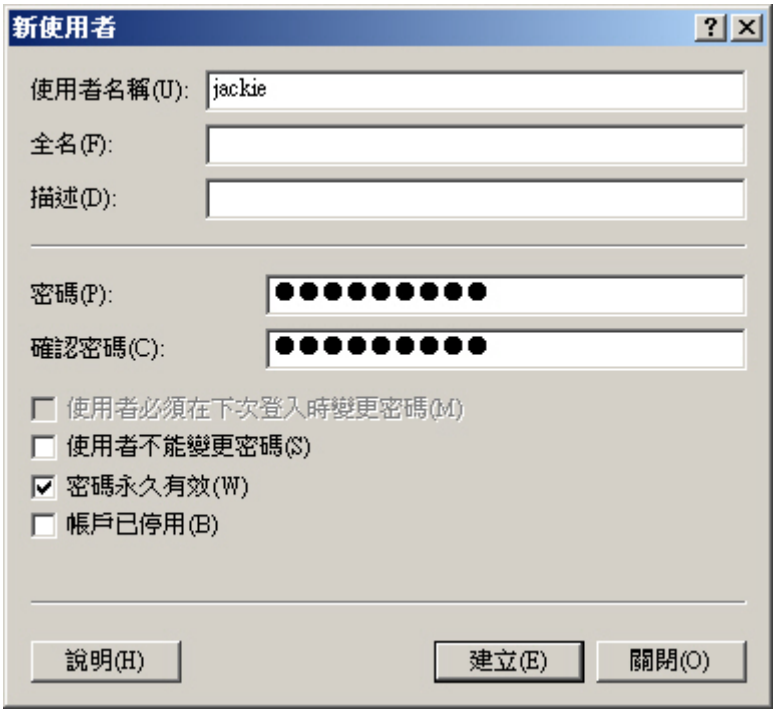


圖 8-43 設定新使用者

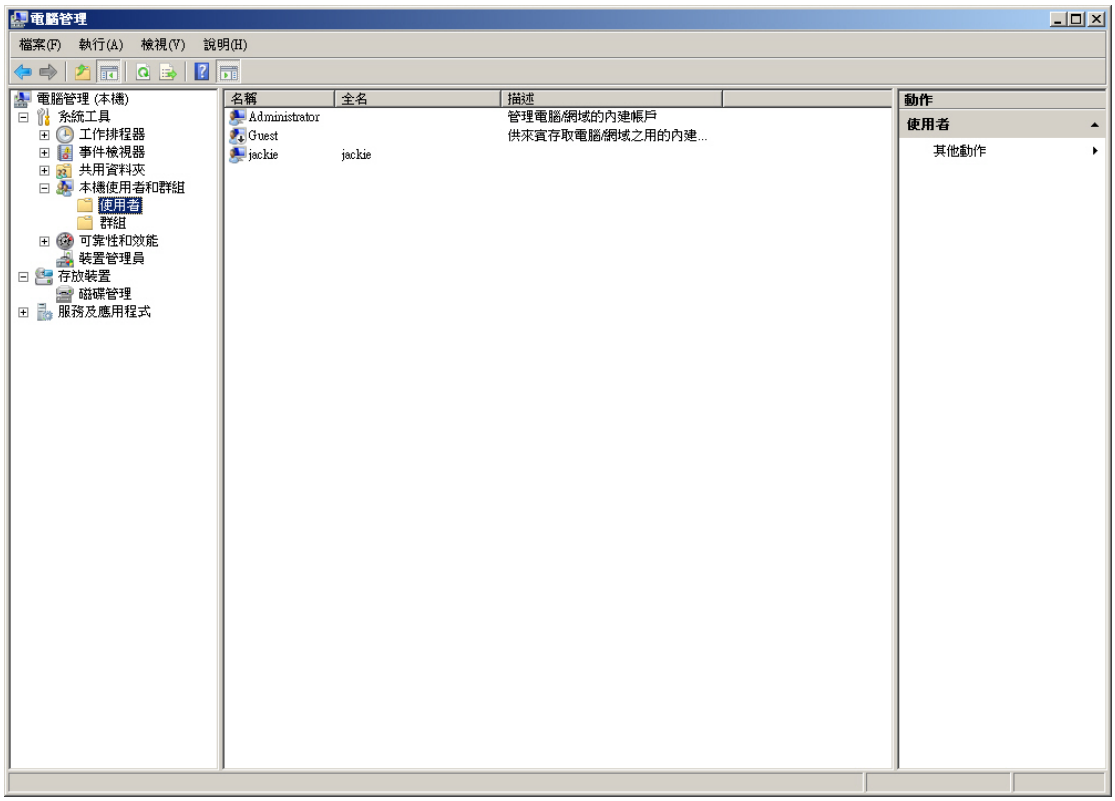


圖 8-44 完成新使用者設定

步驟4. 在【管制條例選項】>【認證表】>【外部 RADIUS】頁面中，輸入 RADIUS 伺服器之連線 IP、Port 和共同密鑰。（如圖 8-45）

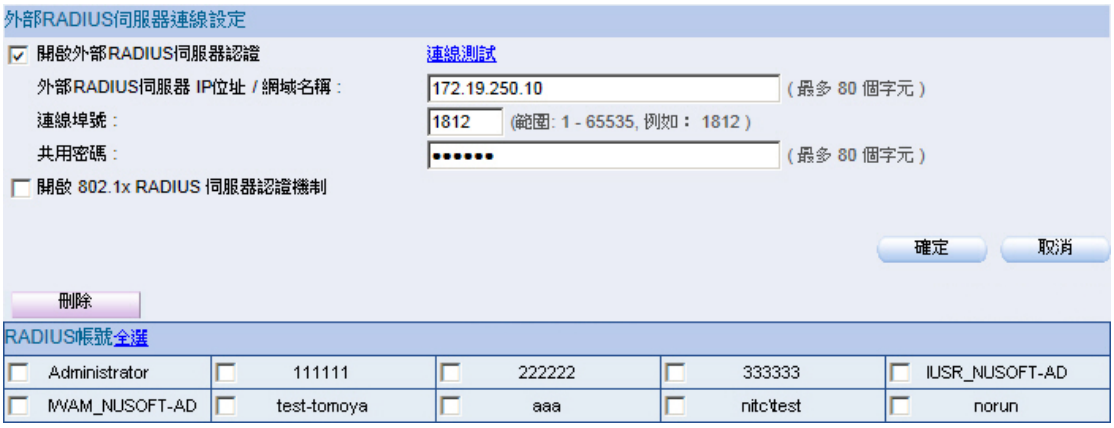


圖 8-45 RADIUS 伺服器連線設定頁面

說明：

1. 按下【測試連線】，可以偵測出目前 MHG-2000 和 RADIUS 伺服器是否可正常連線。
2. 【RADIUS 帳號】為 MHG-2000 連線 RADIUS 伺服器所取得的帳戶清單，可將各帳戶依需求進行群組來提供授權認證。

步驟5. 在【管制條例選項】>【認證表】>【認證群組】頁面中，做下列設定：（如圖 8-46）

圖 8-46 認證群組設定頁面

步驟6. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 8-47）

- 【認證名稱】選擇所設定的認證群組規則。
- 按下【確定】鈕，完成設定。（如圖 8-48）

圖 8-47 管制條例套用認證規則

圖 8-48 完成管制條例設定

步驟7. 當內部使用者欲透過設定的認證管制條例瀏覽網頁時，即會先行連線認證頁面。在輸入正確的認證【帳戶名稱】和【密碼】後，按下【登入】鈕即可透過 MHG-2000 上網。（如圖 8-49）

圖 8-49 認證登入頁面

8.3 POP3 認證功能使用範例

8.3.1 規劃使用者必須通過管制條例之認證機制，方可連線至外部網路。(採用 POP3 Server 認證)

步驟1. 在【管制條例選項】>【認證表】>【外部 POP3】頁面中，做下列設定：（如圖 8-50）

圖 8-50POP3 伺服器連線設定頁面

說明：

1. 按下【連線測試】，可以偵測出目前 MHG-2000 和 POP3 伺服器是否可正常連線。
2. 【開啟網域名稱過濾】機制，可指定與 POP3 伺服器連線驗證的郵件網域。
3. MHG-2000 可【使用 SSL 網路安全機制】，以 POP3S 協定連線 POP3 伺服器進行授權認證作業。

步驟2. 在【管制條例選項】>【認證表】>【認證群組】頁面中，做下列設定：（如圖 8-51）

圖 8-51 認證群組設定頁面

步驟3. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 8-52）

- 【認證名稱】選擇所設定的認證群組規則。
- 按下【確定】鈕，完成設定。（如圖 8-53）

圖 8-52 管制條例套用認證規則

圖 8-53 完成管制條例設定

步驟4. 當內部使用者欲透過設定的認證管制條例瀏覽網頁時，即會先行連線認證頁面。在輸入正確的認證【帳戶名稱】和【密碼】後，按下【登入】鈕即可透過 MHG-2000 上網。（如圖 8-54）

圖 8-54 認證登入頁面

8.4 LDAP 認證功能使用範例

8.4.1 規劃使用者必須通過管制條例之認證機制，方可連線至外部網路。【採用外部 LDAP Server（Windows 2008 Server 內建）認證】

※ Windows 2008 LDAP Server 設置方法

步驟1. 在【開始】>【程式集】>【系統管理工具】>【伺服器管理員】視窗中，做下列設定：**（如圖 8-55）**

- 在【伺服器管理員】>【角色】項目上，按下滑鼠右鍵並選擇【新增角色】。**（如圖 8-56）**
- 在【新增角色精靈】視窗中：
  - 【角色】勾選 Active Directory 網域服務。
  - 按【下一步】鈕。**（如圖 8-57）**
  - 按【下一步】鈕。**（如圖 8-58）**
  - 按下【安裝】鈕。**（如圖 8-59）**
  - 點選【關閉此精靈，然後啟動 Active Directory 網域服務安裝精靈（dcpromo.exe）】連結。**（如圖 8-60）**
- 在【Active Directory 網域服務安裝精靈】視窗中：
  - 按【下一步】鈕。**（如圖 8-61）**
  - 按【下一步】鈕。**（如圖 8-62）**
  - 選擇【在新樹系內建立新網域】。
  - 按【下一步】鈕。**（如圖 8-63）**
  - 【樹系根網域的 FQDN】輸入 my.com。
  - 按【下一步】鈕。**（如圖 8-64）**
  - 【樹系功能等級】選擇 Windows Server 2008。
  - 按【下一步】鈕。**（如圖 8-65）**
  - 勾選【DNS 伺服器】。
  - 按【下一步】鈕。**（如圖 8-66）**
  - 按【下一步】鈕。**（如圖 8-67）**

- 輸入指定【密碼】、【確認密碼】。
- 按【下一步】鈕。（如圖 8-68）
- 按【下一步】鈕。（如圖 8-69）
- 按下【完成】鈕，完成安裝。（如圖 8-70）

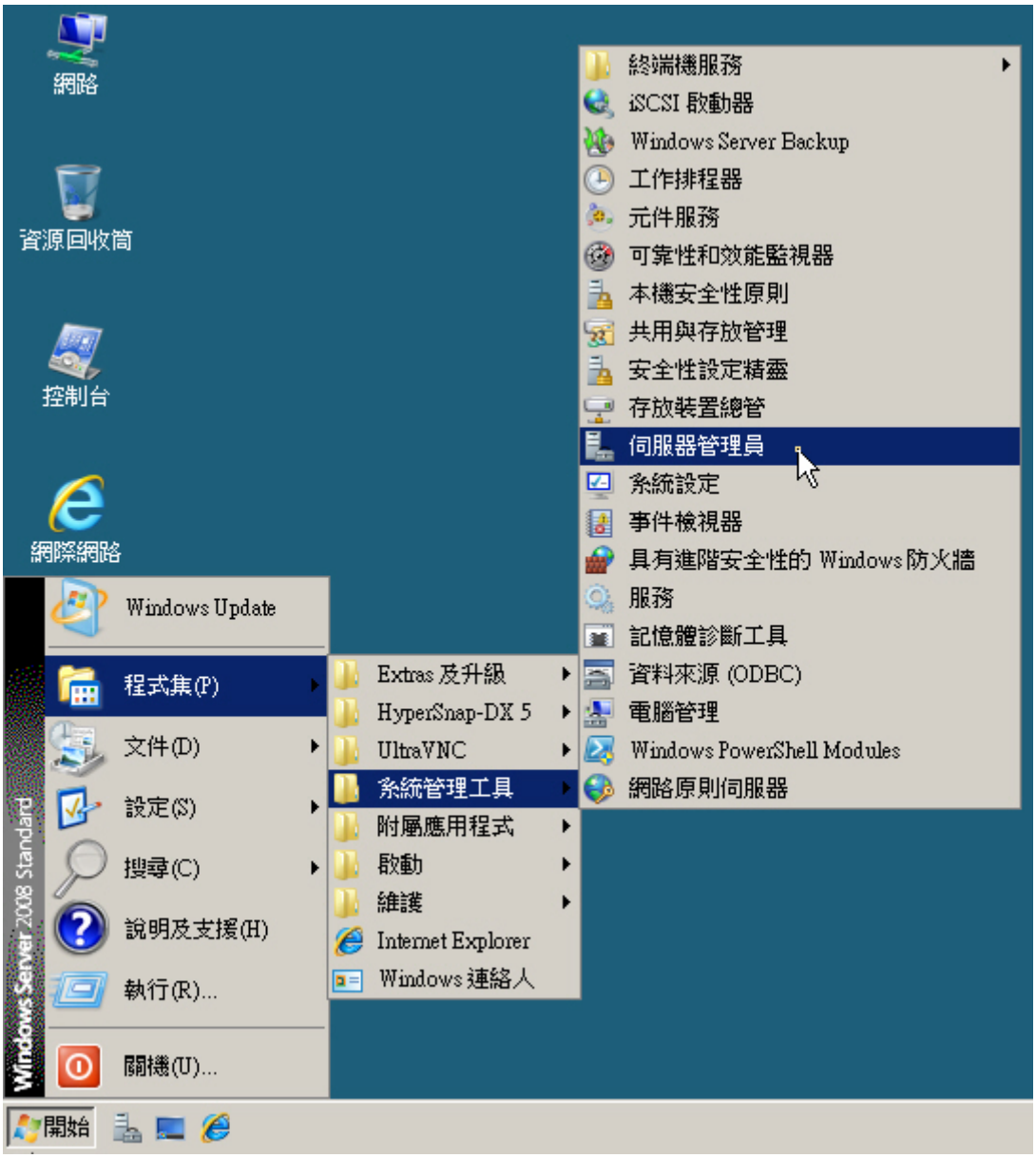


圖 8-55 開啟伺服器管理員視窗

圖 8-56 開啟新增角色精靈視窗

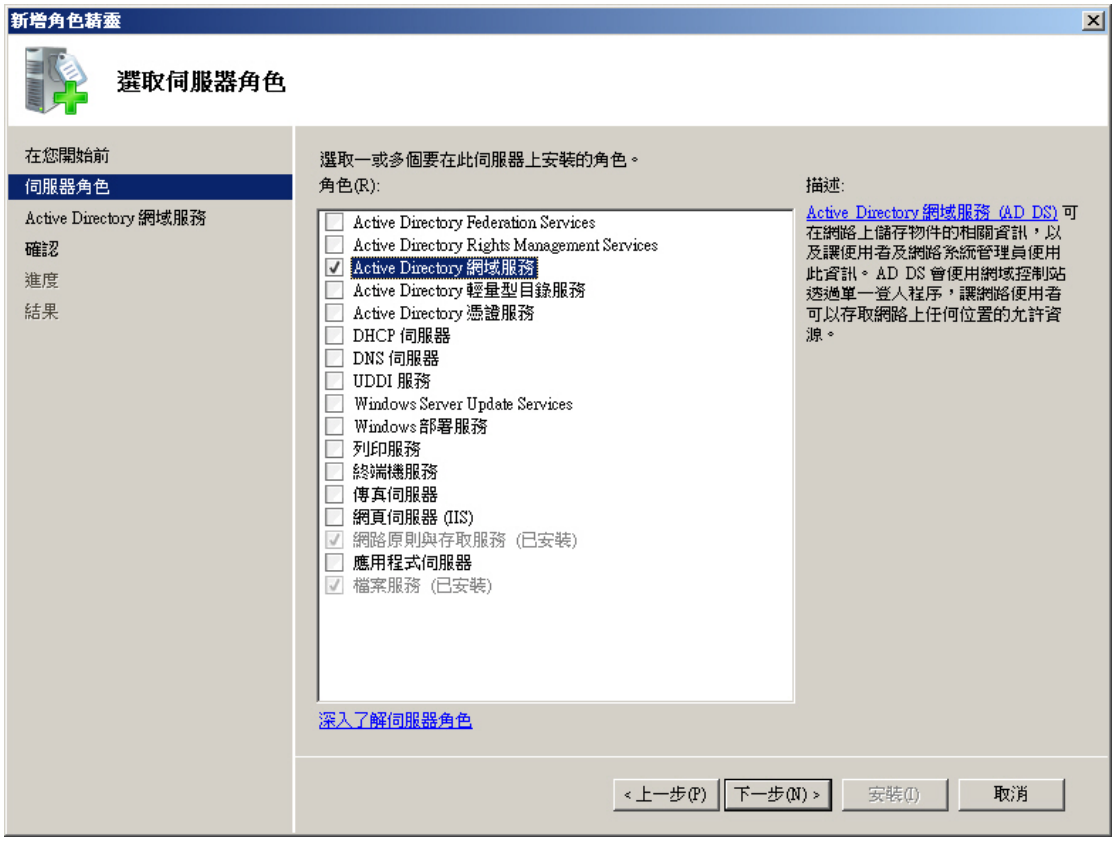


圖 8-57 選擇欲安裝的伺服器角色

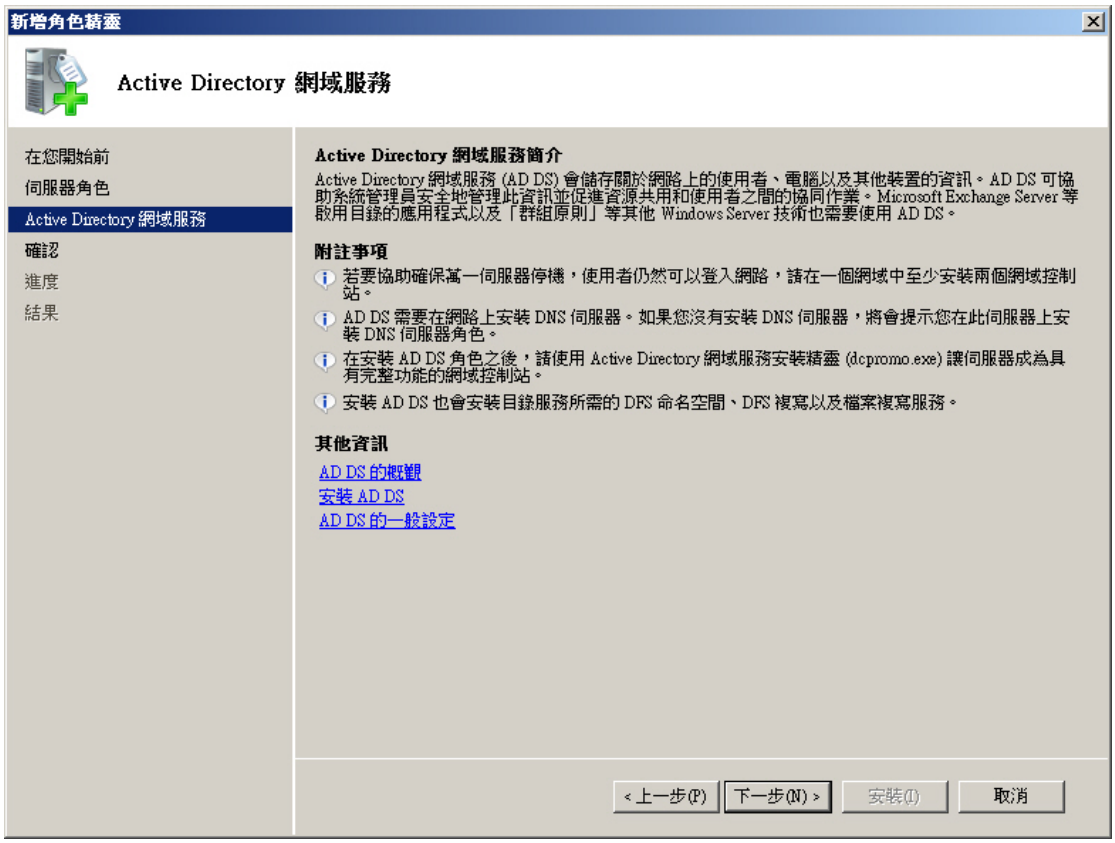


圖 8-58Active Directory 網域服務簡介

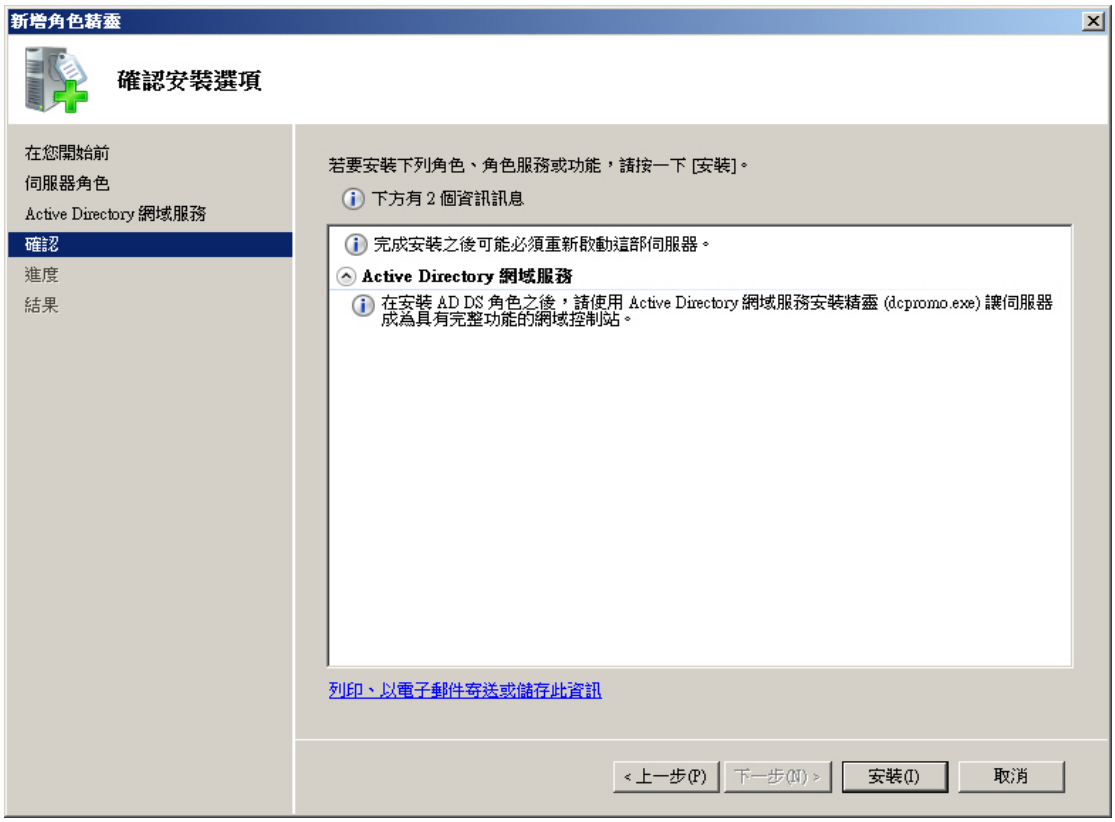


圖 8-59 安裝 Active Directory 網域服務

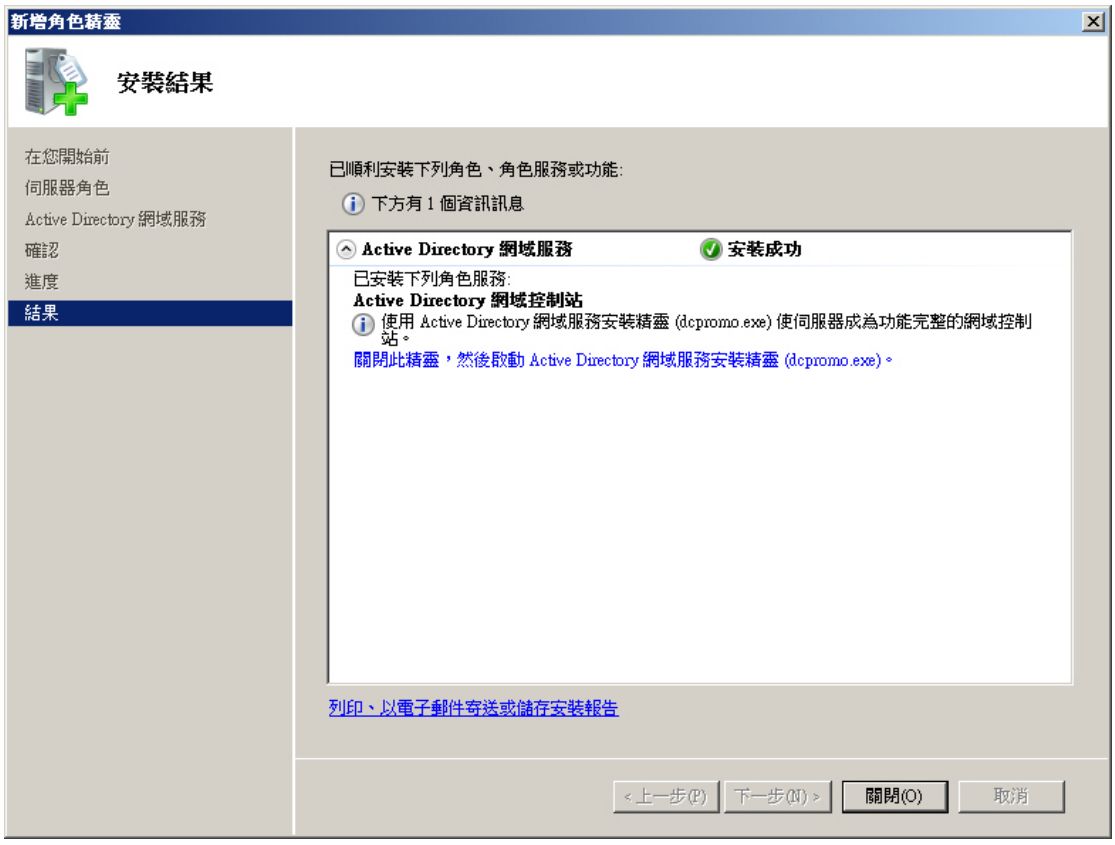


圖 8-60 開啟 Active Directory 網域服務安裝精靈視窗

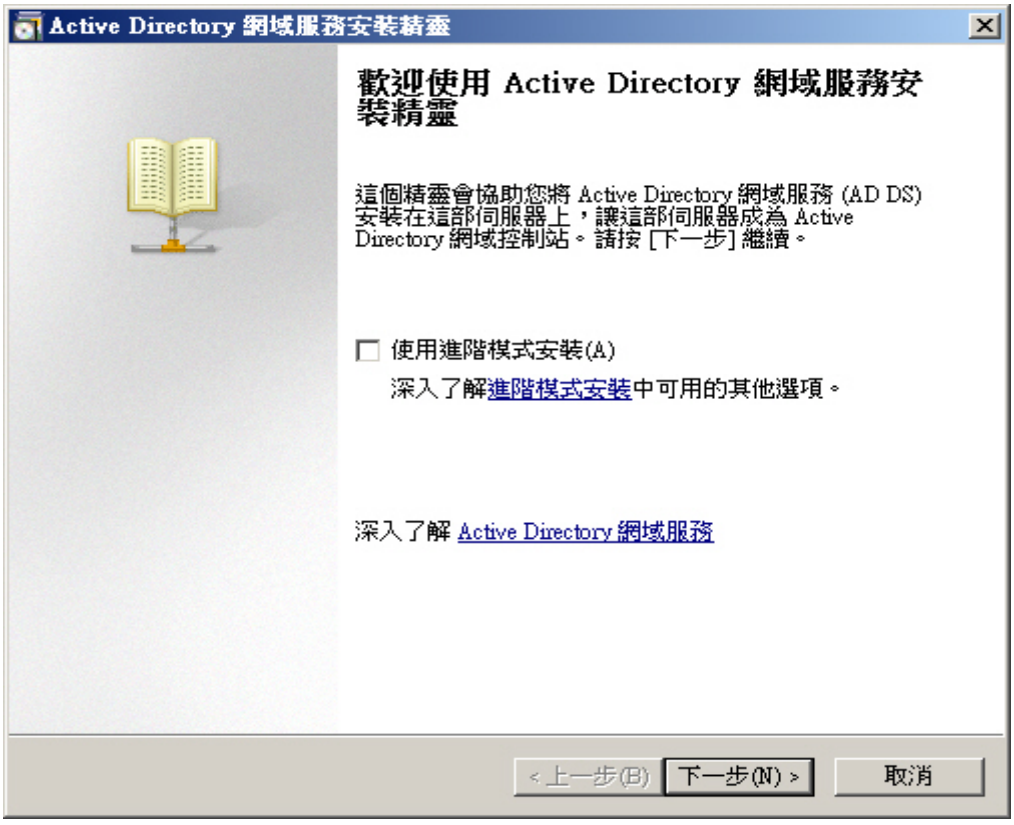


圖 8-61Active Directory 網域服務安裝精靈歡迎訊息

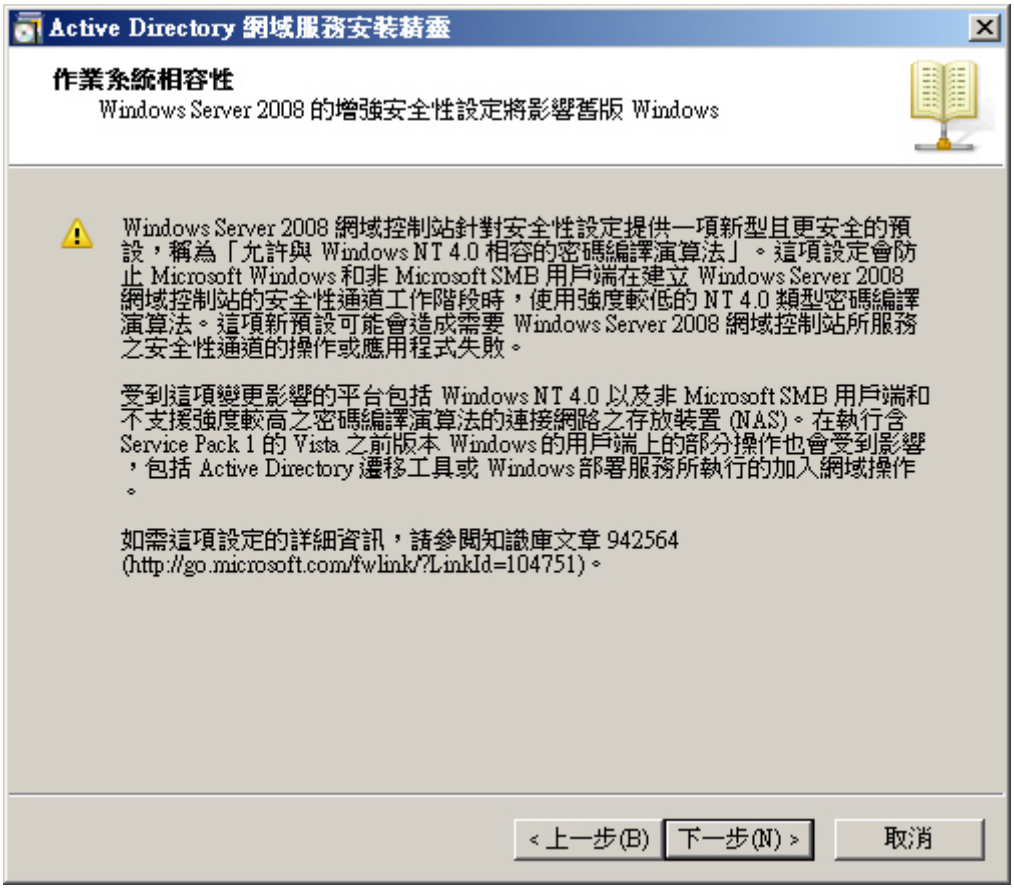


圖 8-62 作業系統相容性資訊

Active Directory 網域服務安裝精靈
選擇部署設定
您可以建立現有樹系或新樹系的網域控制站。
現有樹系(E)
新增現有網域的網域控制站(A)
在現有樹系內建立新網域(C)
這部伺服器會成為新網域的第一部網域控制站。
在新樹系內建立新網域(D)
深入了解可行的部署設定
< 上一步(B)
下一步(N) >
取消

圖 8-63 部署設定

圖 8-64 樹系根網域名稱設定

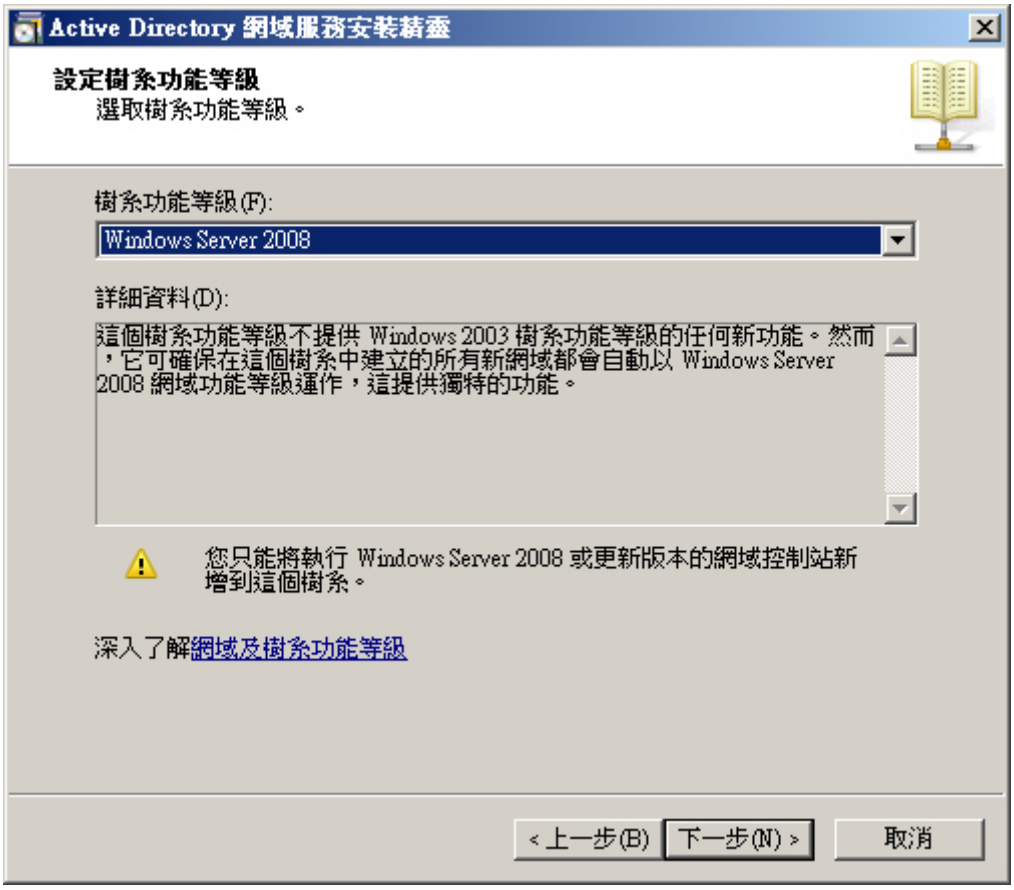


圖 8-65 樹系功能等級設定

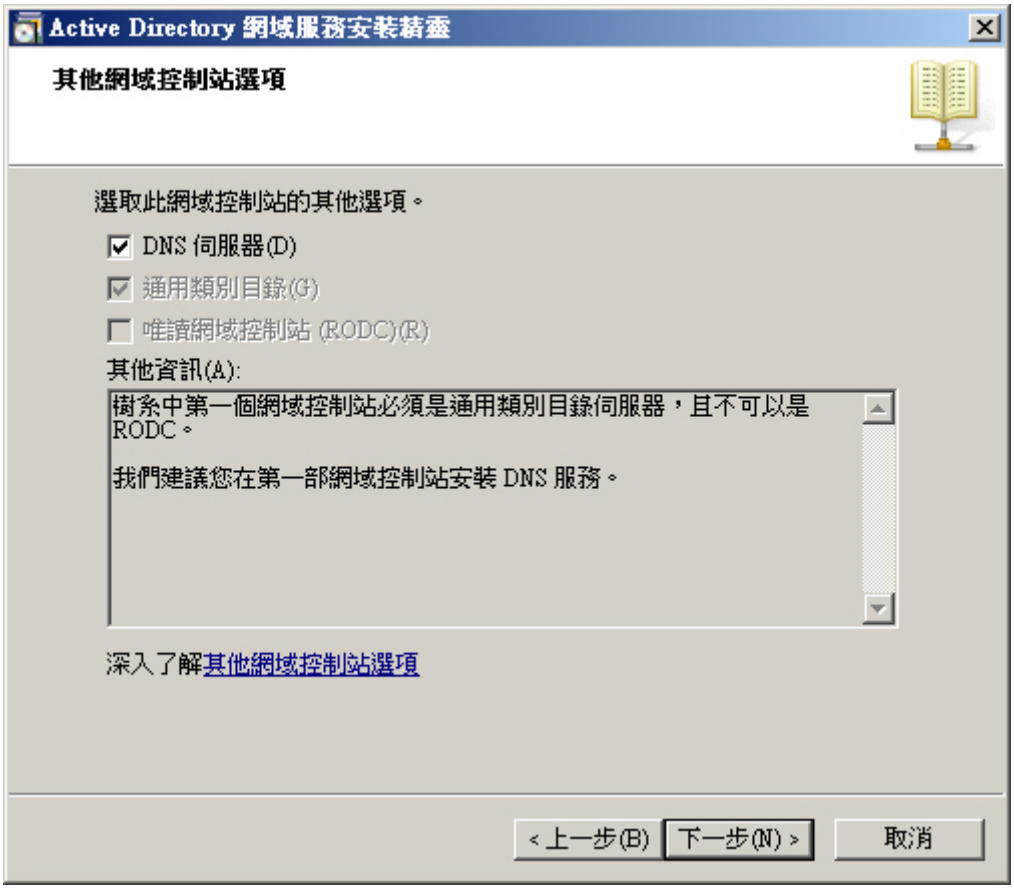


圖 8-66 選擇欲安裝的其他網域控制站選項

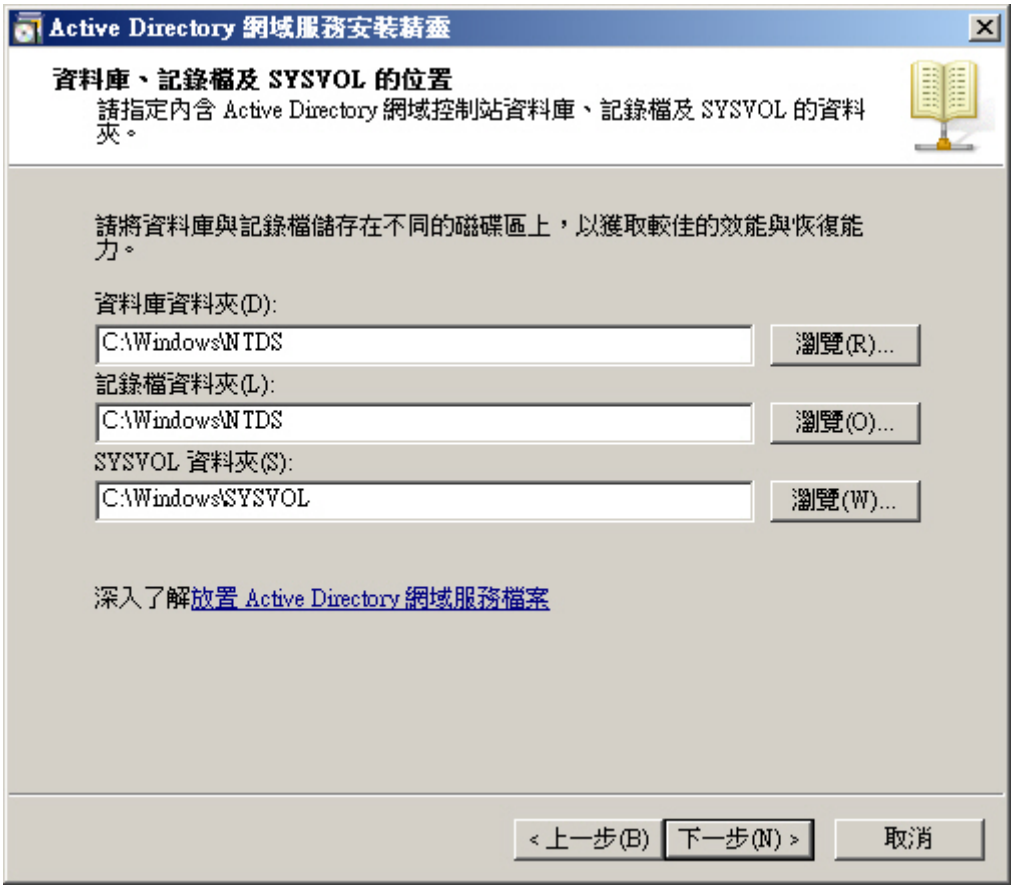


圖 8-67 資料庫、記錄檔及 SYSVOL 的位置設定

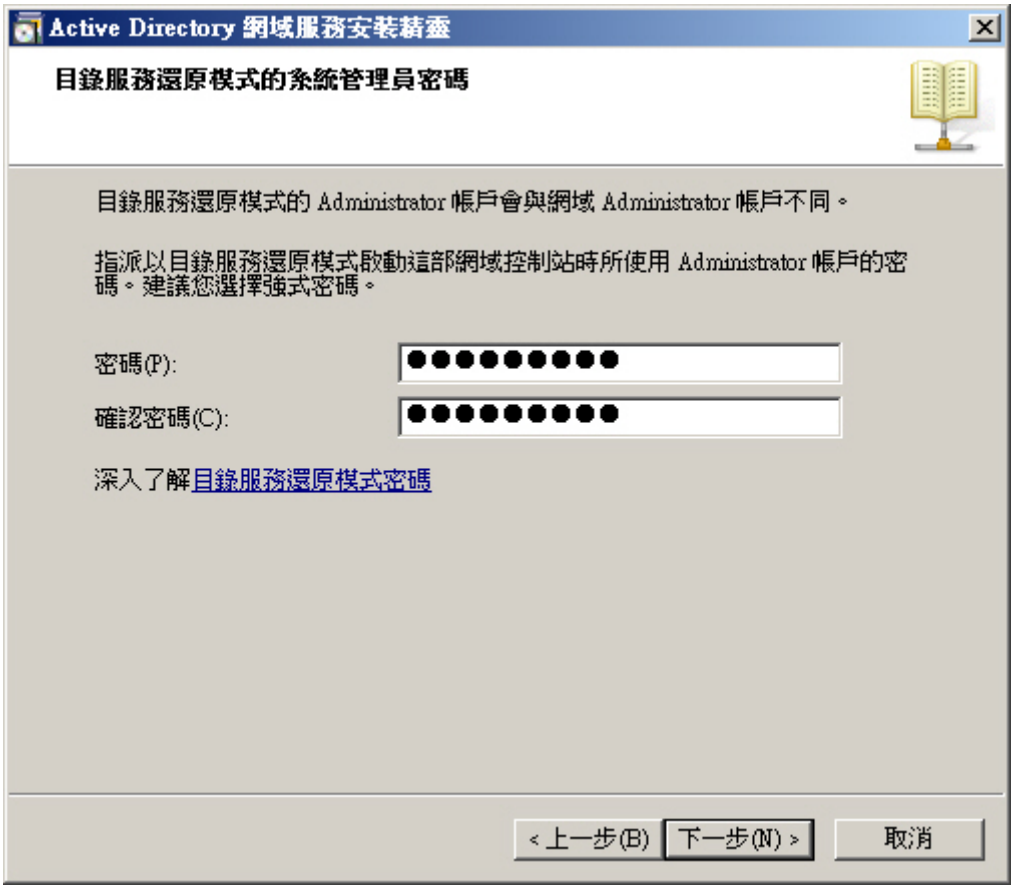


圖 8-68 目錄服務還原模式的系統管理員密碼設定

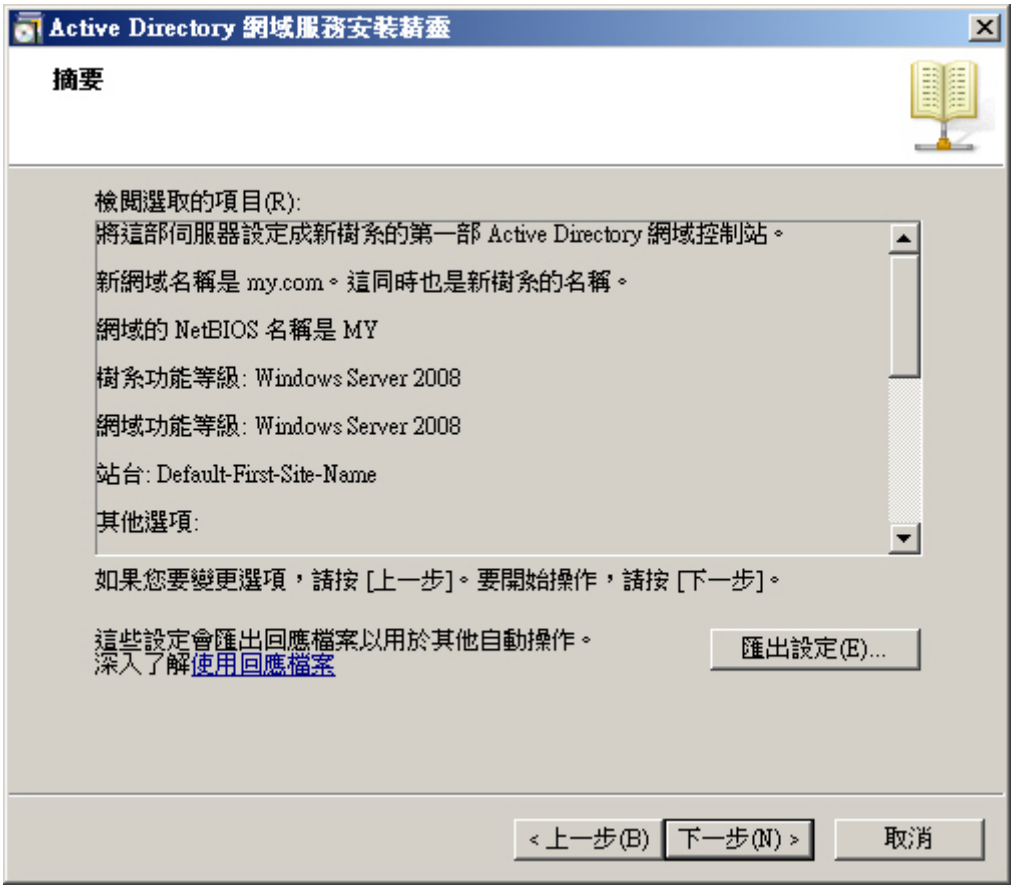


圖 8-69 檢視 Active Directory 網域服務安裝設定

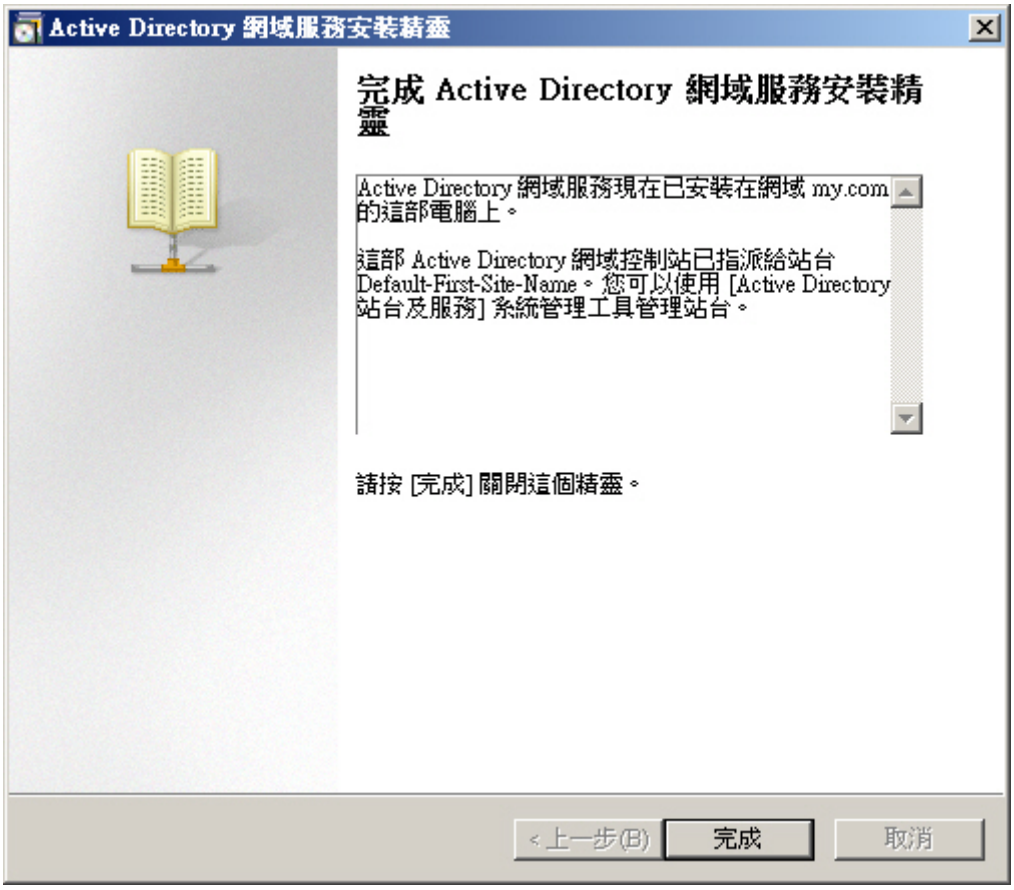


圖 8-70 完成 Active Directory 網域服務安裝

步驟2. 在【開始】>【程式集】>【系統管理工具】>【Active Directory 使用者和電腦】視窗中，做下列設定：（如圖 8-71）

- 在【Active Directory 使用者和電腦】>【所設定的 AD 網域（例如：my.com）】>【Users】項目上，按下滑鼠右鍵並選擇【新增】>【使用者】。（如圖 8-72）
- 在【新增物件-使用者】視窗中：
  - 輸入指定【姓氏】、【全名】、【使用者登入名稱】、【使用者登入名稱（Windows 2000 前版）】。
  - 按【下一步】鈕。（如圖 8-73）
  - 輸入指定【密碼】、【確認密碼】。
  - 勾選【密碼永久有效】。
  - 按【下一步】鈕。（如圖 8-74）
  - 按下【完成】鈕，完成設定。（如圖 8-75, 圖 8-76）

圖 8-71 開啟 Active Directory 使用者和電腦視窗

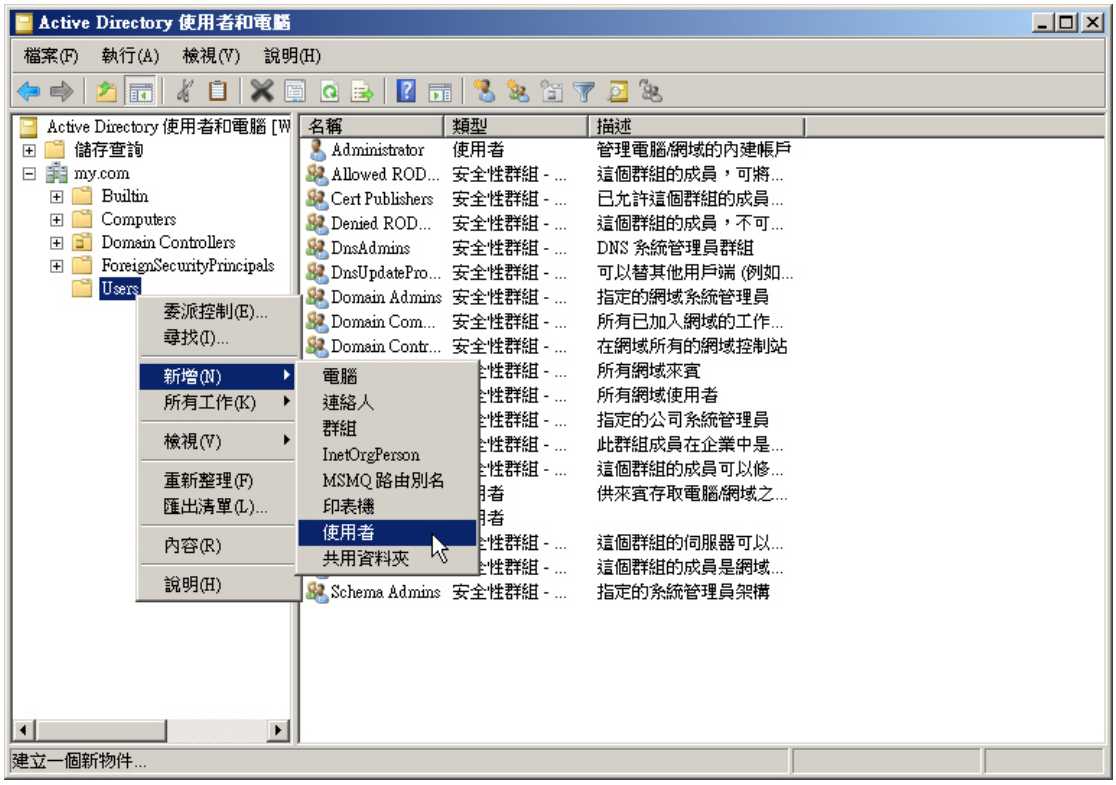


圖 8-72 開啟新增物件-使用者視窗

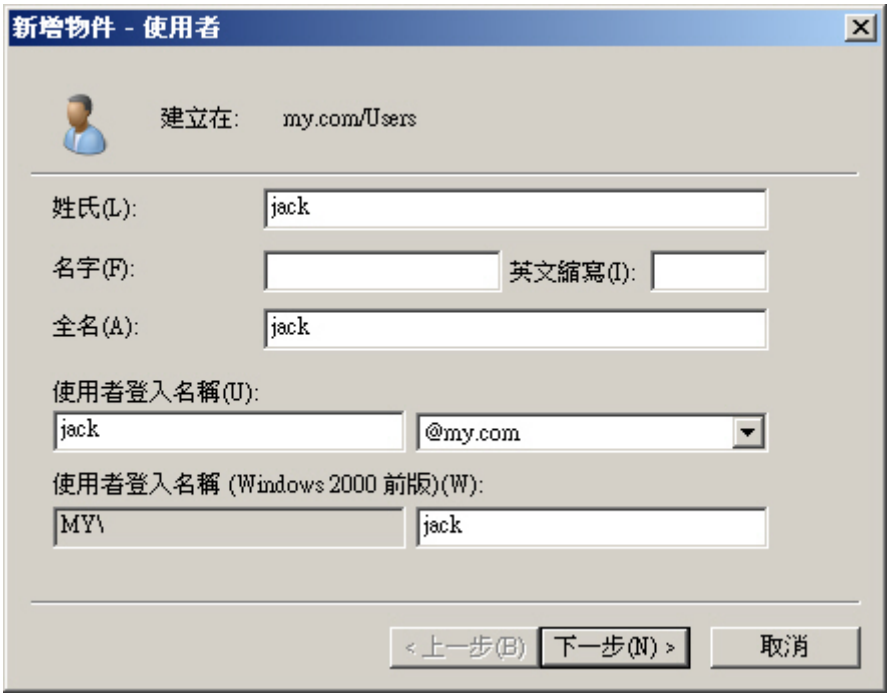


圖 8-73 設定新使用者帳號

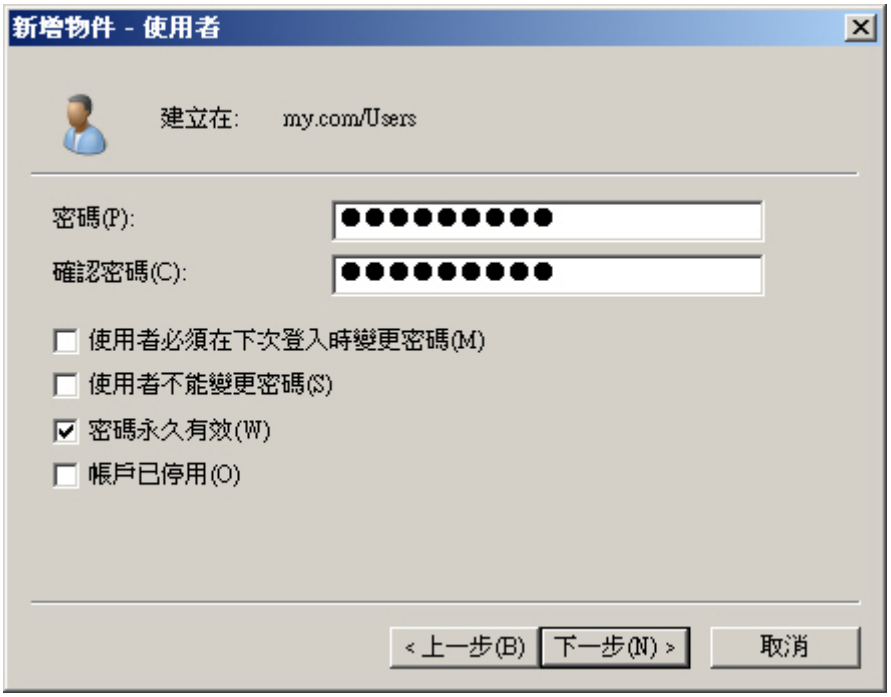


圖 8-74 設定新使用者密碼

圖 8-75 檢視新使用者設定

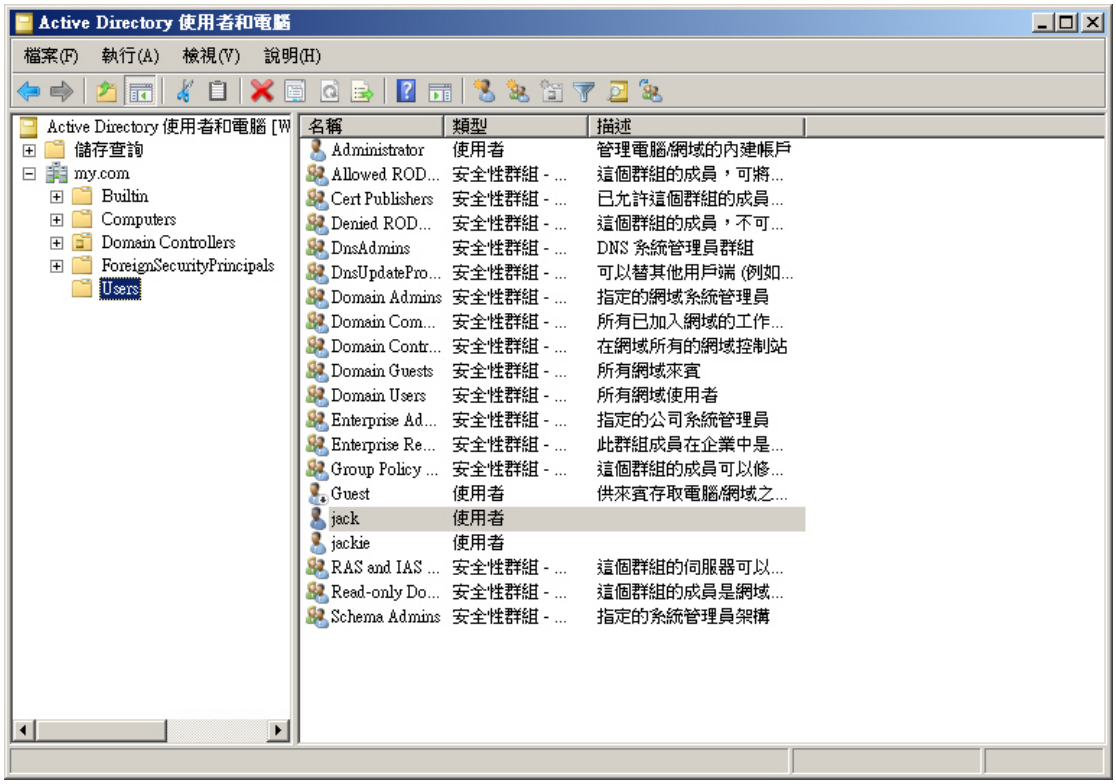


圖 8-76 完成新使用者設定

步驟3. 在【管制條例選項】>【認證表】>【外部 LDAP】頁面中，做下列設定：（如圖 8-77）

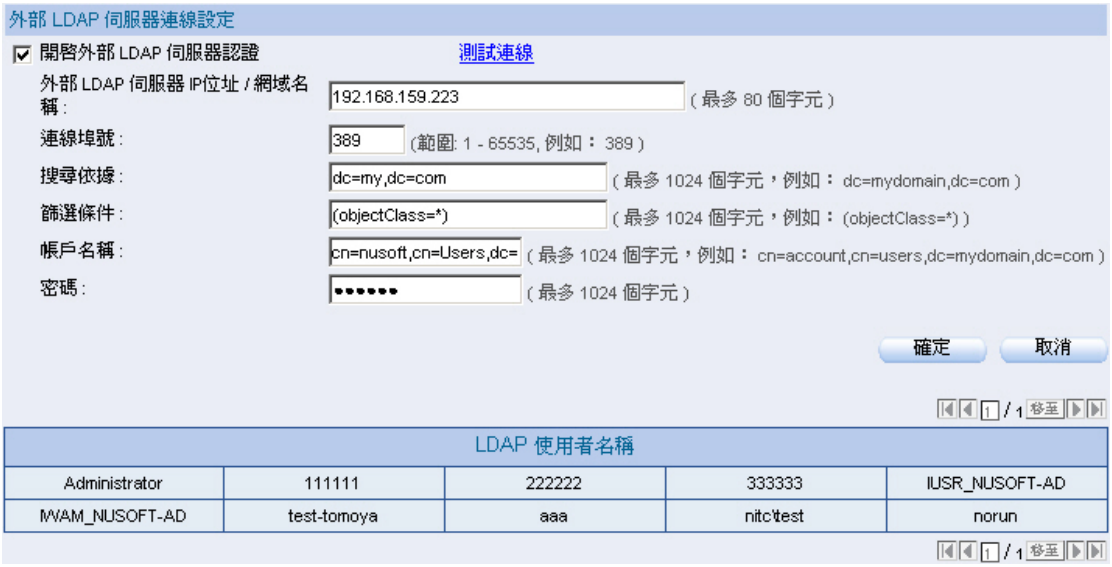


圖 8-77 LDAP 伺服器連線設定頁面

說明：

1. 按下【測試連線】，可以偵測出目前 MHG-2000 和 LDAP 伺服器是否可正常連線。
2. 【LDAP 使用者名稱】為 MHG-2000 連線 LDAP 伺服器所取得的帳戶清單，可將各帳戶依需求進行群組來提供授權認證。

步驟4. 在【管制條例選項】>【認證表】>【認證群組】頁面中，做下列設定：（如圖 8-78）

圖 8-78 認證群組設定頁面

步驟5. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 8-79）

- 【認證名稱】選擇所設定的認證群組規則。
- 按下【確定】鈕，完成設定。（如圖 8-80）

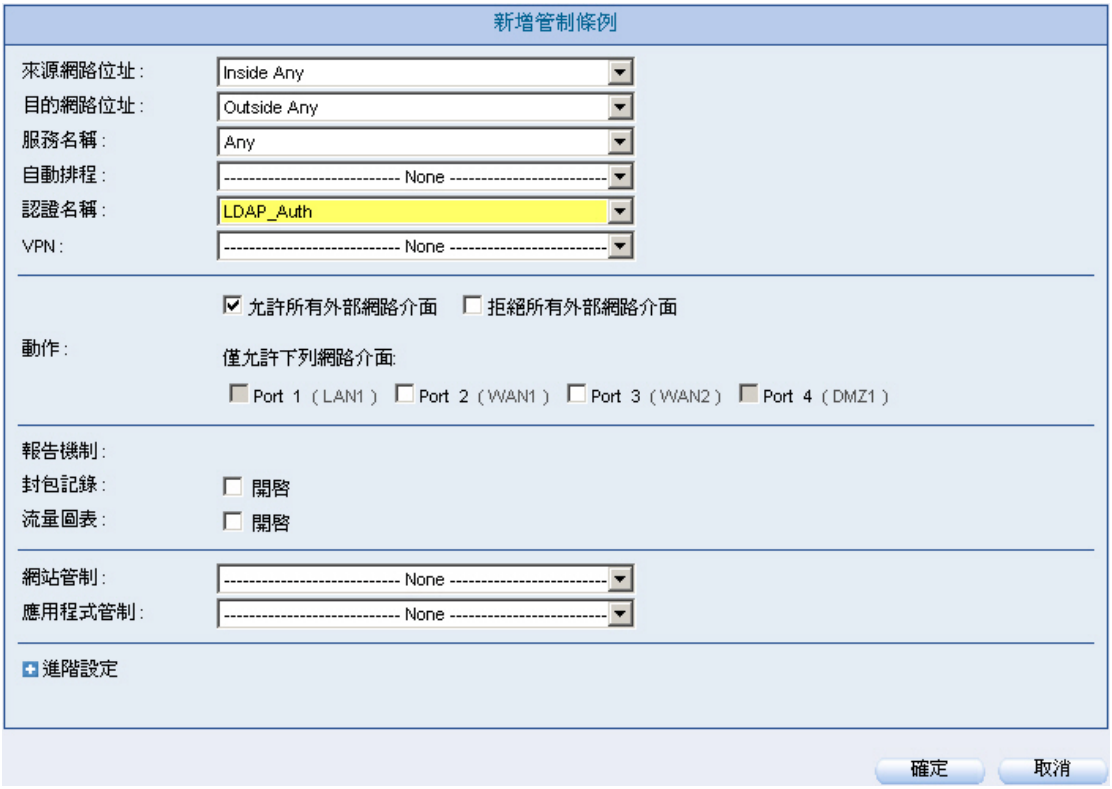


圖 8-79 管制條例套用認證規則

圖 8-80 完成管制條例設定

步驟6. 當內部使用者欲透過設定的認證管制條例瀏覽網頁時，即會先行連線認證頁面。在輸入正確的認證【帳戶名稱】和【密碼】後，按下【登入】鈕即可透過 MHG-2000 上網。（如圖 8-81）

圖 8-81 認證登入頁面

第9章　應用程式管制

可針對即時通訊登入、即時通訊傳檔、點對點軟體、影音軟體、網頁郵件、線上遊戲、通道軟體和遠端控制軟體做管制的動作。

【設定】功能概述：

應用程式特徵檔更新資訊 說明如下：

- 應用程式管制之特徵定義檔每隔 60 分鐘就會自動更新，或可手動做立即更新。同時會顯示特徵定義檔之更新時間和版本。

說明：

1. 若 MHG-2000 外部網路介面必需透過指定代理伺服器方可連線網際網路，可於【系統管理】>【組態】>【系統設定】頁面的【代理伺服器設定】欄位中，建立與該伺服器的連線。

即時通訊登入 說明如下：

- 可阻擋使用者登入 MSN、Yahoo、ICQ/AIM、QQ、Skype、Google Talk、Gadu-Gadu、Rediff、WebIM、阿里旺旺、百度 Hi、新浪 UC、Fetion、Facebook 聊天室、Camfrog、LINE、WhatsApp 和 Viber。

即時通訊傳檔 說明如下：

- 可阻擋使用者透過 MSN、Yahoo、ICQ/AIM、QQ、Google Talk 和 Gadu-Gadu 傳送檔案。

點對點軟體 說明如下：

- 可阻擋使用者建立 eDonkey/eMule、Bit Torrent/BitConnect、WinMX、Foxy、KuGoo、AppleJuice、AudioGalaxy、DirectConnect、iMesh、MUTE、迅雷 5、GoGoBox、QQ 旋風、Ares、Shareaza、BearShare、Morpheus、Limewire、KaZaa 和 FlashGet 連線。

影音軟體 說明如下：

- 可阻擋使用者使用 PPTV 網路電視、PPS 網路電視、UUSee 網路電視、QQLive、ezPeer、快播/波波虎、Funsion、PPMate 網路電視、PiPi、暴風影音、SopCast 網路電視、CNTV 和迅雷看看軟體。

網頁郵件 說明如下：

- 可阻擋使用者登入 Gmail、Hotmail、Yahoo、Hinet、PChome、智邦、Yam 天空、Seednet、163/126/Yeah、Tom、新浪任你郵、搜狐和 QQ 網頁郵件。

線上遊戲 說明如下：

- 可阻擋使用者登入聯眾世界、QQ 遊戲和迅雷遊戲大廳軟體。

通道軟體 說明如下：

- 可阻擋使用者建立 VNN Client、無界瀏覽、Tor、Hamachi、綠盾和自由門連線。

遠端控制軟體 說明如下：

- 可阻擋使用者建立 TeamViewer、VNC、遠端桌面和 ShowMyPC 連線。

9.1 應用程式管制功能使用範例

編碼	適用範圍	範例環境	頁碼
9.1.1	**即時通訊**	限制內部使用者以即時通訊軟體傳送訊息	**227**
9.1.2	**點對點軟體**	限制內部使用者以點對點軟體存取網路上之檔案	**229**

9.1.1 限制內部使用者以即時通訊軟體傳送訊息

步驟1. 在【管制條例選項】>【應用程式管制】>【設定】頁面中，做下列設定：（如圖 9-1）

- 輸入應用程式管制【名稱】。
- 展開【即時通訊登入】選單，勾選【全選】選項。
- 按下【確定】鈕，完成設定。（如圖 9-2）

圖 9-1 設定即時通訊管制

圖 9-2 完成即時通訊管制設定

步驟2. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 9-3）

- 選擇所設定的【應用程式管制】規則。
- 按下【確定】鈕，完成設定。（如圖 9-4）

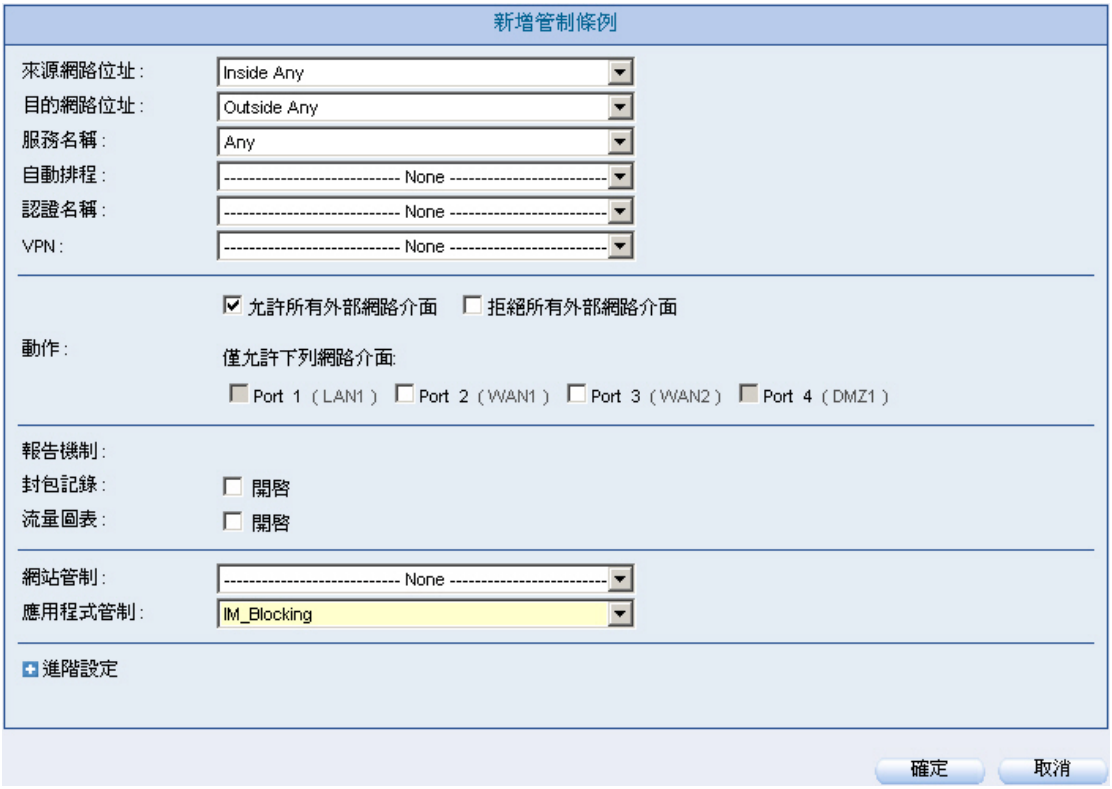


圖 9-3 管制條例套用即時通訊管制規則

圖 9-4 完成管制條例設定

9.1.2 限制內部使用者以點對點軟體存取網路上之檔案

步驟1. 在【管制條例選項】>【應用程式管制】>【設定】頁面中，做下列設定：（如圖 9-5）

- 輸入應用程式管制【名稱】。
- 展開【點對點軟體】選單，勾選【全選】選項。
- 按下【確定】鈕，完成設定。（如圖 9-6）

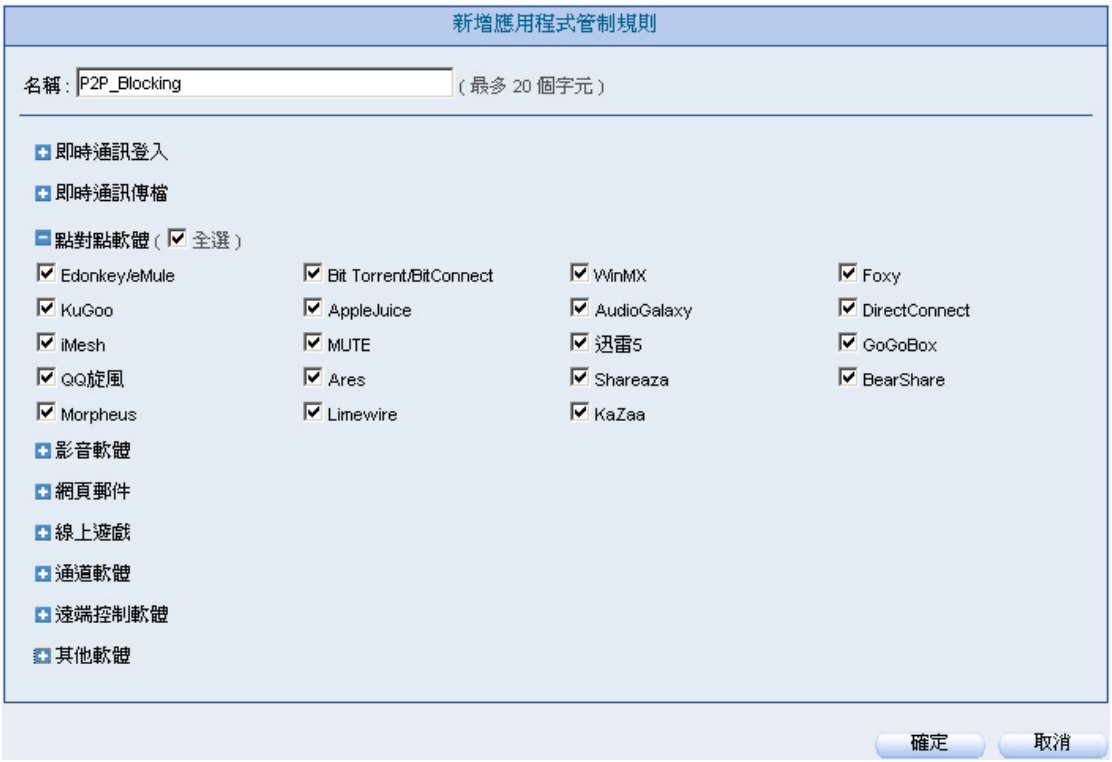


圖 9-5 設定點對點軟體管制

圖 9-6 完成點對點軟體管制設定

步驟2. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 9-7）

- 選擇所設定的【應用程式管制】規則。
- 按下【確定】鈕，完成設定。（如圖 9-8）

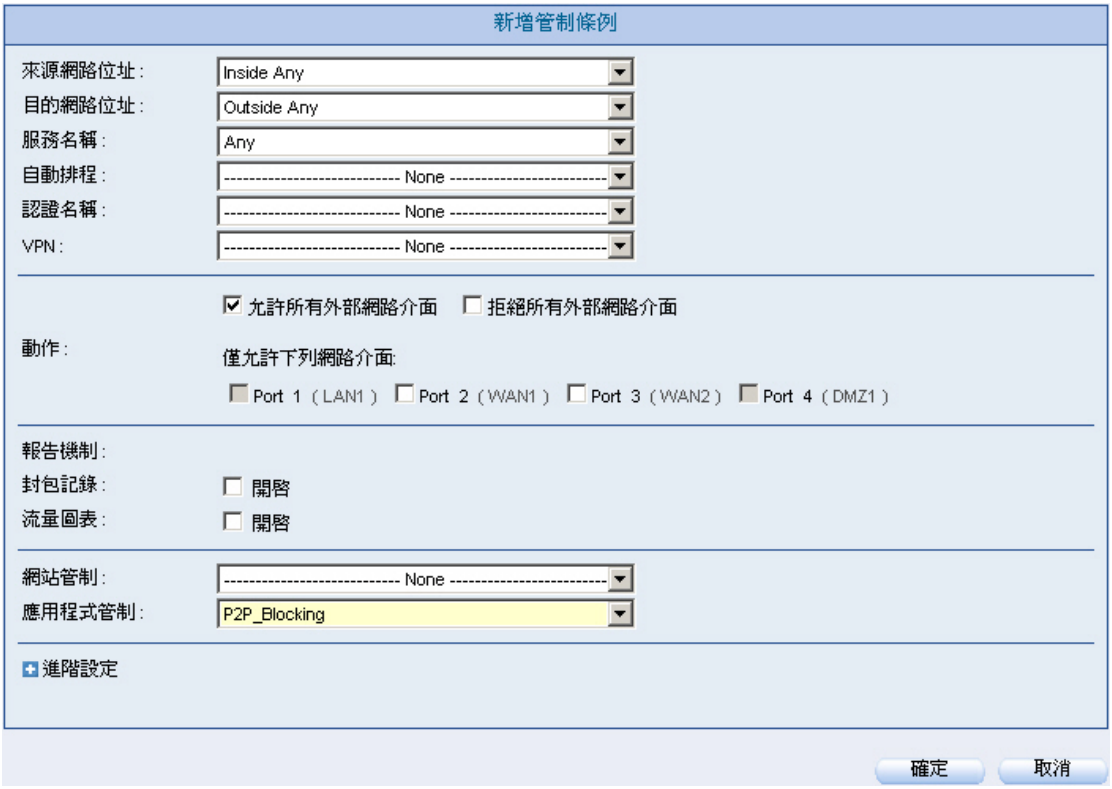


圖 9-7 管制條例套用點對點軟體管制規則

圖 9-8 完成管制條例設定

說明：

1. 點對點傳輸會嚴重佔用網路頻寬，進而影響到其他使用者。且點對點傳輸能自由變更服務埠號，故利用【管制條例選項】>【服務表】來針對點對點傳輸做管制動作，是無效的。因此系統管理員必須利用【管制條例選項】>【應用程式管制】>【設定】頁面的【點對點軟體】管制功能，才能有效阻止使用者使用點對點傳輸。

第10章　虛擬伺服器

用於將 MHG-2000 外部網路介面的真實 IP 位址，對應至內部網路設備的私有 IP 位址，以對外提供特定的網路服務。

- 【IP 對應】: 即一個外部網路真實 IP 位址的所有服務（埠號），對應到一個內部網路私有 IP 位址。
- 【連接埠對應】: 即一個外部網路真實 IP 位址，可對應到提供不同服務的多個內部網路私有 IP 位址。另外，可同時對應多個提供相同服務內容的內部網路私有 IP 位址，將尋求服務的連線循環分配給內部網路的伺服器群組。如此可減少單一伺服器的負載，降低當機的風險，提高伺服器的工作效率。
- 【連接埠對應群組】: 將【連接埠對應】規則群組，以特定的管制條例進行控管。

【IP 對應】功能概述：

外部網路位址 說明如下：

- 外部網路介面的真實 IP 位址。

對應到虛擬網路位址 說明如下：

- 外部網路真實 IP 位址對應的內部網路私有 IP 位址。

【連接埠對應】功能概述：

伺服器真實 IP 說明如下：

- 虛擬伺服器所採用的外部網路真實 IP 位址。

服務 說明如下：

- 虛擬伺服器可對應的服務項目名稱。

對外連線埠號 說明如下：

- 虛擬伺服器所對應的對外服務埠號。若所選擇的服務項目只有使用單一埠號時，則可在此變更其對外的埠號。（如將 HTTP 的埠號改為 8080，則外部使用者就必須以此埠號，存取所提供的 HTTP 服務）

伺服器負載平衡模式 說明如下：

- 循環分配：可將尋求服務的連線，依序分配給內部網路提供相同服務的伺服器群組；可減少單一伺服器的負載，提高伺服器的工作效率。（外部使用者若已有存取伺服器的連線，於其全部終止後 MHG-2000 尚會保留一段時間，以利使用者在限定時間內向同一台主機尋求服務）
- 備援模式：當主要伺服器發生異常或故障時，備援的伺服器會依編號順序接替主要伺服器的工作，使服務不致中斷。
- 依來源位址：辨識尋求服務的來源位址，將其連線至所設定的指定伺服器。

網路介面 說明如下：

- 用於指定虛擬伺服器之私有 IP 位址隸屬的網路介面。

伺服器虛擬 IP 說明如下：

- 虛擬伺服器所對應的內部網路私有 IP 位址。

10.1 虛擬伺服器功能使用範例

編碼	適用範圍	範例環境	頁碼
10.1.1	**IP 對應**	將內部提供FTP、Web、Mail等多項服務之單一伺服器，以IP對應的方式透過管制條例來對外服務	**234**
10.1.2	**連接埠對應**	將內部提供單一相同服務內容之多台伺服器，以連接埠對應的方式透過管制條例來對外服務。(以Web服務為例)	**238**
10.1.3	**連接埠對應**	外部使用者使用VoIP，對內部網路之VoIP連線（VoIP服務埠號：TCP 1720，TCP 15319-15333，UDP 15319-15333）	**242**
10.1.4	**連接埠對應**	將內部提供多項相同服務內容之多台伺服器，以連接埠對應的方式透過管制條例來對外服務。(以HTTP，POP3，SMTP，DNS服務群組為例)	**247**

環境設定

申請兩條有固接 IP 的 ADSL 線路。

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1 所連線路的固接 IP 為 61.11.11.10 ~ 61.11.11.14。

Port3 設為 WAN2 所連線路的固接 IP 為 211.22.22.18 ~ 211.22.22.30。

10.1.1 將內部提供 FTP、Web、Mail 等多項服務之單一伺服器，以 IP 對應的方式透過管制條例來對外服務

步驟1. 在內部網路中架設一提供多項服務之伺服器，其網卡 IP 設定為 192.168.1.100、DNS 設定指向於外部 DNS 伺服器。

步驟2. 在【管制條例選項】>【位址表】>【內部網路】頁面中，做下列設定：（如圖 10-1）

圖 10-1 內部網路位址表設定

步驟3. 在【管制條例選項】>【虛擬伺服器】>【IP 對應】頁面中，做下列設定：

- 輸入 IP 對應規則【名稱】。
- 【外部網路位址】選擇 Port2（WAN1）並輸入 61.11.11.12。（可輔助選取）
- 【對應到虛擬網路位址】選擇 Port1（LAN1）並輸入 192.168.1.100。（可輔助選取）
- 按下【確定】鈕，完成設定。（如圖 10-2）

圖 10-2IP 對應設定頁面

步驟4. 在【管制條例選項】>【服務表】>【服務群組】頁面中，將伺服器所提供的服務（DNS、FTP、HTTP、POP3、SMTP…）群組化（Main_Service），同時新增一條給伺服器對外發送郵件之服務群組規則（Mail_Service）。（如圖 10-3）

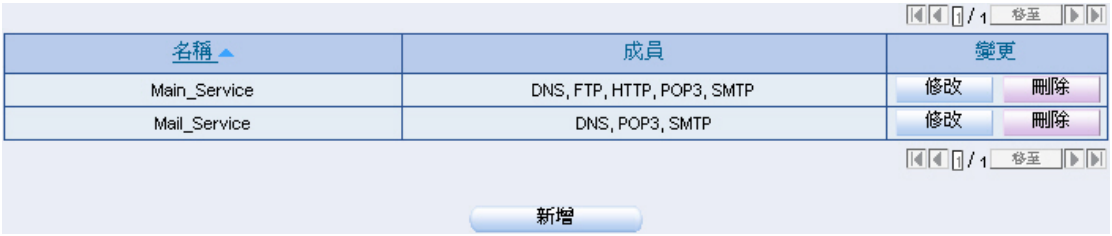


圖 10-3 服務群組設定

步驟5. 在【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 10-4）

- 【目的網路位址】選擇所設定的 IP 對應規則。
- 【服務名稱】選擇 Main_Service。
- 按下【確定】鈕，完成設定。（如圖 10-5）

圖 10-4 設定外部使用者存取內部伺服器服務之管制條例

圖 10-5 完成管制條例設定

步驟6. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 10-6）

- 【來源網路位址】選擇所設定的內部網路位址表規則。
- 【服務名稱】選擇 Mail_Service。
- 按下【確定】鈕，完成設定。（如圖 10-7）

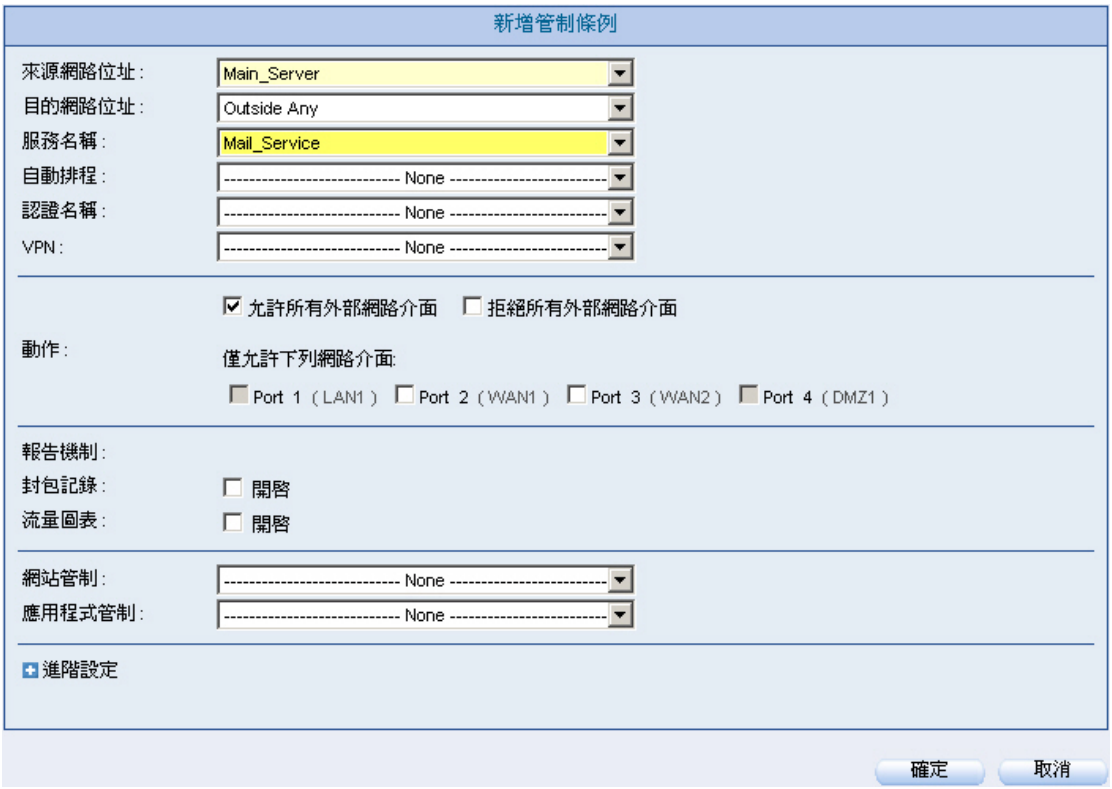


圖 10-6 設定內部伺服器對外發送郵件之管制條例

圖 10-7 完成管制條例設定

步驟7.　以 IP 對應對外提供多項服務之架設環境。（如圖 10-8）

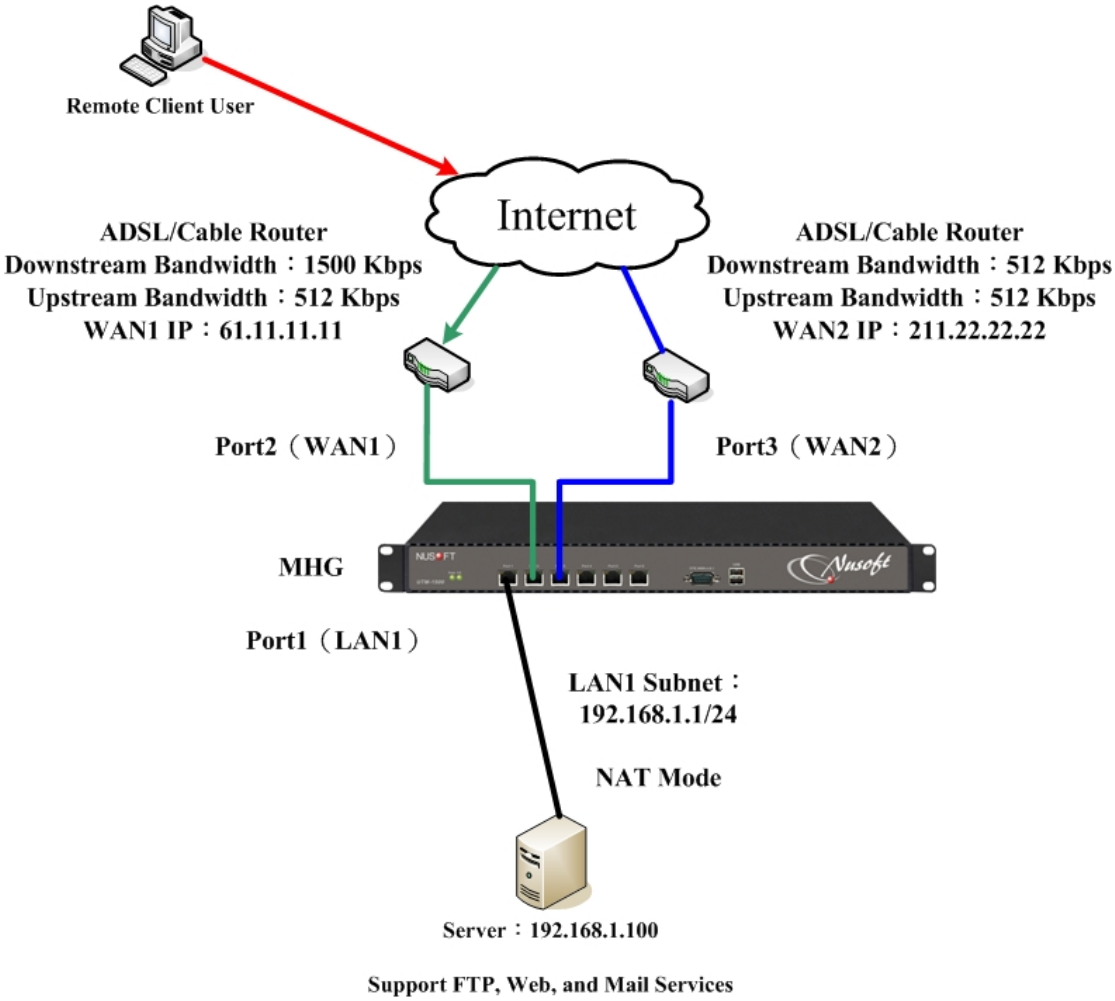


圖 10-8 伺服器透過 IP 對應提供多項服務之架設環境

說明：

1. 在用【IP 對應】設定管制條例時，強力建議服務不要選擇 ANY。否則易將【IP 對應】的對象暴露在網際網路中，而遭受駭客的入侵。

10.1.2 將內部提供單一相同服務內容之多台伺服器，以連接埠對應的方式透過管制條例來對外服務。(以 Web 服務為例)

步驟1. 在內部網路中架設多台提供相同 Web 服務內容之伺服器，其 IP 位址為 192.168.1.101、192.168.1.102、192.168.1.103、192.168.1.104。

步驟2. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 10-9）

- 輸入連接埠對應規則【名稱】。
- 【伺服器真實 IP】選擇 Port3（WAN2）並輸入 211.22.22.23。（可輔助選取）
- 【服務】選擇 HTTP(80)。
- 【對外連線埠號】更改為 8080。
- 【伺服器負載平衡模式】選擇循環分配。
- 【網路介面】選擇 LAN，按【下一列】鈕。
- 【伺服器虛擬 IP1】輸入 192.168.1.101，按【下一列】鈕。（可輔助選取）
- 【伺服器虛擬 IP2】輸入 192.168.1.102，按【下一列】鈕。（可輔助選取）
- 【伺服器虛擬 IP3】輸入 192.168.1.103，按【下一列】鈕。（可輔助選取）
- 【伺服器虛擬 IP4】輸入 192.168.1.104。（可輔助選取）
- 按下【確定】鈕，完成設定。（如圖 10-10）

圖 10-9 設定連接埠對應

圖 10-10 完成連接埠對應設定

步驟3. 在【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 10-11）

- 【目的網路位址】選擇所設定的虛擬伺服器規則。
- 【服務名稱】選擇 HTTP(8080)。
- 按下【確定】鈕，完成設定。（如圖 10-12）

圖 10-11 設定外部使用者存取內部伺服器服務之管制條例

圖 10-12 完成管制條例設定

說明：

1. 在此範例中，外部網路使用者如需進入該 Web 伺服器所架設的網站，則必須更改埠號為 8080，方可進入該網站。

步驟4. 透過虛擬伺服器將多台提供單一相同服務內容的主機對外開放之架設環境。（如圖 10-13）

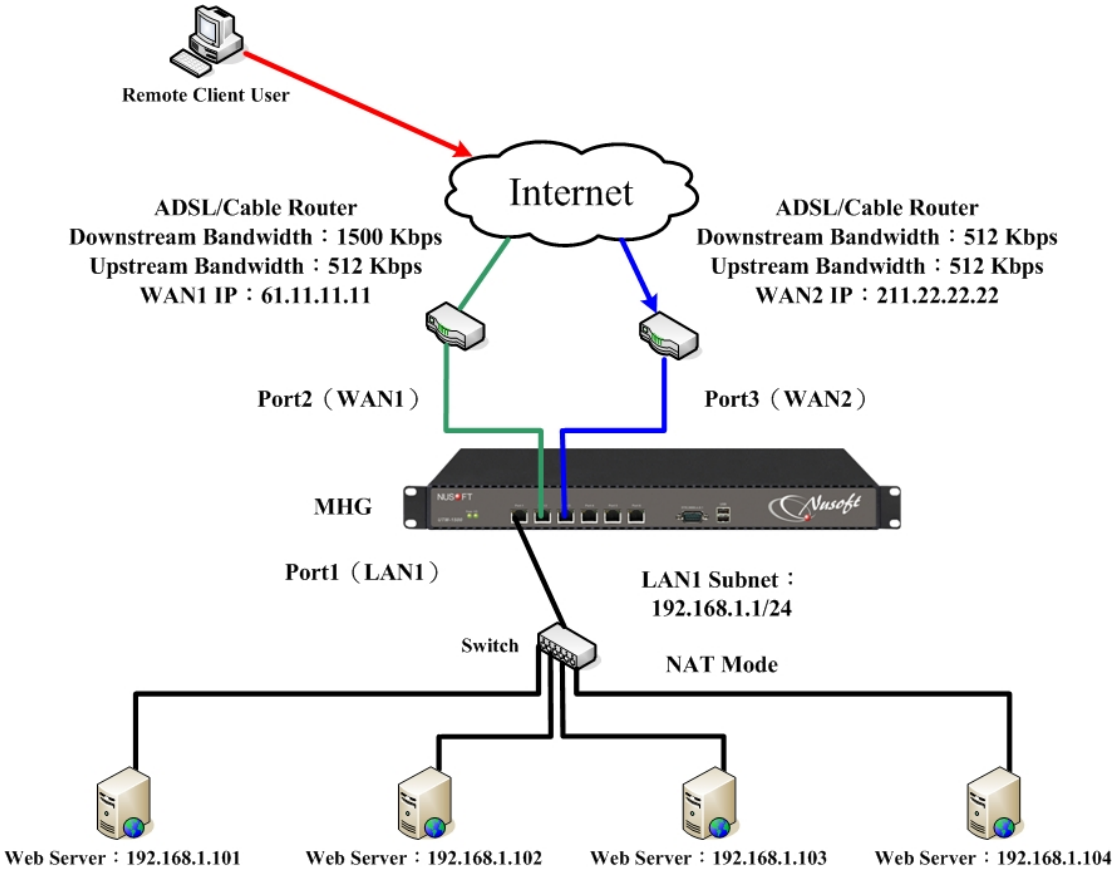


圖 10-13 多台主機透過虛擬伺服器提供單一相同服務內容之架設環境

10.1.3 外部使用者使用 VoIP，對內部網路之 VoIP 連線（VoIP 服務埠號：TCP 1720，TCP 15319-15333，UDP 15319-15333）

步驟1. 在內部網路架設 VoIP，其 IP 位址為 192.168.1.100。

步驟2. 在【管制條例選項】>【位址表】>【內部網路】頁面中，做下列設定：（如圖 10-14）

圖 10-14 內部網路位址表設定

步驟3. 在【管制條例選項】>【服務表】>【自訂服務】頁面中，做下列設定：（如圖 10-15）

圖 10-15 自訂服務設定

步驟4. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 10-16）

- 輸入連接埠對應規則【名稱】。
- 【伺服器真實 IP】選擇 Port2（WAN1）並輸入 61.11.11.12。（可輔助選取）
- 【服務】選擇所設定的自訂服務規則。
- 【對外連線埠號】自動設為自訂服務。
- 【伺服器負載平衡模式】選擇循環分配。
- 【網路介面】選擇 LAN。
- 【伺服器虛擬 IP1】輸入 192.168.1.100。（可輔助選取）
- 按下【確定】鈕，完成設定。（如圖 10-17）

圖 10-16 設定連接埠對應

圖 10-17 完成連接埠對應設定

說明：

1. 若所自訂的服務只有用到單一個埠號，則連接埠對應中的【對外連線埠號】可以更動；相反的，當所自訂的服務有用到一個以上的埠號時，則連接埠對應中的【對外連線埠號】不可更動。

步驟5. 在【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 10-18）

- 【目的網路位址】選擇所設定的虛擬伺服器規則。
- 【服務名稱】選擇所設定的自訂服務規則。
- 按下【確定】鈕，完成設定。（如圖 10-19）

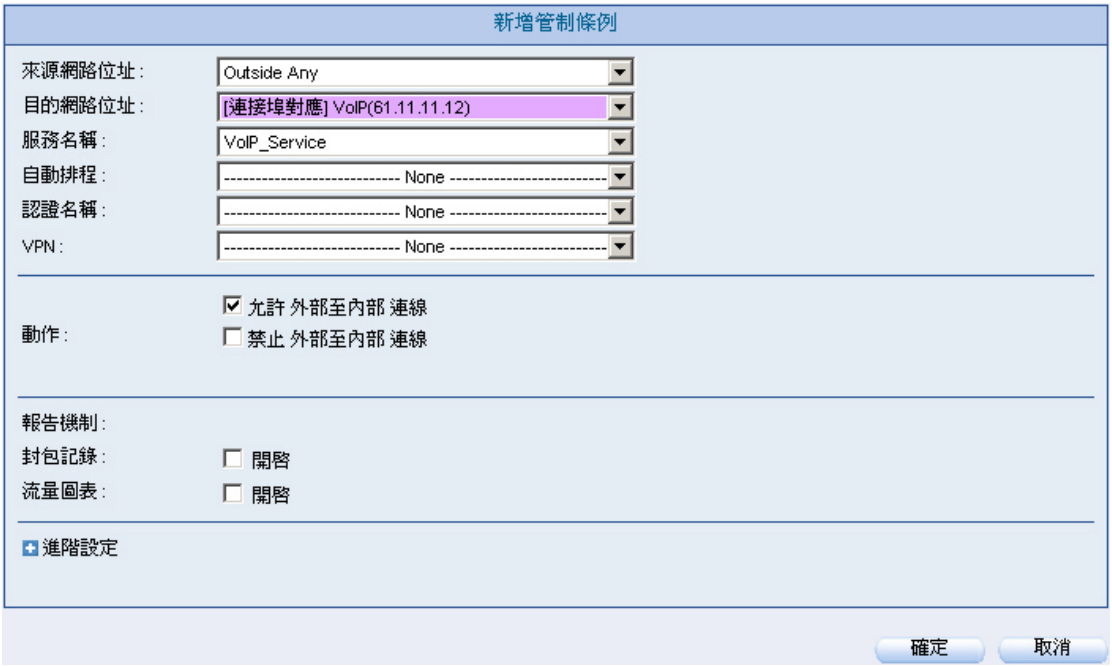


圖 10-18 設定外部對內部 VoIP 溝通之管制條例

圖 10-19 完成管制條例設定

步驟6. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 10-20）

- 【來源網路位址】選擇所設定的內部網路位址表規則。
- 【服務名稱】選擇所設定的自訂服務規則。
- 【管制動作,外部網路埠】勾選 Port2（WAN1）。
- 按下【確定】鈕，完成設定。（如圖 10-21）

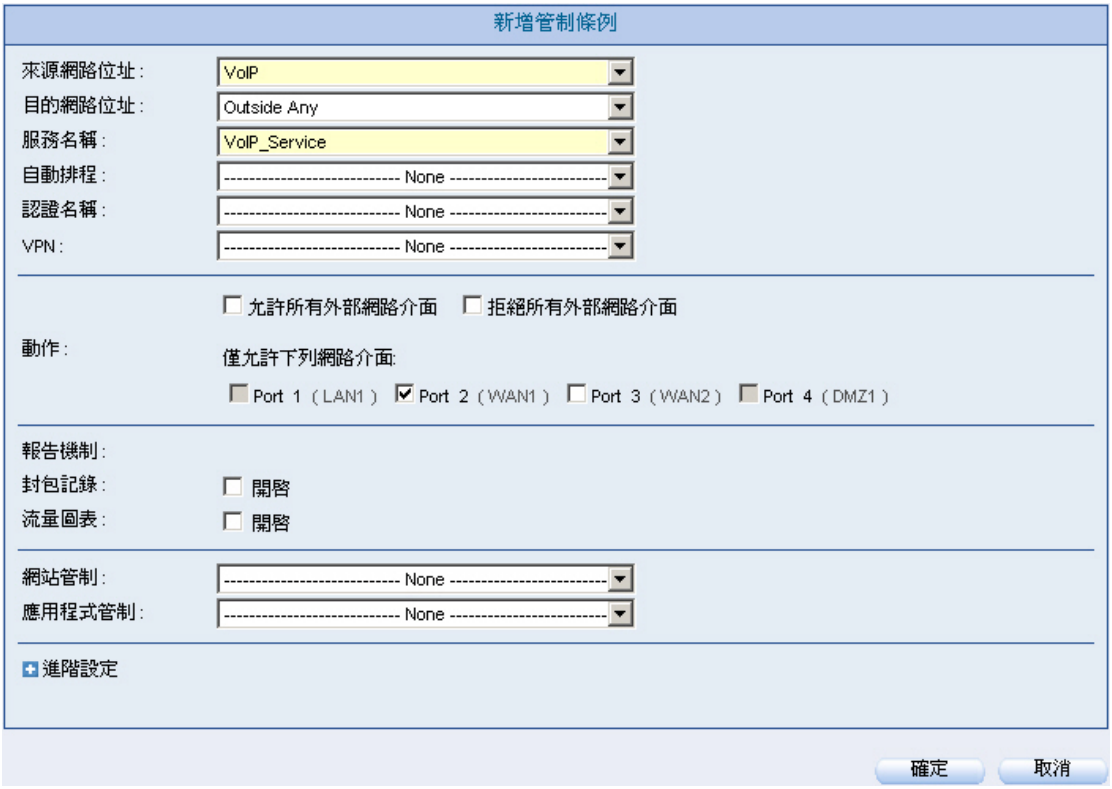


圖 10-20 設定內部對外部 VoIP 溝通之管制條例

圖 10-21 完成管制條例設定

步驟7. 透過虛擬伺服器將使用特定服務的設備對外開放之架設環境。（如圖 10-22）

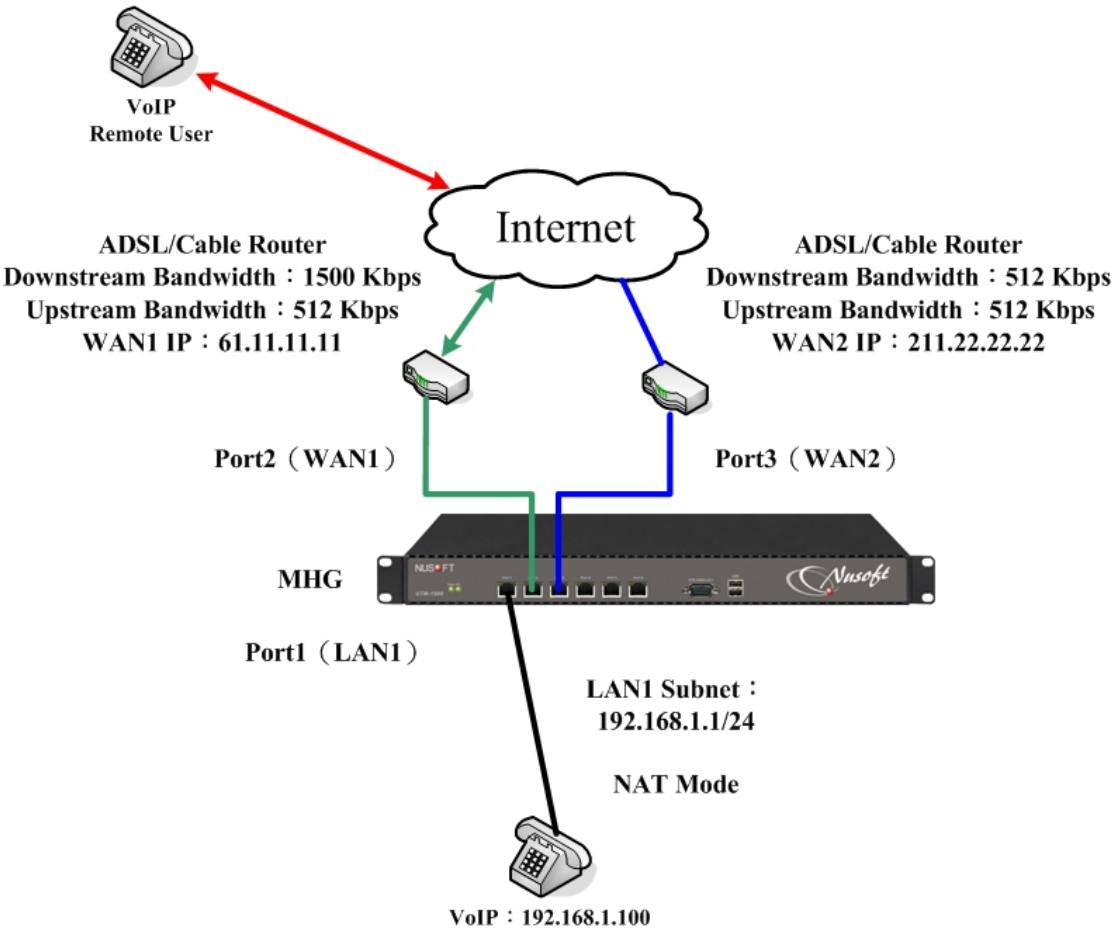


圖 10-22 使用特定服務的設備透過虛擬伺服器互相溝通之架設環境

10.1.4 將內部提供多項相同服務內容之多台伺服器，以連接埠對應的方式透過管制條例來對外服務。(以 HTTP，POP3，SMTP，DNS 服務群組為例)

步驟1. 在內部網路中架設多台提供多項相同服務內容之伺服器，其網卡 IP 設定為 192.168.1.101、192.168.1.102、192.168.1.103、192.168.1.104，且其 DNS 設定指向於外部 DNS 伺服器。

步驟2. 在【管制條例選項】>【位址表】>【內部網路】和【內部網路群組】頁面中，做下列設定：（如圖 10-23, 圖 10-24）

圖 10-23 內部網路位址表設定

圖 10-24 內部網路位址群組設定

步驟3. 在【管制條例選項】>【服務表】>【服務群組】頁面中，將伺服器所提供的服務（DNS、HTTP、POP3、SMTP）群組化（Main_Service），同時新增一條給伺服器對外發送郵件之服務群組規則（Mail_Service）。（如圖 10-25）

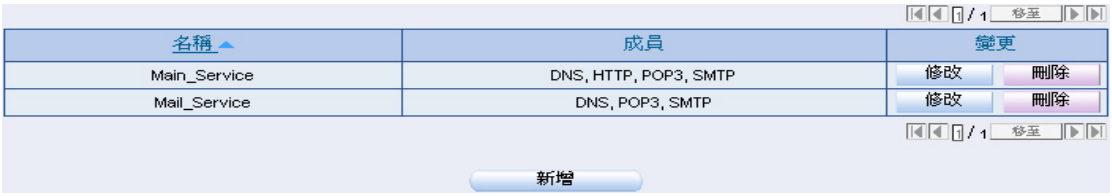


圖 10-25 服務群組設定

步驟4. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 10-26）

- 輸入連接埠對應規則【名稱】。
- 【伺服器真實 IP】選擇 Port3（WAN2）並輸入 211.22.22.23。（可輔助選取）
- 【服務】選擇所設定的服務群組。
- 【對外連線埠號】自動設為服務群組。
- 【伺服器負載平衡模式】選擇循環分配。
- 【網路介面】選擇 LAN，按【下一列】鈕。
- 【伺服器虛擬 IP 1】輸入 192.168.1.101，按【下一列】鈕。（可輔助選取）
- 【伺服器虛擬 IP 2】輸入 192.168.1.102，按【下一列】鈕。（可輔助選取）
- 【伺服器虛擬 IP 3】輸入 192.168.1.103，按【下一列】鈕。（可輔助選取）
- 【伺服器虛擬 IP 4】輸入 192.168.1.104。（可輔助選取）
- 按下【確定】鈕，完成設定。（如圖 10-27）

圖 10-26 設定連接埠對應

圖 10-27 完成連接埠對應設定

步驟5. 在【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 10-28）

- 【目的網路位址】選擇所設定的虛擬伺服器規則。
- 【服務名稱】選擇 Main_Service。
- 按下【確定】鈕，完成設定。（如圖 10-29）

圖 10-28 設定外部使用者存取內部伺服器服務之管制條例

圖 10-29 完成管制條例設定

步驟6. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 10-30）

- 【來源網路位址】選擇所設定的內部網路位址表規則。
- 【服務名稱】選擇 Mail_Service。
- 按下【確定】鈕，完成設定。（如圖 10-31）

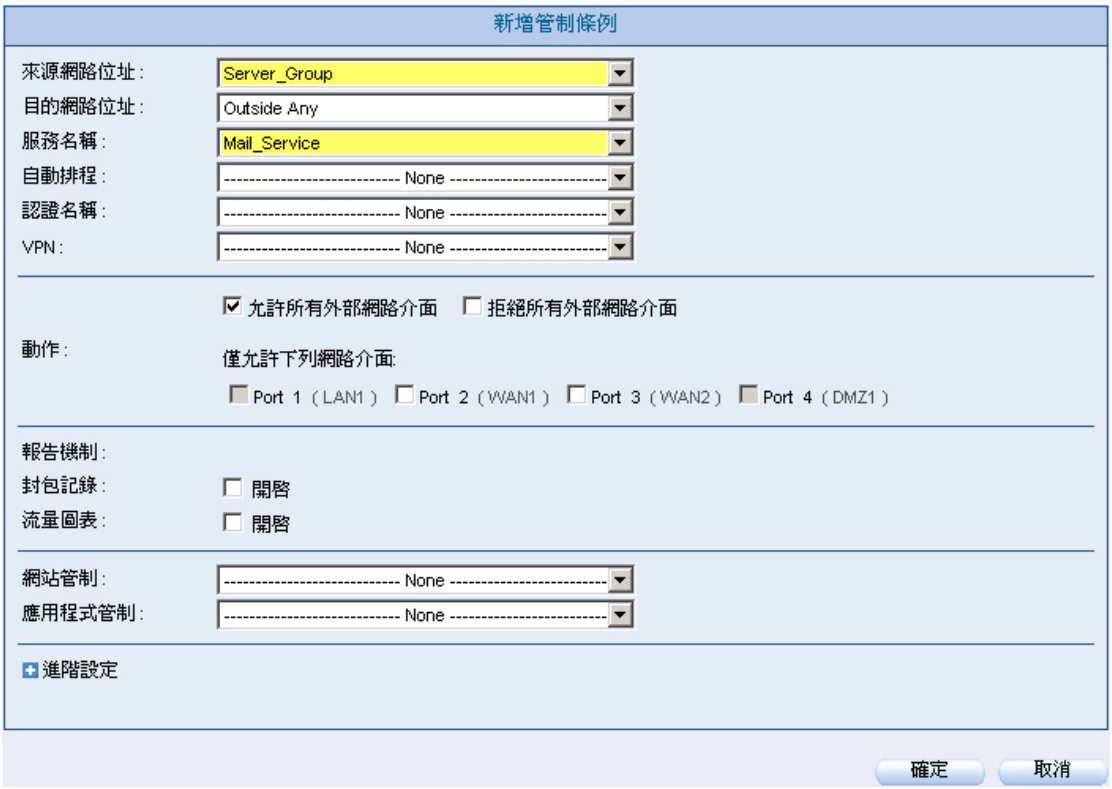


圖 10-30 設定內部伺服器對外發送郵件之管制條例

圖 10-31 完成管制條例設定

步驟7. 透過虛擬伺服器將多台提供多項相同服務內容的主機對外開放之架設環境。（如圖 10-32）

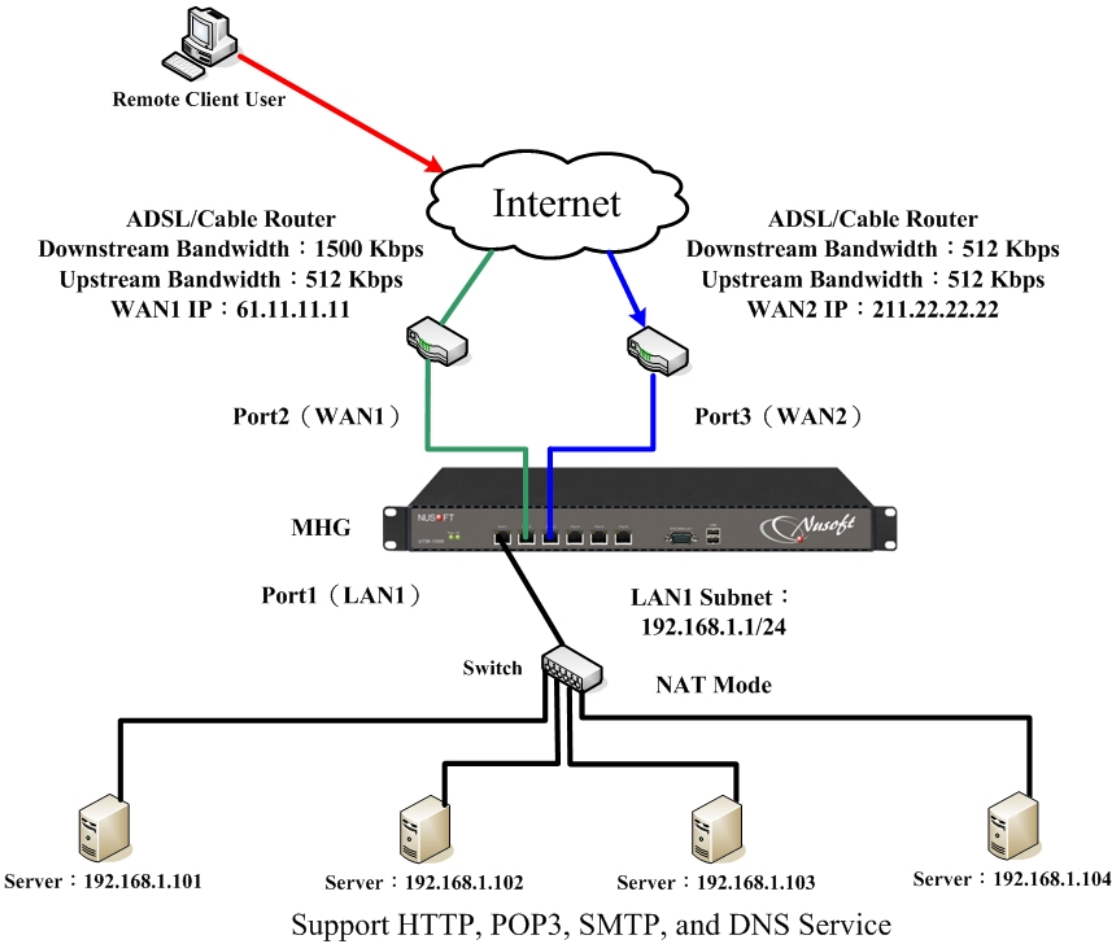


圖 10-32 多台主機透過虛擬伺服器提供多項相同服務內容之架設環境

第11章　VPN

用來建立安全與私密的網路連線，藉以整合企業各分點網路，讓外勤人員便於連線企業網路；企業在網際網路上傳遞資料時，亦能得到最佳的保密效果。

說明：

1. 建立虛擬私人網路 Virtual Private Network (VPN)，需先將【管制條例選項】>【VPN】>【IPSec 自動加密】、【PPTP 伺服器】或【PPTP 用戶端】的連線設定套用到【Trunk】中，並將要彼此連線溝通的 VPN Trunk 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】專有名詞概述：

Diffie-Hellman 說明如下：

- 為對稱性密碼系統，它可以讓連線兩端在完全沒有彼此任何預先資訊的條件下，透過不安全通道建立起一個金鑰，並使用此金鑰將訊息加密傳送。

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，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。

Pre-Shared Key 說明如下：

- IPSec 連線時用來進行驗證的專用密碼。

ISAKMP 說明如下：

- 「IP Security Association Key Management Protocol」(ISAKMP) 就是提供一種方法讓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 做為起點，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 IPSec 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 IPSec 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，使用的加密金鑰爲 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，使用的加密金鑰爲 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 VPN 一起使用，由 VPN 爲用戶資料加密，給用戶提供更好的安全服務。

延伸認證（Xauth） 說明如下：

- 會在 IPSec 第一階段和第二階段的 IKE 之間插入一個新訊息，為 IPSec 提供 Challenge/Response、Two-factor 等單向非對稱用戶認證方法。

說明：

1. 【延伸認證】會以【管制條例選項】>【認證表】>【認證帳戶】做為驗證依據。

【IPSec 一步設定】功能概述：

IPSec 一步設定 說明如下：

- 用一個步驟快速完成 IPSec VPN 的連線設定。
  - 在【管制條例選項】>【VPN】>【IPSec 一步設定】頁面中，做下列設定：
    - 輸入指定的 VPN 連線【名稱】。（如圖 11-1）
    - 選擇本地端用來建立 VPN 的【連線介面】。
    - 選擇本地端欲透過 VPN 連線傳輸封包的【本地端 IP 位址 / 子網路遮罩】。
    - 輸入遠端用來建立 VPN 連線的【遠端閘道固定 IP 位址 / 網域名稱】。
    - 輸入遠端欲透過 VPN 連線傳輸封包的【遠端 IP 位址 / 子網路遮罩】。
    - 輸入【預先公用金鑰】。
    - 按下【確定】鈕。
    - 系統自動完成相關的【IPSec 自動加密】、【Trunk】和【管制條例】規則新增動作。（如圖 11-2, 圖 11-3, 圖 11-4, 圖 11-5）

圖 11-1 IPSec 一步設定頁面

圖 11-2 自動新增 IPSec 自動加密規則

圖 11-3 自動新增 VPN Trunk 規則

圖 11-4 自動新增 VPN Trunk 內部至外部管制條例

圖 11-5 自動新增 VPN Trunk 外部至內部管制條例

說明：

1. 為方便使用者建立 IPSec VPN 連線，【IPSec 一步設定】將許多必填資料和執行步驟，以內定值（如下所列）迅速完成設置作業：
   - 使用模式：Main mode。
   - 認證方法：Preshare。
   - ISAKMP 演算法：DES + MD5 + Diffie-Hellman 1。
   - IPSec 演算法：DES + MD5。
   - 系統會自動新增相關的【IPSec 自動加密】、【Trunk】和【管制條例】規則。

【VPN 精靈】功能概述：

VPN 精靈 說明如下：

- 依照系統提示逐步完成建立 VPN 連線的設定。
  - 在【管制條例選項】>【VPN】>【VPN 精靈】頁面中，做下列設定：
    - 選擇欲建立的 VPN 連線方式，按【下一步】鈕。**（如圖 11-6）**
    - 輸入 VPN 的連線設定，按【下一步】鈕。**（如圖 11-7）**
    - 設定 VPN Trunk 套用指定的 VPN 規則，按【下一步】鈕。**（如圖 11-8）**
    - 選擇指定的 Trunk 來進行【管制條例設定】。**（如圖 11-9）**
    - 按下【完成】鈕。**（如圖 11-10）**
    - 此時會完成套用 VPN Trunk 的相關【管制條例】設定，並於 VPN 建起連線時，能正常透過此機制傳輸封包。**（如圖 11-11, 圖 11-12）**

圖 11-6 選擇欲建立的 VPN 連線方式

圖 11-7 建立 VPN 規則

圖 11-8 設定 VPN Trunk

圖 11-9 選擇欲套用至管制條例的 VPN Trunk 規則

圖 11-10 完成 VPN 連線設定

圖 11-11 完成 VPN Trunk 內部至外部管制條例的設定

圖 11-12 完成 VPN Trunk 外部至內部管制條例的設定

【IPSec 自動加密】規則表概述：

i 說明如下：

■ 以圖示顯示 VPN 連線建立的狀況。

圖例		
代表涵義	斷線	連線

名稱 說明如下：

■ 用來定義 IPSec 自動加密名稱（不可重複）。

連線介面 說明如下：

■ 本地端外部網路介面。

遠端閘道 說明如下：

■ 遠端閘道外部網路介面位址。

IPSec 演算法 說明如下：

■ 顯示目前 VPN 連線的資料加密模式。

連線歷時 說明如下：

■ 顯示 IPSec VPN 持續連線時間。

變更 說明如下：

■ 修改或刪除 IPSec 自動加密規則。（如圖 11-13）

圖 11-13 IPSec 自動加密規則表

說明：

1. 在預設的情況下，MHG-2000 會利用【斷線偵測機制】(Dead Peer Detection)檢查 IPSec VPN 的連線狀態。當【遠端設定】選填遠端閘道 固定 IP 位址 / 網域名稱時，可讓管理者利用【手動連線】方式來建立 IPSec VPN 連線。

【PPTP 伺服器】規則表概述：

PPTP 伺服器設定 說明如下：

- 用來啟動或關閉 PPTP 伺服器。
- 可讓 PPTP 伺服器支援 RADIUS 連線驗證。
- 設定 PPTP 用戶端連入時分配的 IP 位址範圍、DNS 伺服器、WINS 伺服器。

i 說明如下：

- 以圖示顯示 VPN 連線建立的狀況。

圖例		
代表涵義	斷線	連線

使用者名稱 說明如下：

- PPTP 用戶端連入時所使用的驗證名稱。

用戶端 IP 位址 說明如下：

- PPTP 用戶端連入時取得的連線 IP 位址。

連線歷時 說明如下：

- 顯示 PPTP 用戶端與 PPTP 伺服器持續連線時間。

變更 說明如下：

- 修改或刪除 PPTP 伺服器規則。（如圖 11-14）

圖 11-14PPTP 伺服器規則表

說明：

1. 在預設的情況下，MHG-2000 會利用【Echo-Request】機制，檢查 PPTP VPN 的連線狀態。啟用【手動斷線】功能，可讓管理者立即中斷連入 PPTP 伺服器的 VPN 連線。

【PPTP 用戶端】規則表概述：

i 說明如下：

■ 以圖示顯示 VPN 連線建立的狀況。

圖例		
代表涵義	斷線	連線

使用者名稱 說明如下：

■ PPTP 用戶端連入 PPTP 伺服器時所使用的驗證名稱。

伺服器 IP 位址 / 網域名稱 說明如下：

■ PPTP 用戶端連入的 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，是否開啟加密認證機制。

連線歷時 說明如下：

■ 顯示 PPTP 用戶端與 PPTP 伺服器持續連線時間。

變更 說明如下：

■ 修改或刪除 PPTP 用戶端規則。（如圖 11-15）

圖 11-15 PPTP 用戶端規則表

說明：

1. 在預設的情況下，MHG-2000 會利用【Echo-Request】機制，檢查 PPTP VPN 的連線狀態。或讓管理者利用【手動連線】方式來建立 PPTP VPN 連線。

【Trunk】規則表概述：

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	斷線	連線

名稱 說明如下：

■ 用來定義 VPN Trunk 名稱（不可重複）。

本地端子網路 說明如下：

■ 本地端欲透過 VPN 傳輸封包的子網路。

遠端子網路 說明如下：

■ 遠端欲透過 VPN 傳輸封包的子網路。

VPN 通道 說明如下：

■ 顯示 VPN Trunk 所包含的虛擬私人網路（VPN）通道（IPSec、PPTP 伺服器、PPTP 用戶端）。

變更 說明如下：

■ 修改或刪除 VPN Trunk 規則。**（如圖 11-16）**

圖 11-16 VPN Trunk 規則表

說明：

1. 在【啟動 Trunk 負載平衡】機制時，會將單一連線的封包分由所整合的各 VPN 通道同時傳輸，加快完成的速度；同時，亦會依照【網路介面】>【介面位址】頁面的【負載平衡模式】，自動調整資料傳送的連線、傳輸狀態。兩端點必須是支援此機制的設備，才能發揮實質效果。

【Trunk 群組】規則表概述：

名稱 說明如下：

- 用來定義 Trunk 群組名稱（不可重複）。

成員 說明如下：

- 群組欲採用相同管制條例的 VPN Trunk 規則。

變更 說明如下：

- 修改或刪除 Trunk 群組規則。（如圖 11-17）

圖 11-17Trunk 群組規則表

11.1 VPN 功能使用範例

編碼	適用範圍	範例環境	頁碼
11.1.1	**IPSec 自動加密**	使用兩台MHG-2000 建立的IPSec VPN連線，存取特定網段的資源	**267**
11.1.2	**IPSec 自動加密**	使用一台MHG-2000 與Windows 7 設定IPSec VPN連線的方法	**278**
11.1.3	**IPSec 自動加密**	使用兩台MHG-2000 設定IPSec VPN連線的方法（連線使用Aggressive mode演算法）	**315**
11.1.4	**IPSec 自動加密**	使用兩台MHG-2000 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）	**327**
11.1.5	**IPSec 自動加密**	使用三台MHG-2000 設定IPSec VPN Hub連線的方法	**357**
11.1.6	**PPTP**	使用兩台MHG-2000設定PPTP VPN的OutBound Load Balance連線方法	**377**
11.1.7	**PPTP**	使用兩台MHG-2000 設定PPTP VPN用戶端透過伺服器端連上網際網路的方法	**391**
11.1.8	**PPTP**	使用一台MHG-2000 與Windows 7 設定PPTP VPN連線的方法	**398**

11.1.1 使用兩台 MHG-2000 建立的 IPSec VPN 連線，存取特定網段的資源

環境設定

甲公司 Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

乙公司 Port1 設為 LAN1（192.168.20.1）為 192.168.20.x/24 網段。

Port2 設為 WAN1（211.22.22.22）和 ATU-R 對接，連上網際網路。

有多重網段（192.168.85.1）為 192.168.85.X/24 網段。

本範例以兩台 MHG-2000 做為平台操作，甲公司和乙公司建立 VPN（虛擬私人網路）連線以傳送資料。

甲公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。**（如圖 11-18）**

圖 11-18IPSec 自動加密頁面

步驟2. 【名稱】輸入 VPN_A、【連線介面】選擇 Port2（WAN1）。**（如圖 11-19）**

圖 11-19 設定 IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的乙公司閘道位址。**（如圖 11-20）**

圖 11-20 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-21）

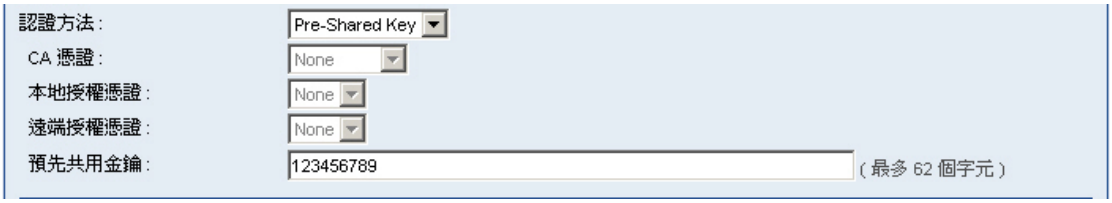


圖 11-21 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-22）

圖 11-22 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-23）

圖 11-23 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-24）

圖 11-24 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟8. 完成 IPSec 自動加密設定。（如圖 11-25）

圖 11-25 完成 IPSec 自動加密設定

步驟9. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-26）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入乙公司的子網路 192.168.85.0/255.255.255.0。
- 將【可選取的通道】VPN_A 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-27）

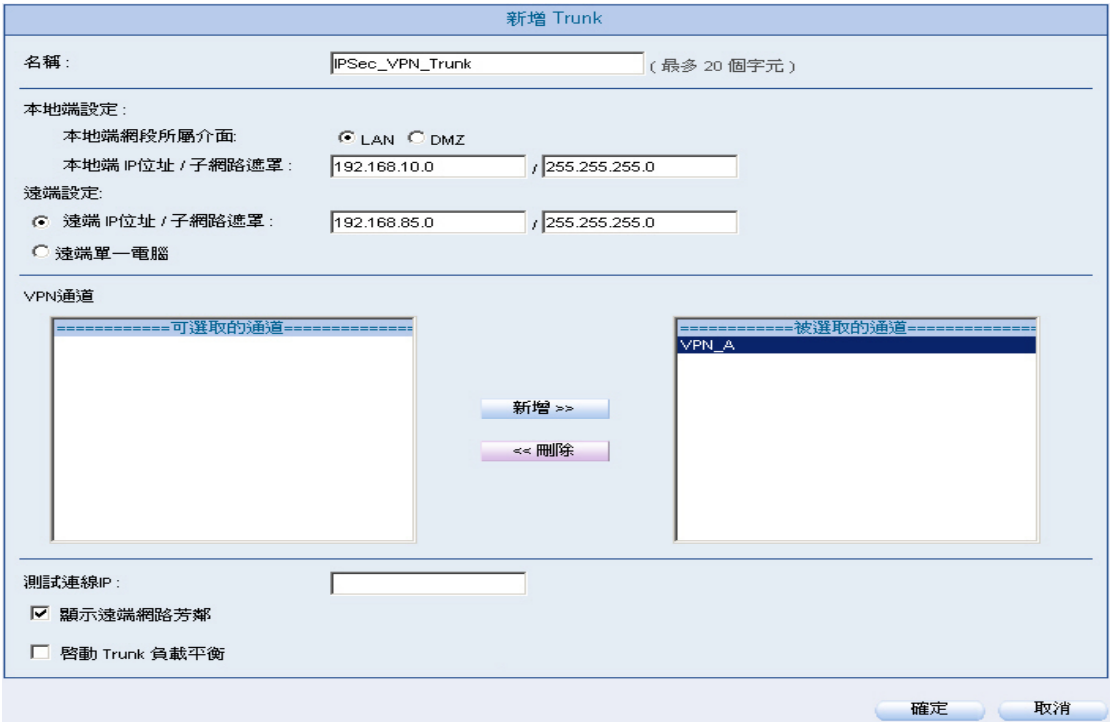


圖 11-26 設定 Trunk

圖 11-27 完成 Trunk 設定

步驟10. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-28）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-29）

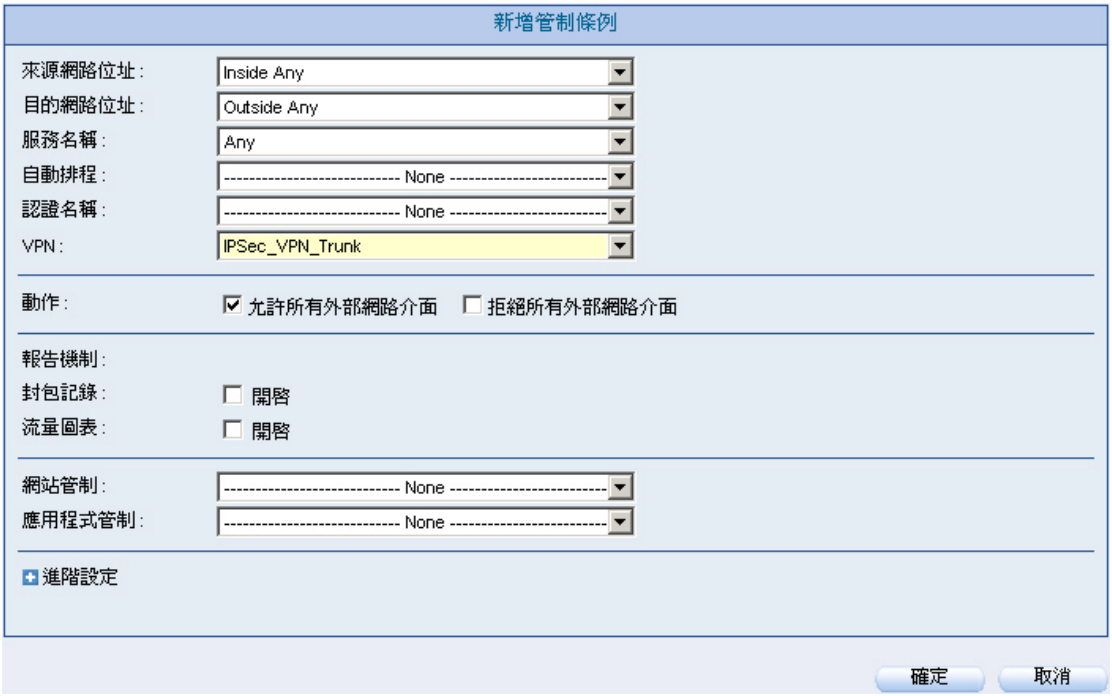


圖 11-28 設定 VPN Trunk 內部至外部之管制條例

圖 11-29 完成管制條例設定

步驟11. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-30）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-31）

圖 11-30 設定 VPN Trunk 外部至內部之管制條例

圖 11-31 完成管制條例設定

說明：

1. 若【遠端設定】選擇遠端閘道 / 用戶端 採用動態 IP 位址，則【使用模式】需採用 Aggressive mode 並填入指定的【本地 ID】、【遠端 ID】，讓遠端（【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱）能以相映的設定，主動來建立正確的連線。

乙公司的設定步驟如下：

步驟1. 在【系統管理】>【組態】>【多重網段】頁面中，做下列設定：（如圖 11-32）

圖 11-32 多重網段設定

步驟2. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 11-33）

圖 11-33IPSec 自動加密頁面

步驟3. 【名稱】輸入 VPN_B、【連線介面】選擇 Port2（WAN1）。（如圖 11-34）

圖 11-34 設定 IPSec 名稱和外部網路介面

步驟4. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的甲公司閘道位址。（如圖 11-35）

圖 11-35 設定 IPSec 到目的位址

步驟5. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-36）

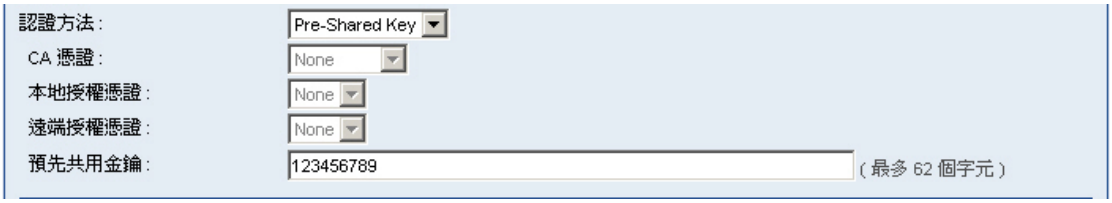


圖 11-36 設定 IPSec 認證方法

步驟6. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-37）

圖 11-37 設定 ISAKMP 演算法

步驟7. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-38）

圖 11-38 設定 IPSec 演算法

步驟8. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-39）

圖 11-39 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟9. 完成 IPSec 自動加密設定。（如圖 11-40）

圖 11-40 完成 IPSec 自動加密設定

步驟10. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-41）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入乙公司的子網路 192.168.85.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 將【可選取的通道】VPN_B 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-42）

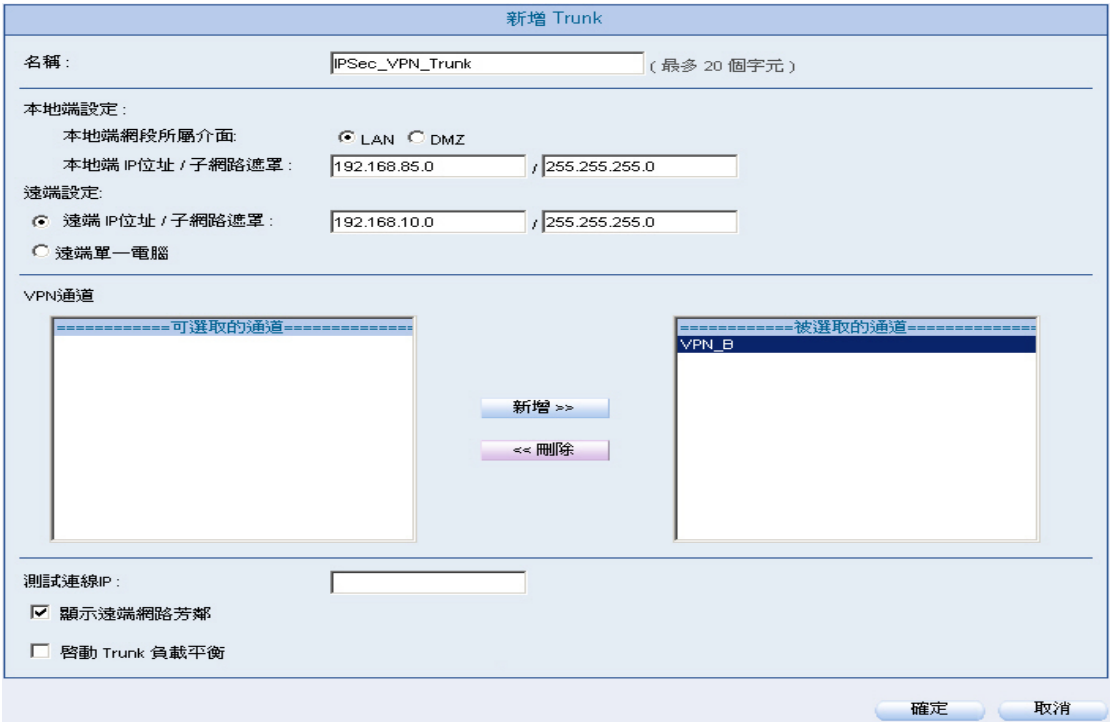


圖 11-41 設定 Trunk

圖 11-42 完成 Trunk 設定

步驟11. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-43）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-44）

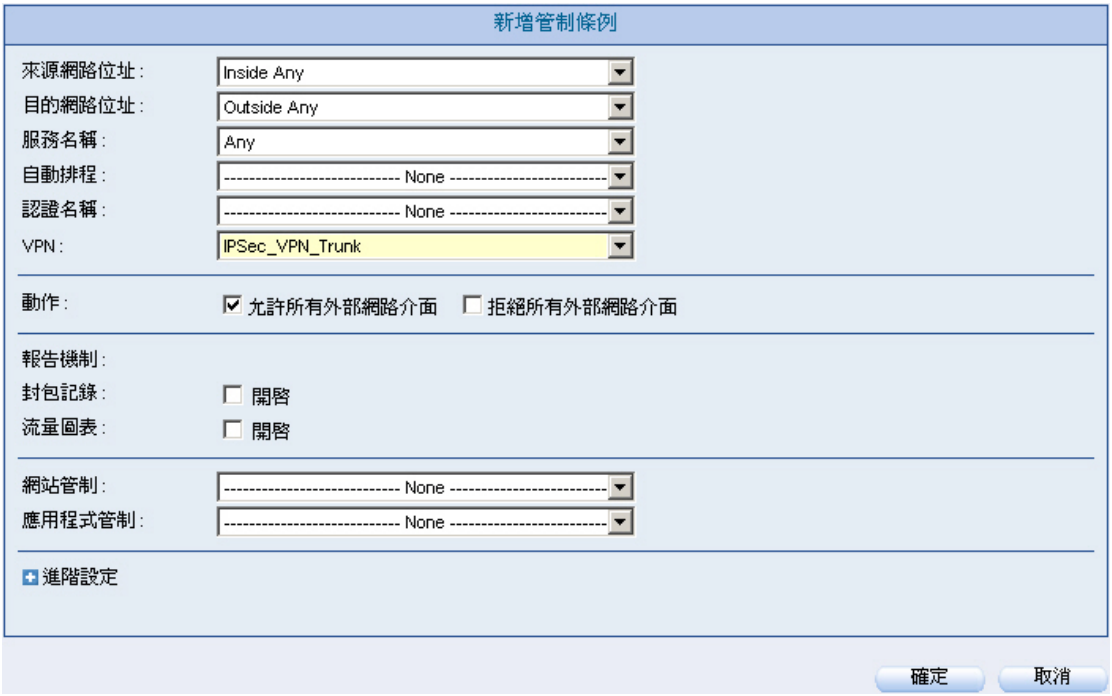


圖 11-43 設定 VPN Trunk 內部至外部之管制條例

圖 11-44 完成管制條例設定

步驟12. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-45）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-46）

圖 11-45 設定 VPN Trunk 外部至內部之管制條例

圖 11-46 完成管制條例設定

步驟13. 完成 IPSec VPN 連線。（如圖 11-47）

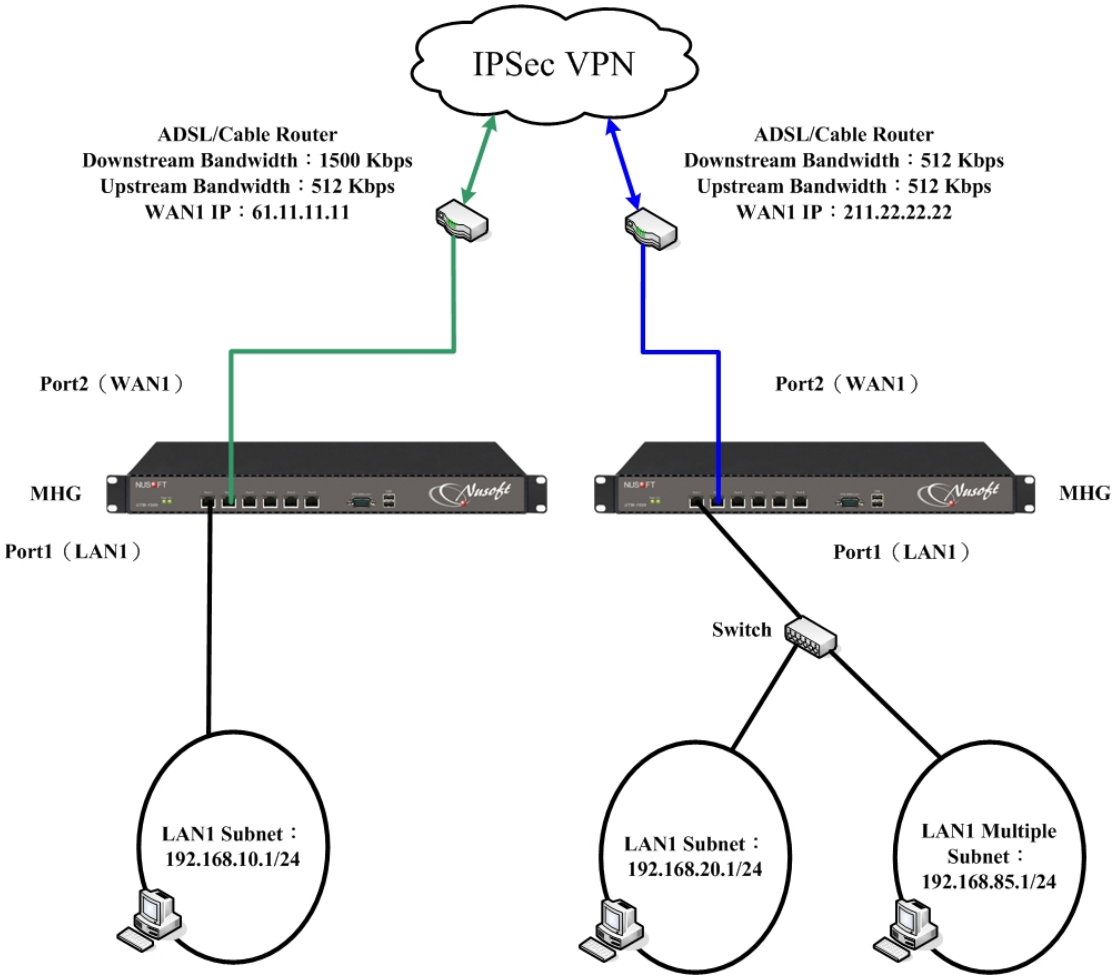


圖 11-47IPSec VPN 連線環境

11.1.2 使用一台 MHG-2000 與 Windows 7 設定 IPSec VPN 連線的方法

環境設定

甲公司使用 MHG-2000。

Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

乙公司使用以 Windows 7 作業之單一 PC，IP 位址為 211.22.22.22。

本範例以一台 MHG-2000 及 Windows 7 作業的 PC 做為平台操作，甲公司和乙公司建立 VPN（虛擬私人網路）連線以傳送資料。

甲公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。**（如圖 11-48）**

圖 11-48 IPSec 自動加密頁面

步驟2. 【名稱】輸入 VPN_A、【連線介面】選擇 Port2（WAN1）。**（如圖 11-49）**

圖 11-49 設定 IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 / 用戶端 採用動態 IP 位址。**（如圖 11-50）**

圖 11-50 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-51）

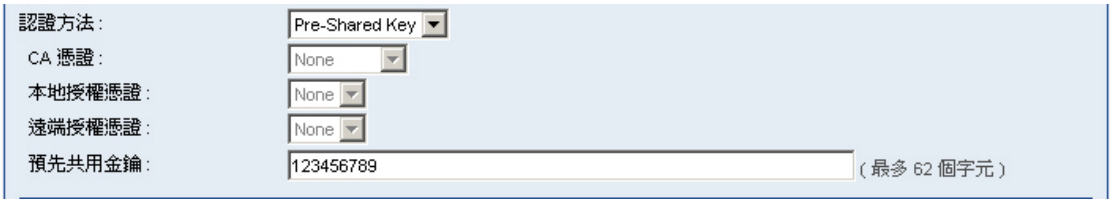


圖 11-51 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 2。（如圖 11-52）

圖 11-52 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-53）

圖 11-53 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-54）

圖 11-54 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟8. 完成 IPSec 自動加密設定。（如圖 11-55）

圖 11-55 完成 IPSec 自動加密設定

步驟9. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-56）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 【遠端設定】選擇遠端單一電腦。
- 將【可選取的通道】VPN_A 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-57）

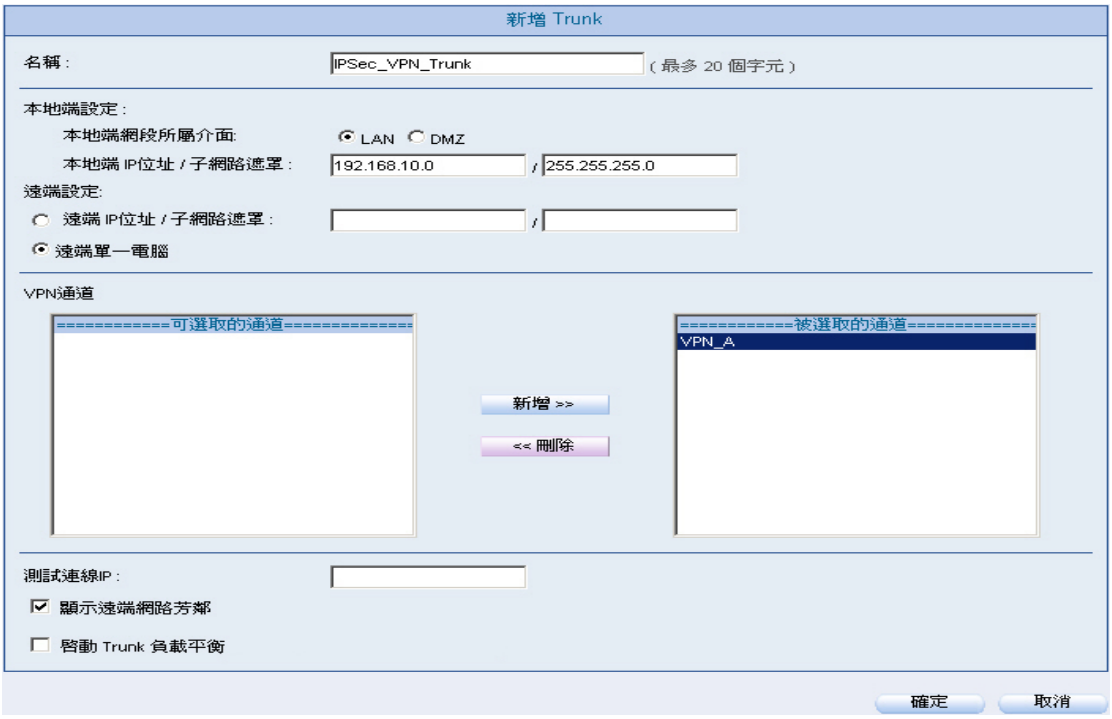


圖 11-56 設定 Trunk

圖 11-57 完成 Trunk 設定

步驟10. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-58）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-59）

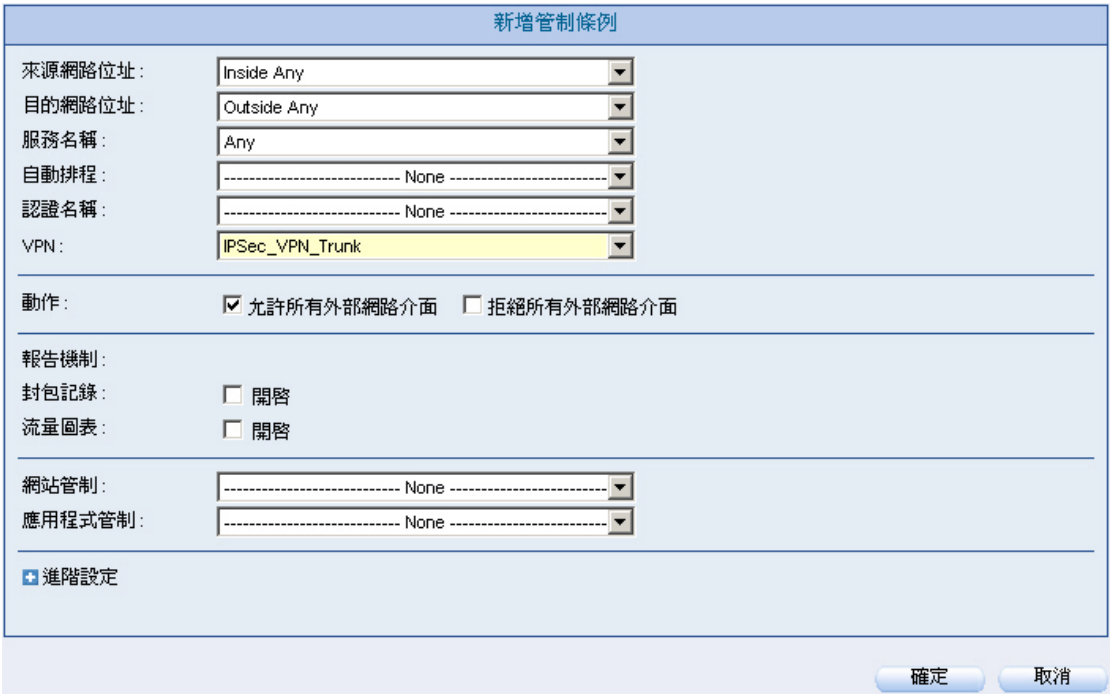


圖 11-58 設定 VPN Trunk 內部至外部之管制條例

圖 11-59 完成管制條例設定

步驟11. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-60）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-61）

圖 11-60 設定 VPN Trunk 外部至內部之管制條例

圖 11-61 完成管制條例設定

乙公司的設定步驟如下：

步驟1. 在【開始】>【執行】視窗中，【開啟】mmc（Micorsoft Management Console）並做下列設定：（如圖 11-62, 圖 11-63）

- 點選【檔案】>【新增/移除嵌入式管理單元】功能。（如圖 11-64）
- 在【新增或移除嵌入式管理單元】視窗中：
  - 將【可用的嵌入式管理單元】IP 安全性原則管理新增至【選取的嵌入式管理單元】清單中：（如圖 11-65）
    - 在【選取電腦或網域】視窗中，選擇【本機電腦】並按下【完成】鈕。（如圖 11-66）
  - 按下【確定】鈕，完成設定。（如圖 11-67）
- 在【主控台根目錄】>【IP 安全性原則（位置：本機電腦）】項目上，按下滑鼠右鍵並選擇【建立 IP 安全性原則】。（如圖 11-68）
- 在【IP 安全性原則精靈】視窗中：
  - 按【下一步】鈕。（如圖 11-69）
  - 【名稱】輸入 VPN_B。
  - 按【下一步】鈕。（如圖 11-70）
  - 按【下一步】鈕。（如圖 11-71）
  - 勾選【編輯內容】。
  - 按下【完成】鈕。（如圖 11-72）

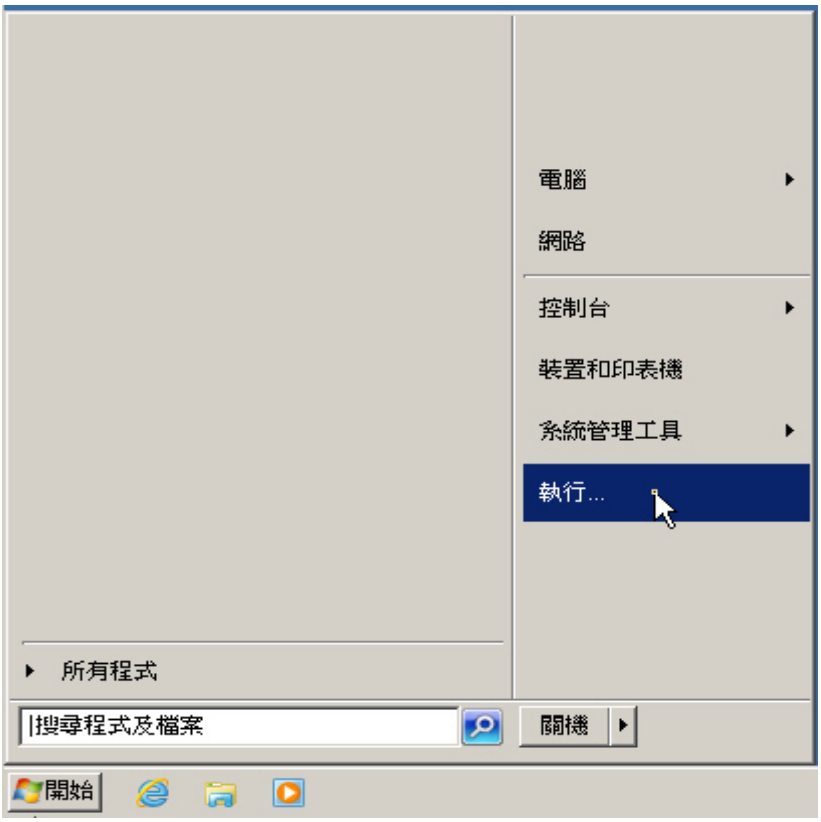


圖 11-62 開啟執行視窗

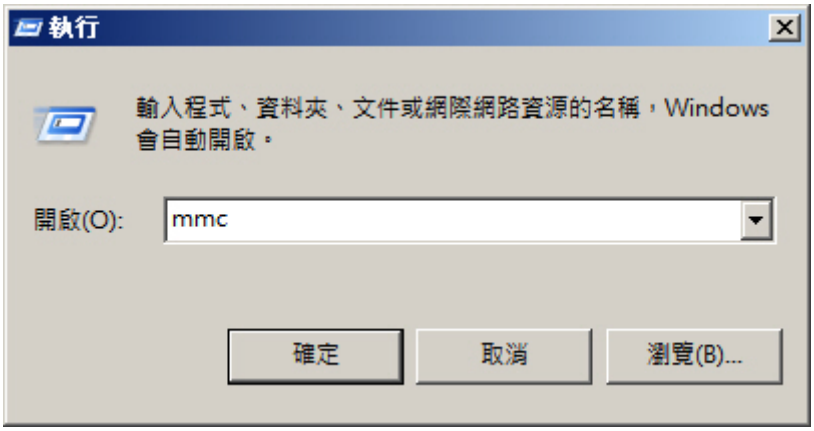


圖 11-63 開啟 Microsoft 管理主控台視窗

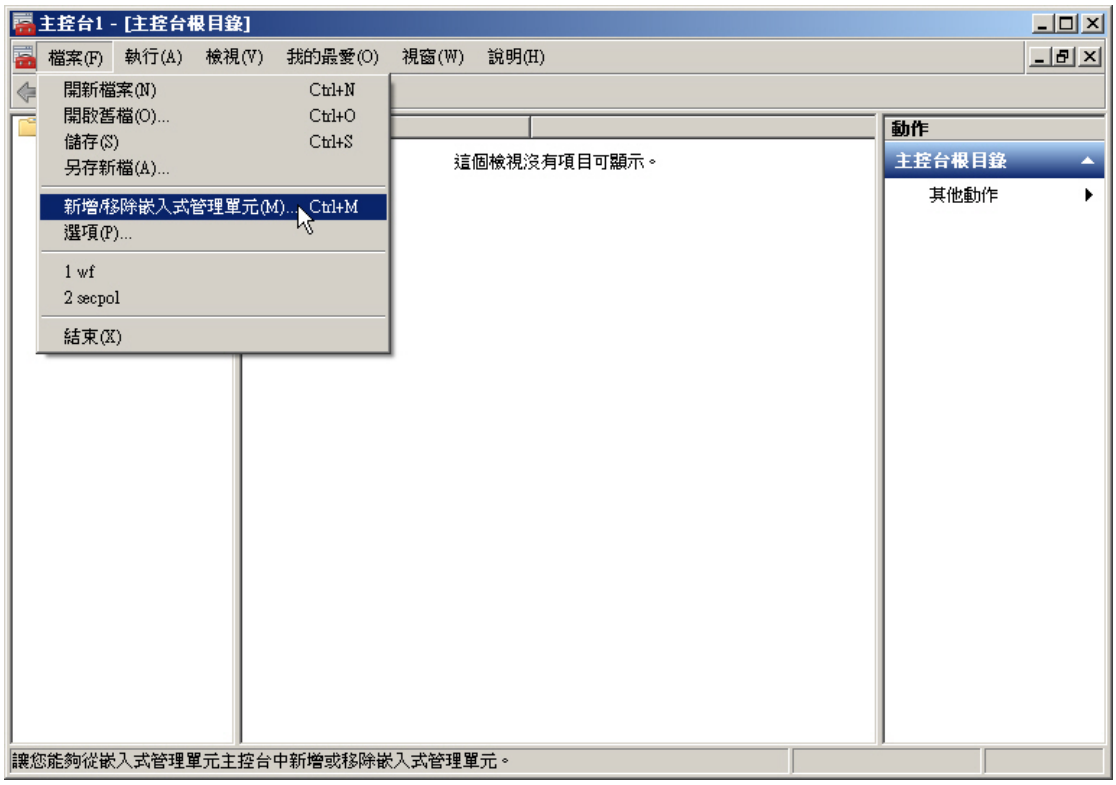


圖 11-64 開啟新增或移除嵌入式管理單元視窗

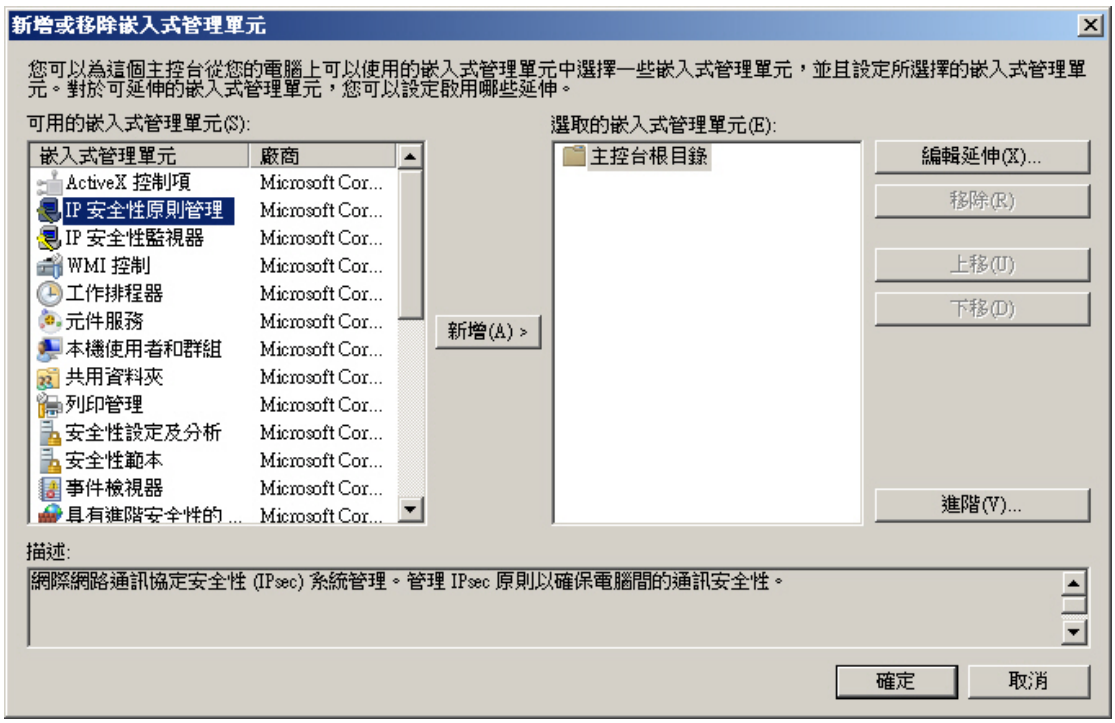


圖 11-65 新增 IP 安全性原則嵌入式管理單元

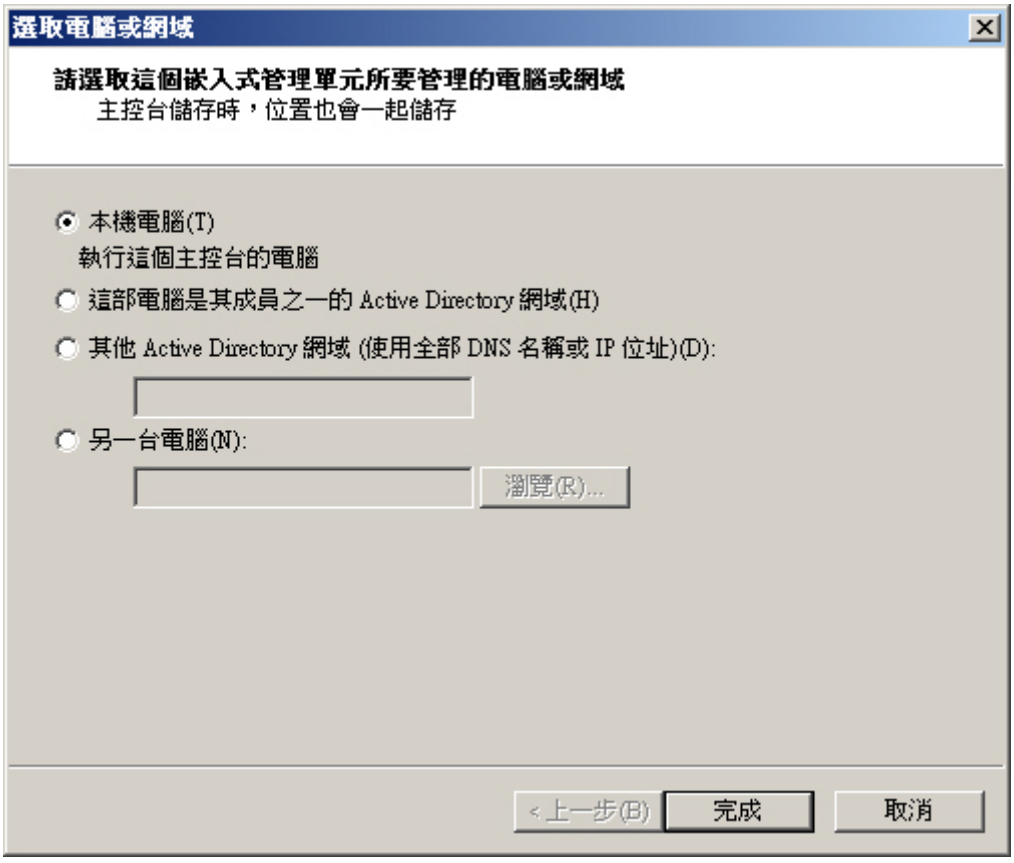


圖 11-66 IP 安全性原則管理的電腦或網域設定

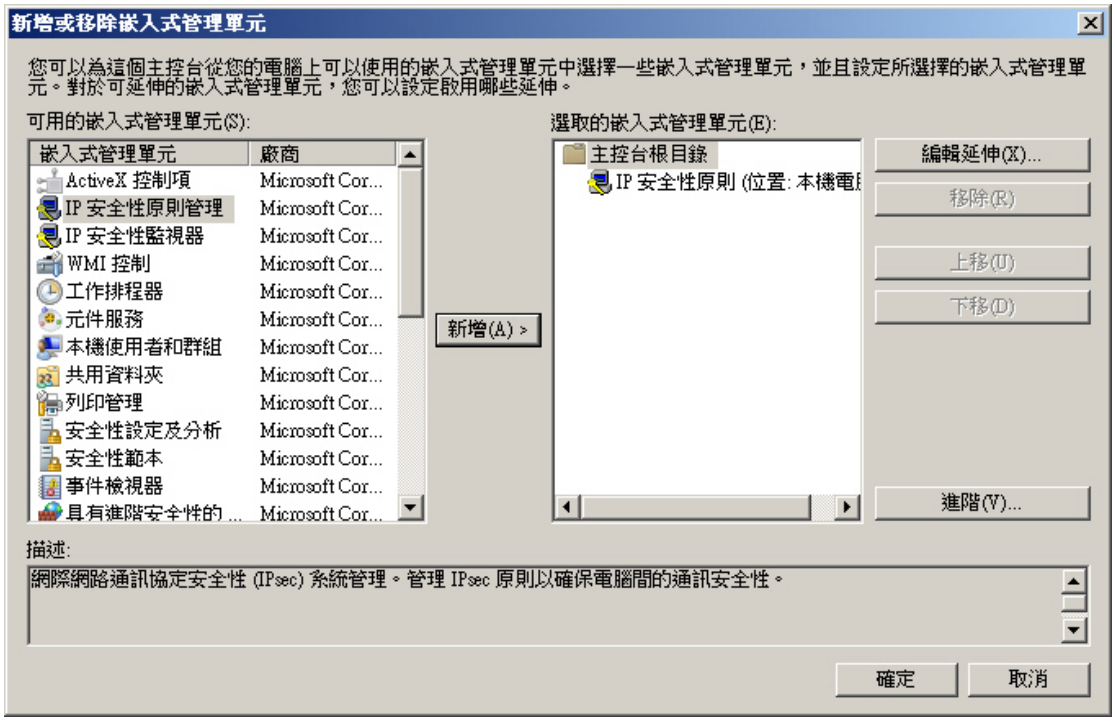


圖 11-67 完成 IP 安全性原則嵌入式管理單元設定

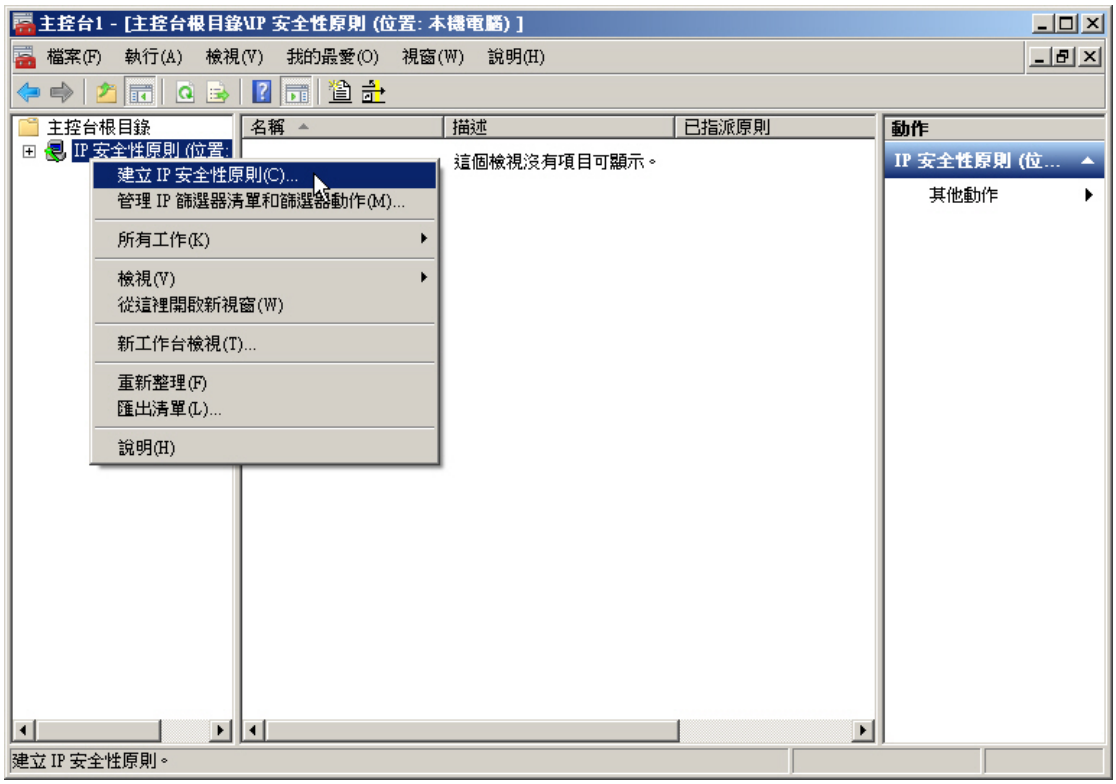


圖 11-68 開啟 IP 安全性原則精靈視窗

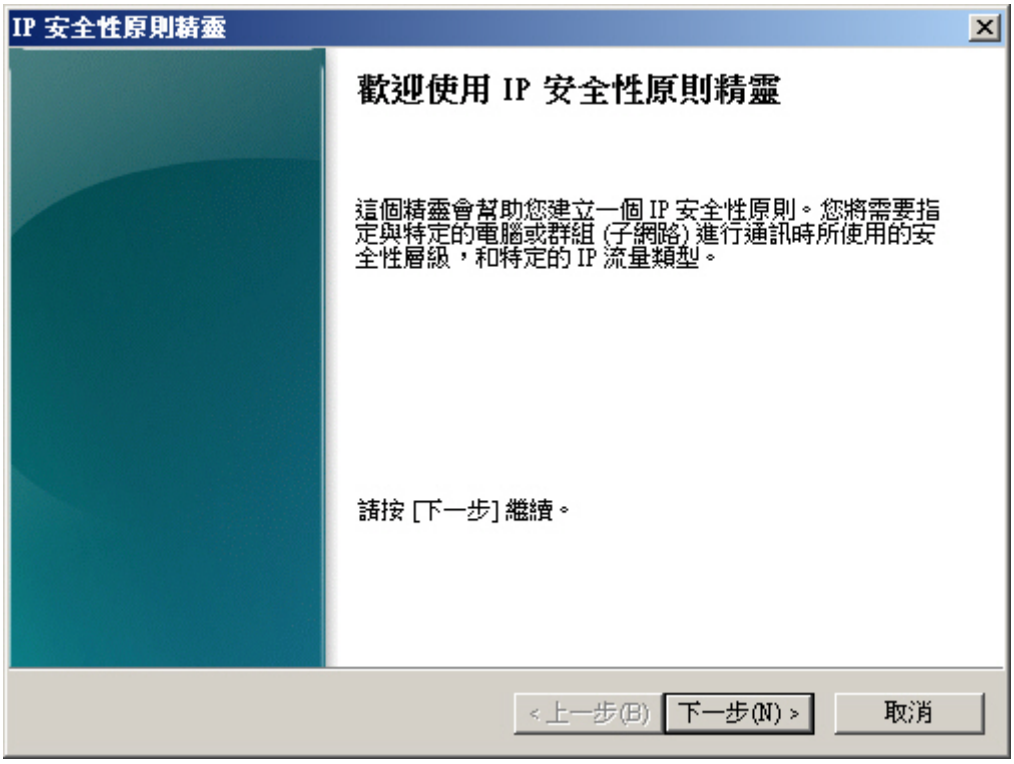


圖 11-69IP 安全性原則精靈歡迎訊息

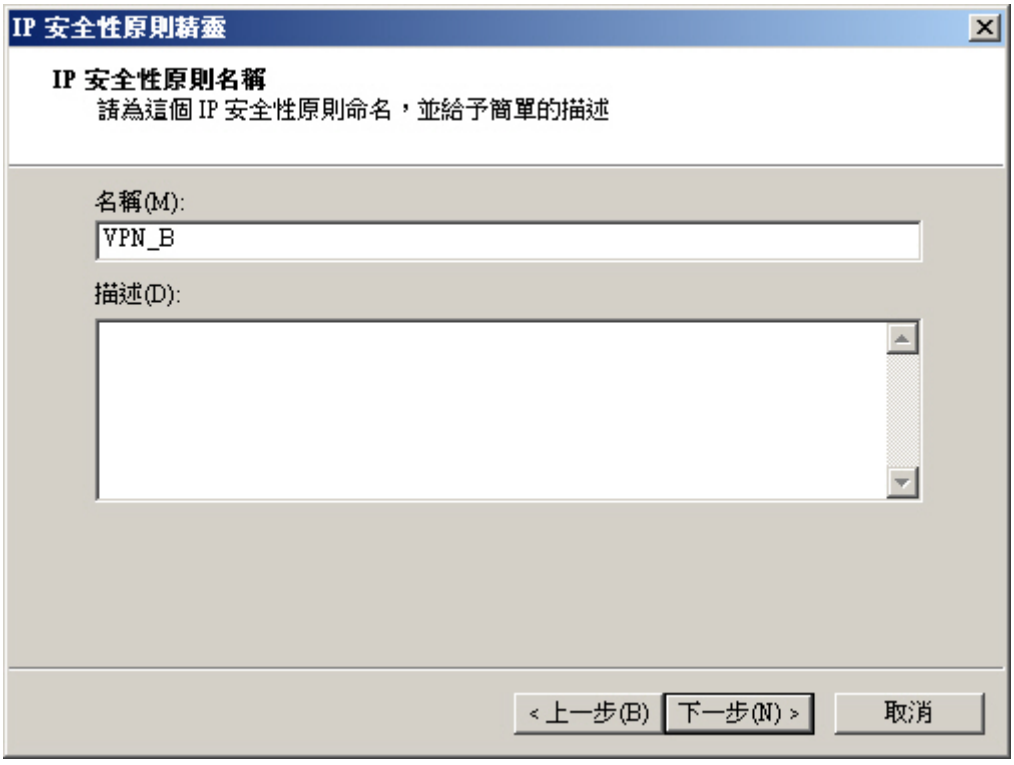


圖 11-70IP 安全性原則名稱設定

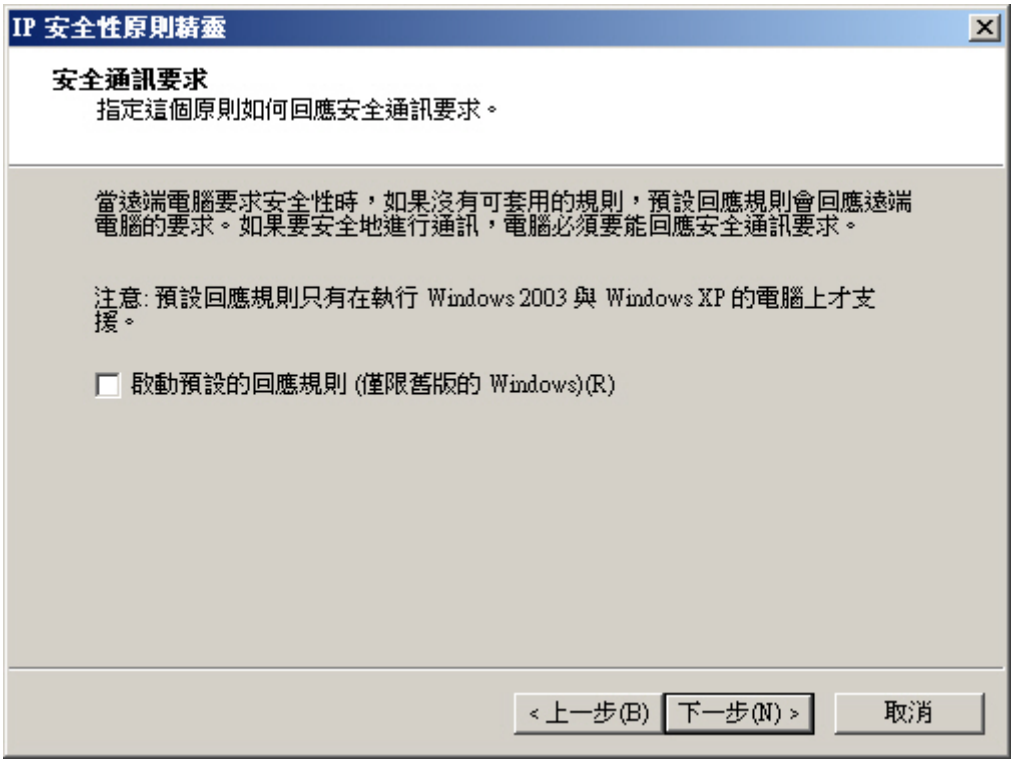


圖 11-71 安全通訊要求設定

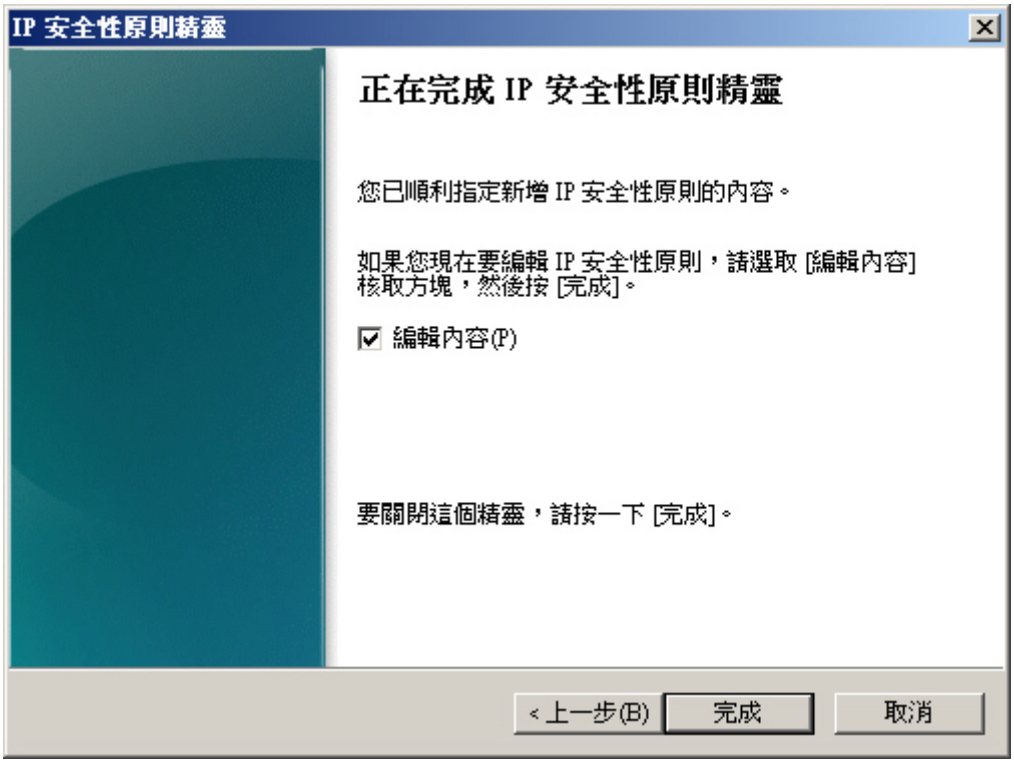


圖 11-72 編輯 IP 安全性原則內容

步驟2. 在【VPN_B-內容】>【規則】視窗中，做下列設定：

- 按下【新增】鈕。（如圖 11-73）
- 在【新增規則-內容】>【IP 篩選器清單】視窗中，按下【新增】鈕：（如圖 11-74）
  - 在【IP 篩選器清單】視窗中，【名稱】輸入 VPN_B Local To Remote 並按下【新增】鈕：（如圖 11-75）
    - 在【IP 篩選器-內容】>【位址】視窗中：（如圖 11-76）
      - 【來源位址】選擇並輸入特定 IP 位址或子網路 211.22.22.22/32。
      - 【目的地位址】選擇並輸入特定 IP 位址或子網路 192.168.10.0/24。
      - 按下【確定】鈕，完成設定。
    - 按下【確定】鈕，完成設定。（如圖 11-77）
  - 【IP 篩選器清單】選擇 VPN_B Local To Remote。（如圖 11-78）
- 在【新增規則-內容】>【篩選器動作】視窗中，按下【新增】鈕：（如圖 11-79）
  - 在【新增篩選器動作-內容】>【安全性方法】視窗中：（如圖 11-80）
    - 選擇【交涉安全性】。
    - 勾選【接受無安全性的通訊，但永遠使用 IPSec 來回應】、【使用工作階段金鑰完全正向加密（PFS）】。
    - 按下【新增】鈕。
    - 在【新增安全性方法】>【安全性方法】視窗中，選擇【自訂】並按下【設定】鈕：（如圖 11-81）
      - 在【自訂安全性方法設定】視窗中：（如圖 11-82）
        - 勾選【資料完整性及加密（ESP）】。
        - 【完整性演算法】選擇 MD5。
        - 【加密演算法】選擇 3DES。
        - 【工作階段金鑰設定】勾選並輸入產生新金鑰間隔 3600 秒。
        - 按下【確定】鈕。
      - 按下【確定】鈕，完成設定。
    - 按下【確定】鈕，完成設定。（如圖 11-83）
  - 【篩選器動作】選擇新增篩選器動作。（如圖 11-84）
- 在【新增規則-內容】>【驗證方法】視窗中，【驗證方法的喜好設定順序】選擇 Kerberos 並按下【編輯】鈕：（如圖 11-85）
  - 在【編輯驗證方法-內容】>【驗證方法】視窗中：（如圖 11-86）
    - 選擇並輸入【使用這個字串（預先共用金鑰）】123456789。
    - 按下【確定】鈕，完成設定。

- ◆ 【驗證方法的喜好設定順序】選擇預先共用金鑰。（如圖 11-87）

■ 在【新增規則-內容】>【通道設定】視窗中：（如圖 11-88）
- ◆ 選擇【通道端點是由下列 IP 位址指定】。
- ◆ 【IPv4 通道端點】輸入 61.11.11.11。

■ 在【新增規則-內容】>【連線類型】視窗中：（如圖 11-89）
- ◆ 選擇【所有網路連線】。
- ◆ 按下【套用】鈕。
- ◆ 按下【確定】鈕，完成設定。

■ 【IP 安全性原則】勾選 VPN_B Local To Remote。（如圖 11-90）

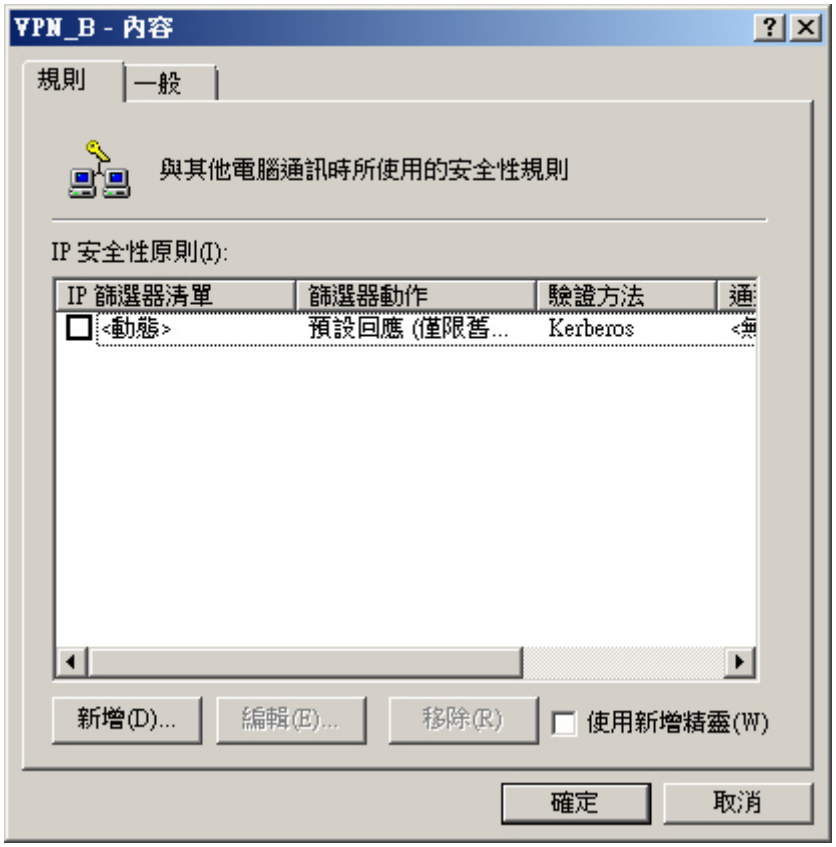


圖 11-73 新增 IP 安全性原則

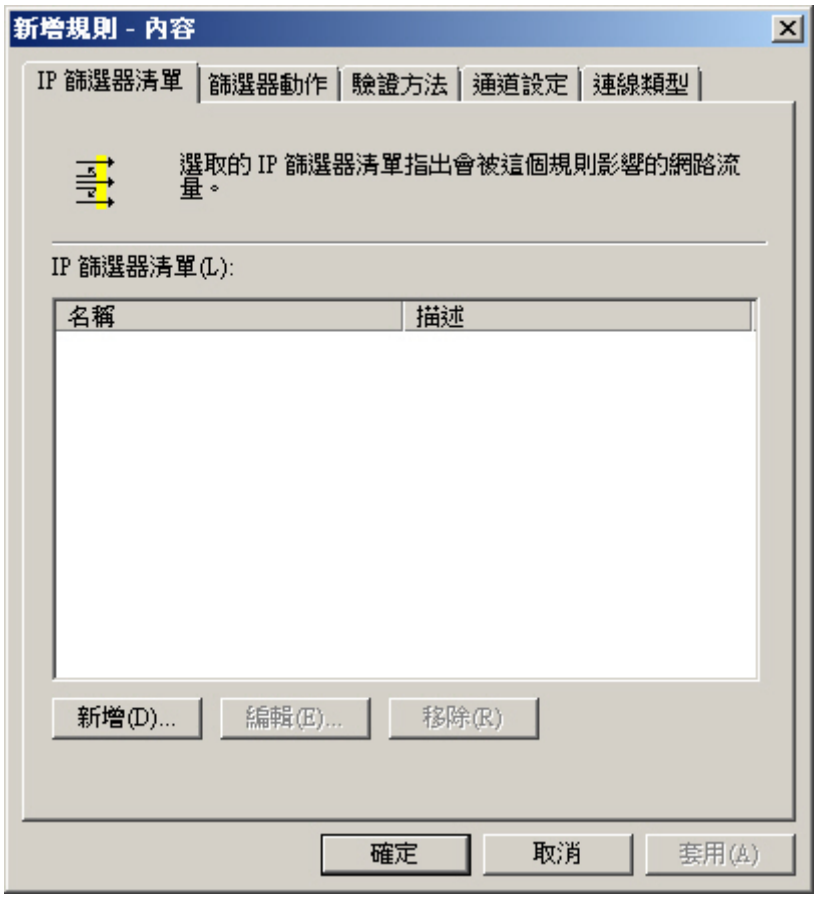


圖 11-74 新增 IP 篩選器清單

圖 11-75 新增 IP 篩選器

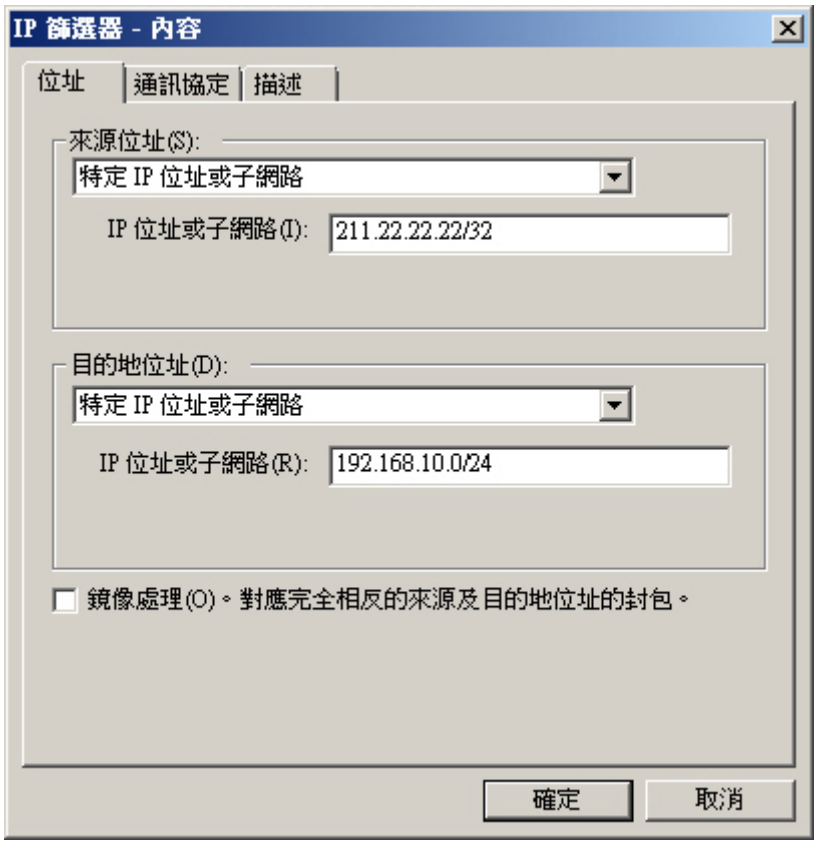


圖 11-76 設定 IP 篩選器

圖 11-77 完成 IP 篩選器設定

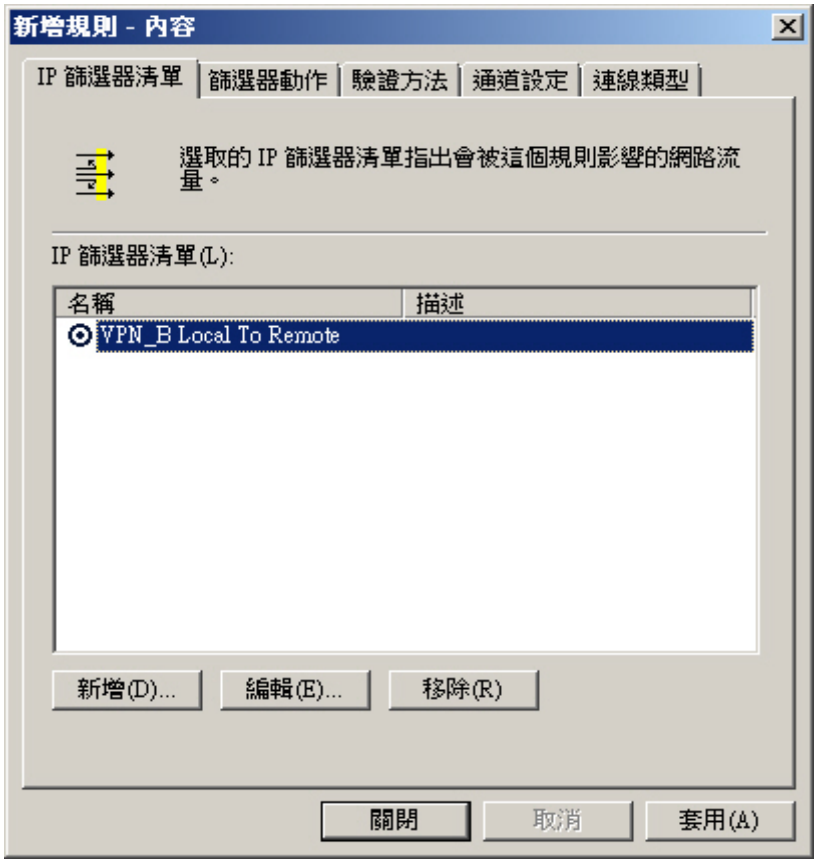


圖 11-78 完成 IP 篩選器清單設定

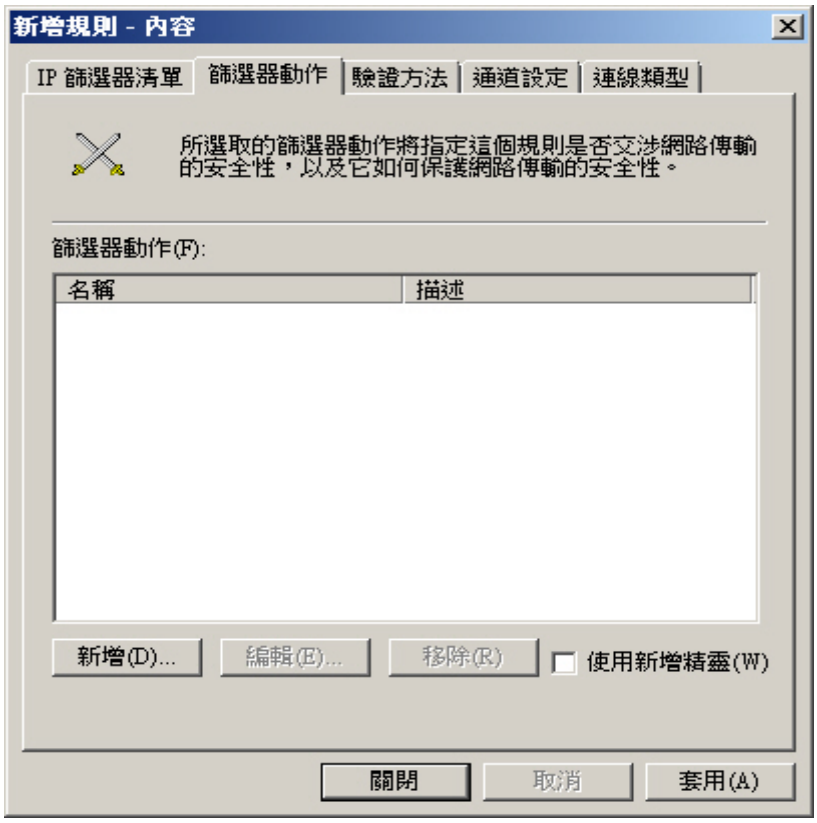


圖 11-79 新增篩選器動作

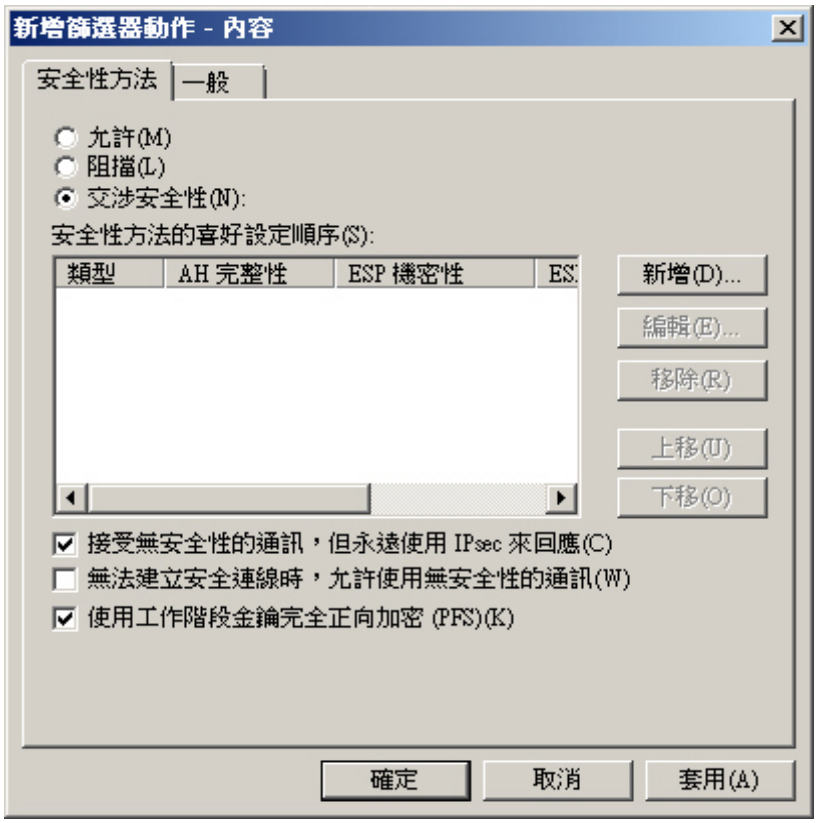


圖 11-80 新增安全性方法

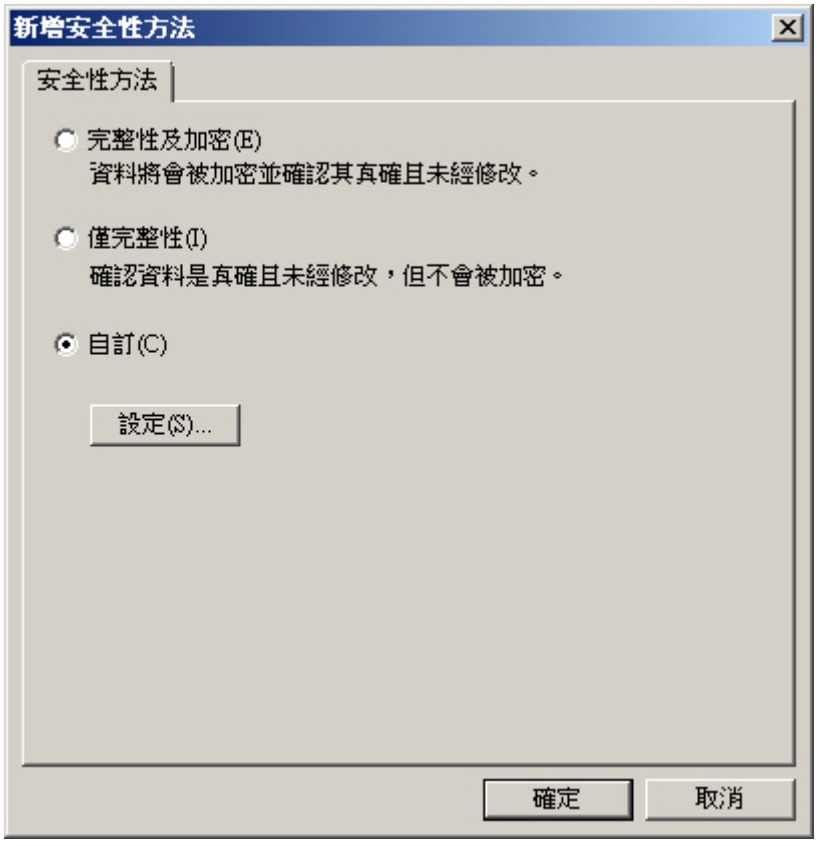


圖 11-81 自訂安全性方法

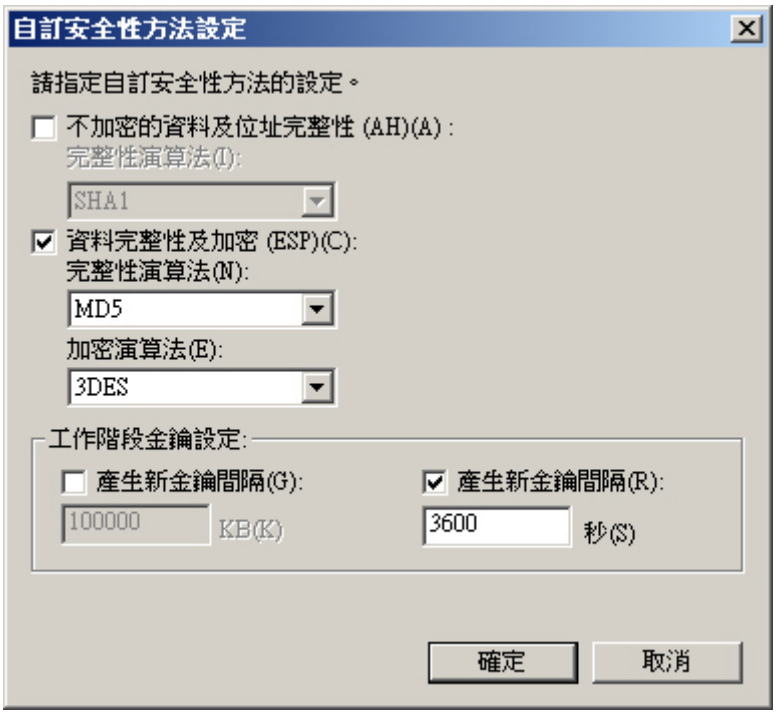


圖 11-82 設定安全性方法

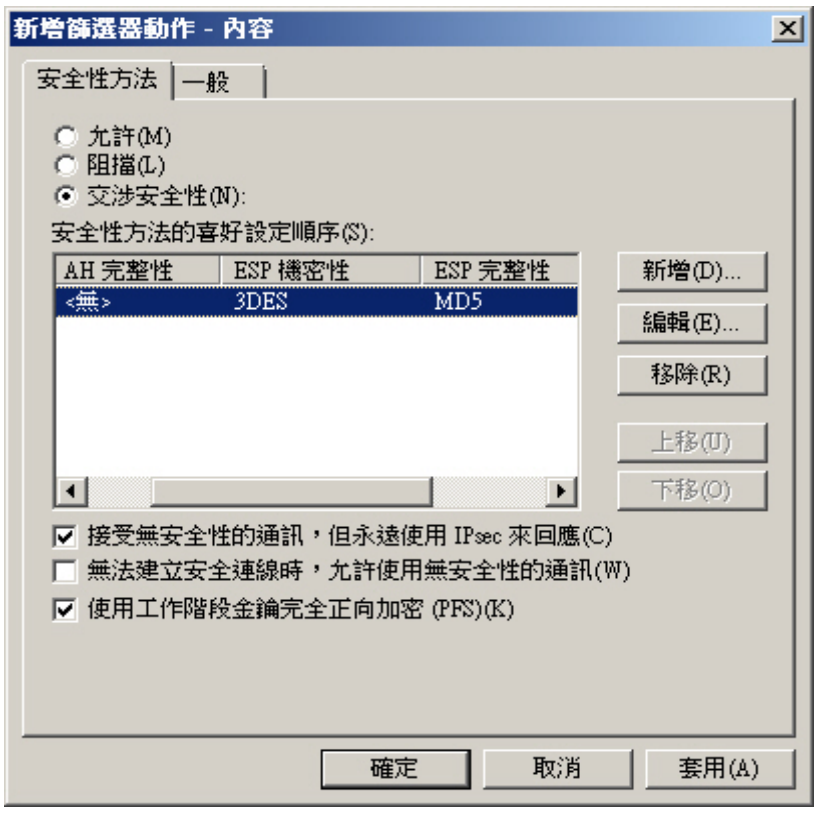


圖 11-83 完成安全性方法設定

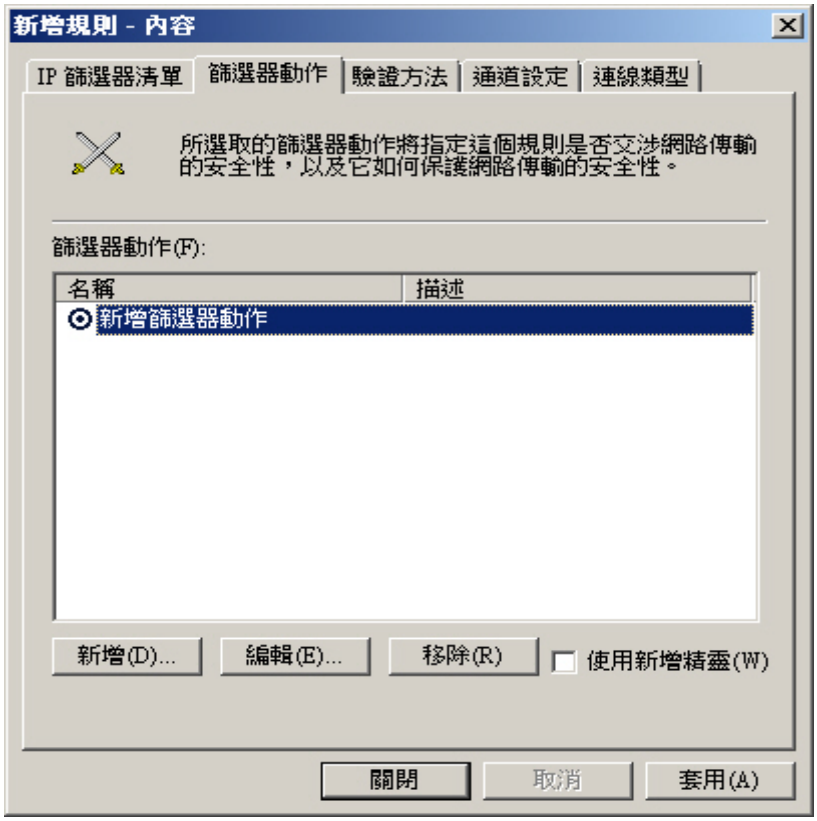


圖 11-84 完成篩選器動作設定

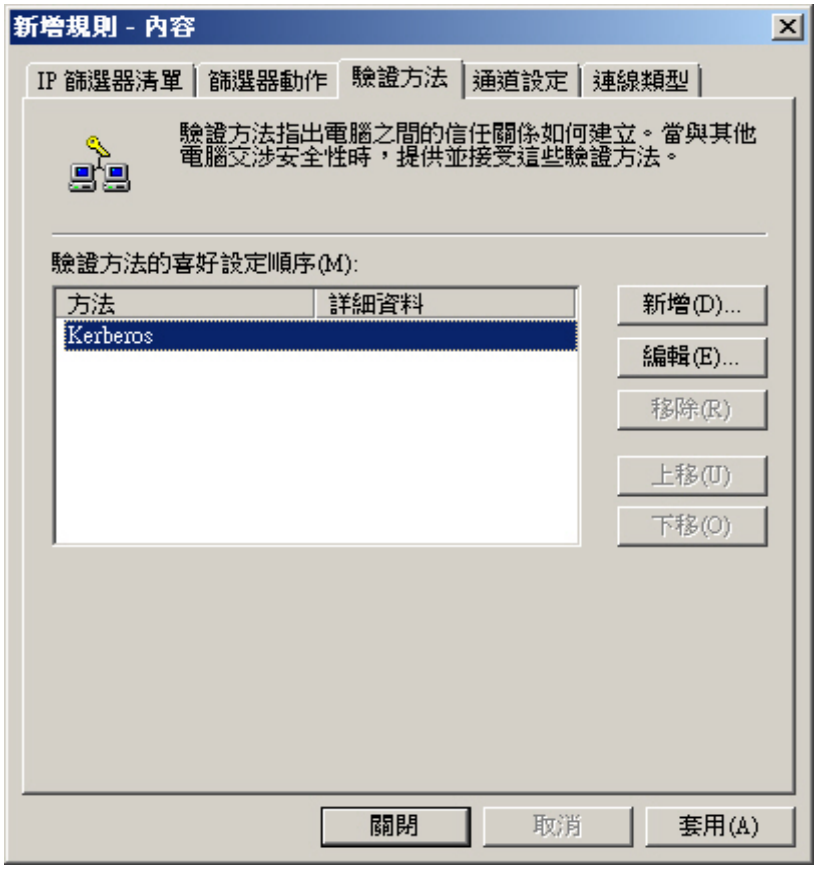


圖 11-85 編輯驗證方法

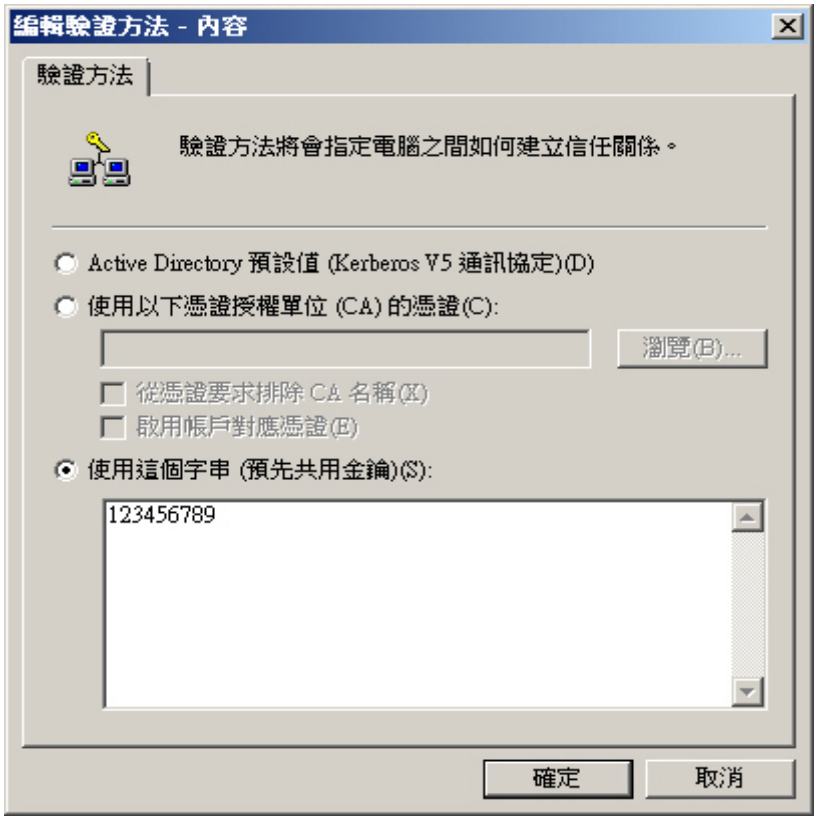


圖 11-86 設定驗證方法

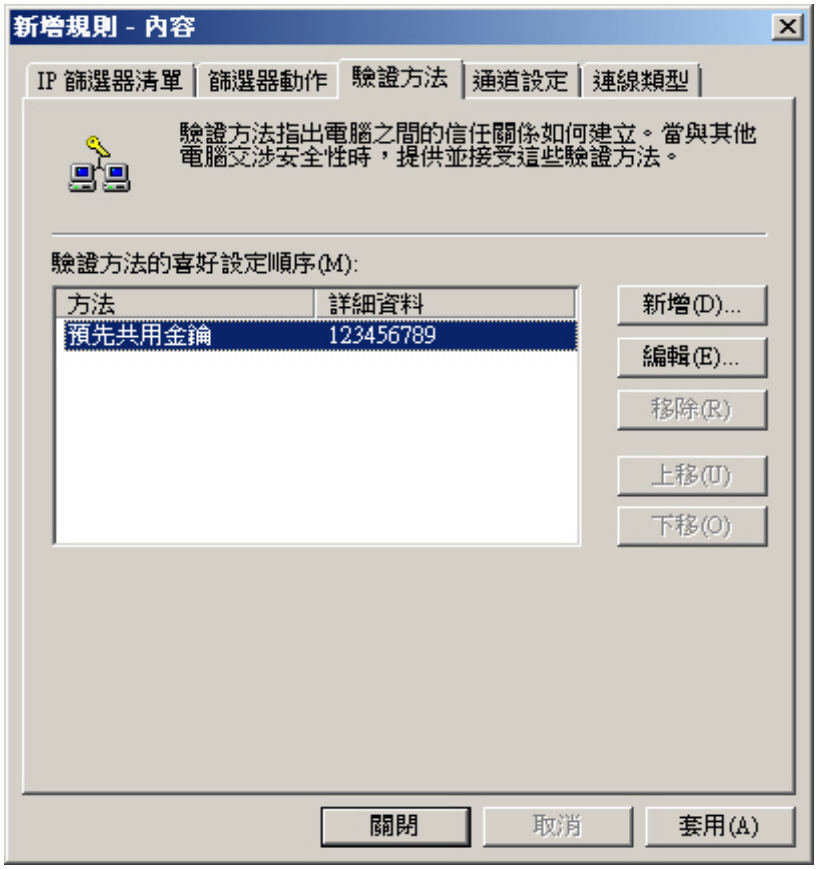


圖 11-87 完成驗證方法設定

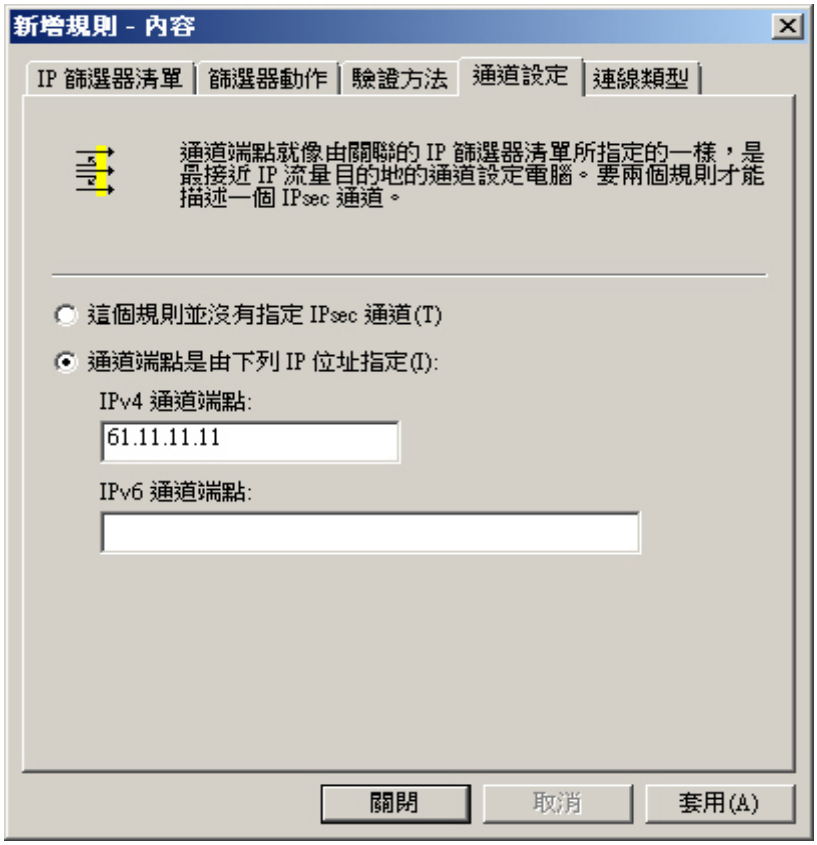


圖 11-88 通道設定

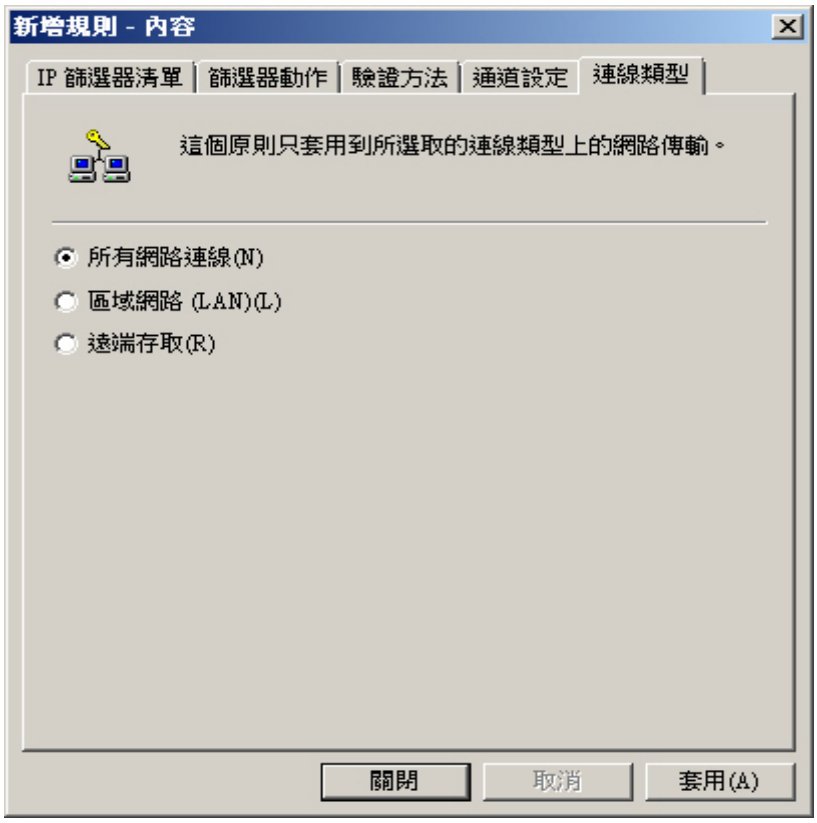


圖 11-89 連線類型設定

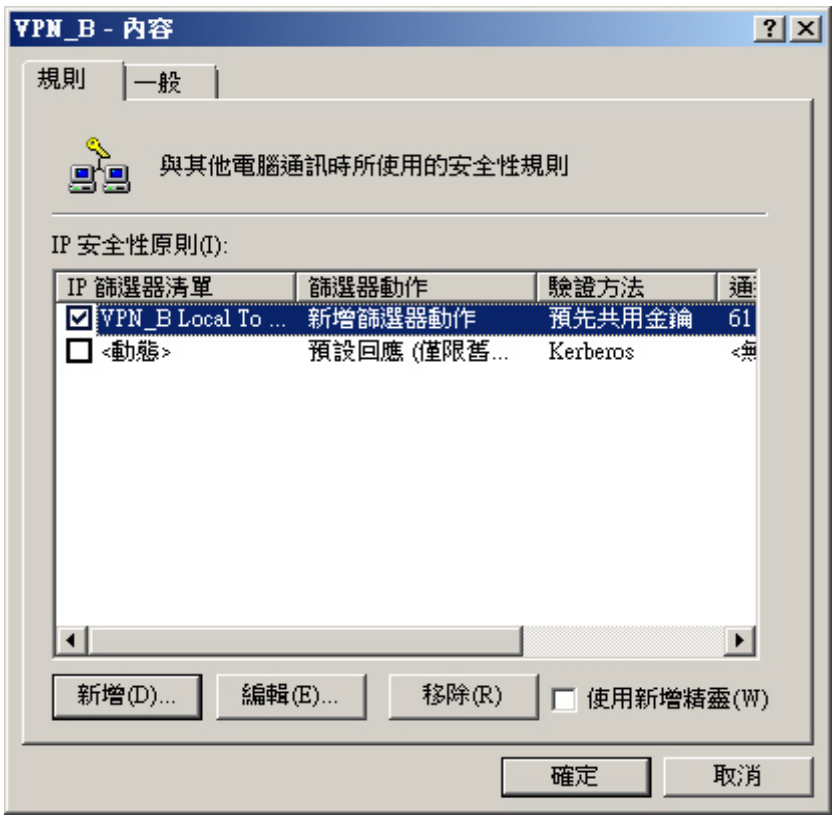


圖 11-90 完成 IP 安全性原則設定

步驟3. 在【VPN_B-內容】>【規則】視窗中，做下列設定：

- 按下【新增】鈕。（如圖 11-91）
- 在【新增規則-內容】>【IP 篩選器清單】視窗中，按下【新增】鈕：（如圖 11-92）
  - 在【IP 篩選器清單】視窗中，【名稱】輸入 VPN_B Remote To Local 並按下【新增】鈕：（如圖 11-93）
    - 在【IP 篩選器-內容】>【位址】視窗中：（如圖 11-94）
      - 【來源位址】選擇並輸入特定 IP 位址或子網路 192.168.10.0/24。
      - 【目的地位址】選擇並輸入特定 IP 位址或子網路 211.22.22.22/32。
      - 按下【確定】鈕，完成設定。
    - 按下【確定】鈕，完成設定。（如圖 11-95）
  - 【IP 篩選器清單】選擇 VPN_B Remote To Local。（如圖 11-96）
- 在【新增規則-內容】>【篩選器動作】視窗中，【篩選器動作】選擇新增篩選器動作。（如圖 11-97）
- 在【新增規則-內容】>【驗證方法】視窗中，【驗證方法的喜好設定順序】選擇 Kerberos 並按下【編輯】鈕：（如圖 11-98）
  - 在【編輯驗證方法-內容】>【驗證方法】視窗中：（如圖 11-99）
    - 選擇並輸入【使用這個字串（預先共用金鑰）】123456789。
    - 按下【確定】鈕，完成設定。
  - 【驗證方法的喜好設定順序】選擇預先共用金鑰。（如圖 11-100）
- 在【新增規則-內容】>【通道設定】視窗中：（如圖 11-101）
  - 選擇【通道端點是由下列 IP 位址指定】。
  - 【IPv4 通道端點】輸入 211.22.22.22。
- 在【新增規則-內容】>【連線類型】視窗中：（如圖 11-102）
  - 選擇【所有網路連線】。
  - 按下【套用】鈕。
  - 按下【確定】鈕，完成設定。
- 【IP 安全性原則】勾選 VPN_B Remote To Local。（如圖 11-103）

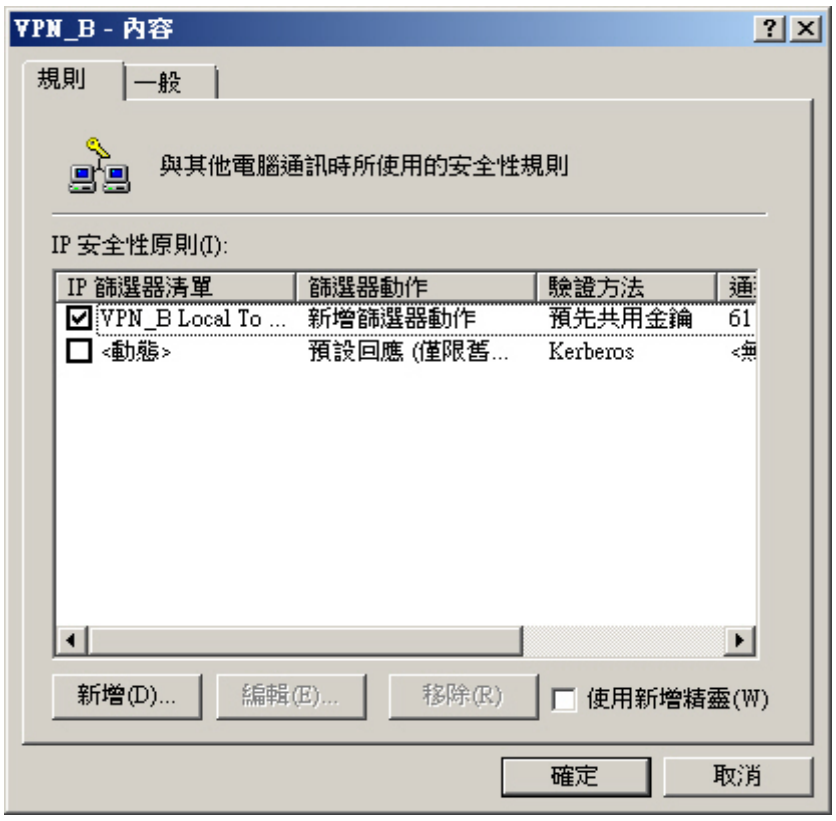


圖 11-91 新增 IP 安全性原則

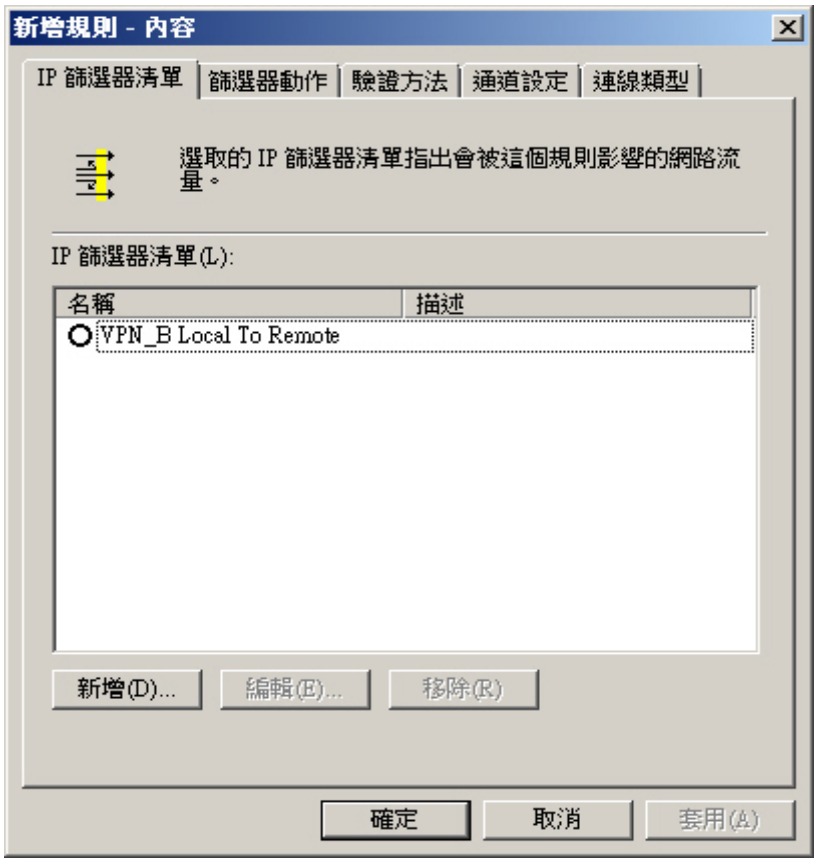


圖 11-92 新增 IP 篩選器清單

圖 11-93 新增 IP 篩選器

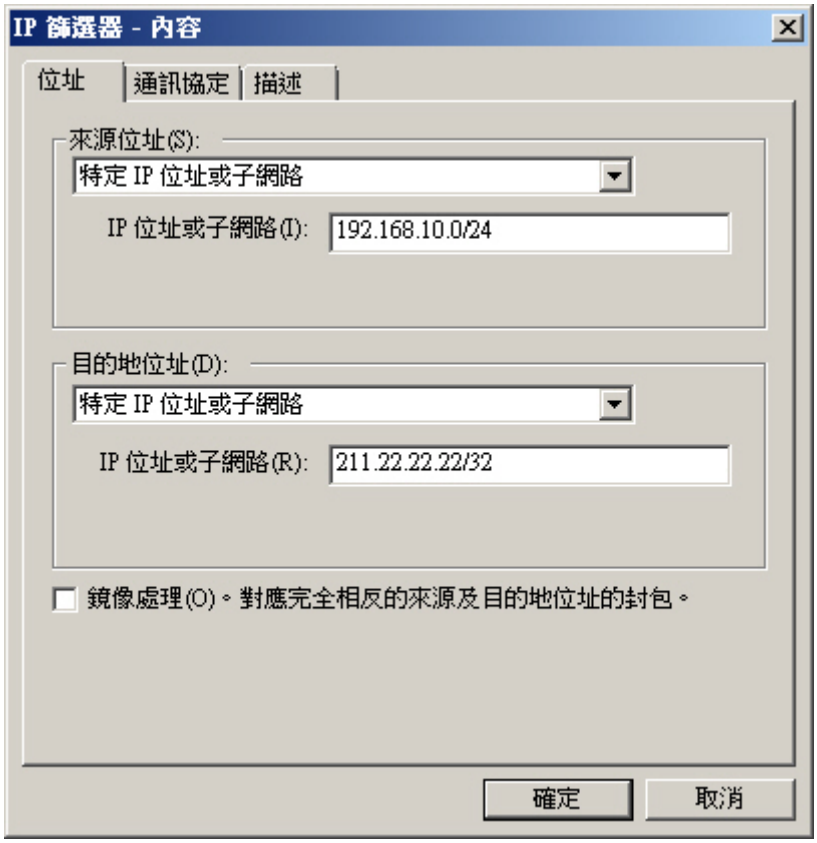


圖 11-94 設定 IP 篩選器

圖 11-95 完成 IP 篩選器設定

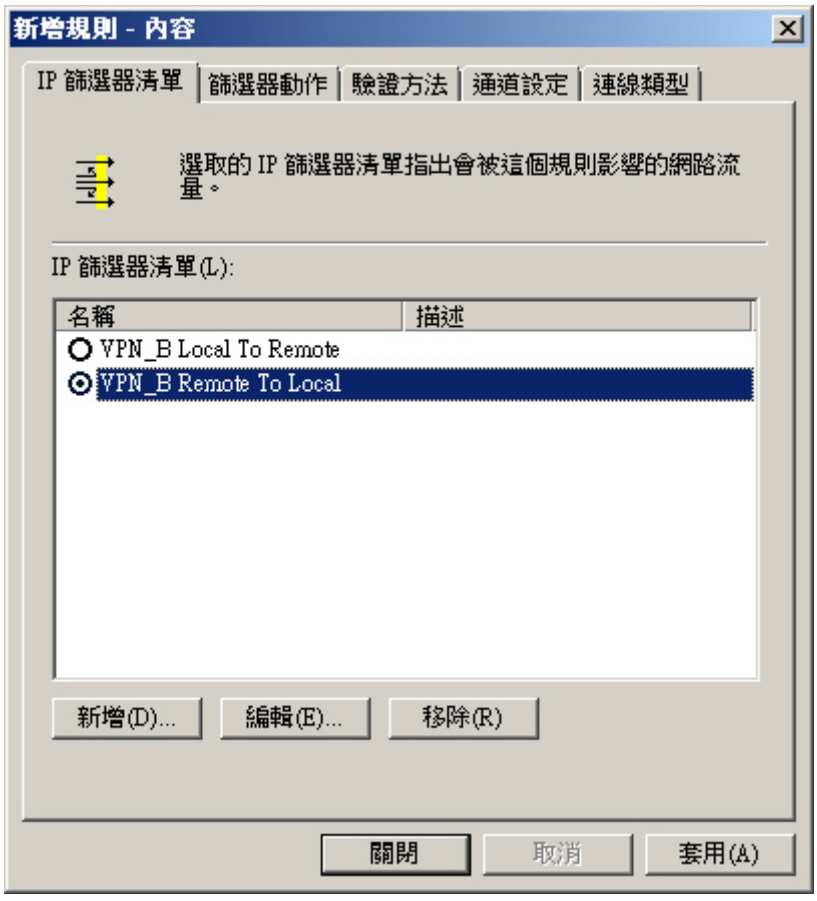


圖 11-96 完成 IP 篩選器清單設定

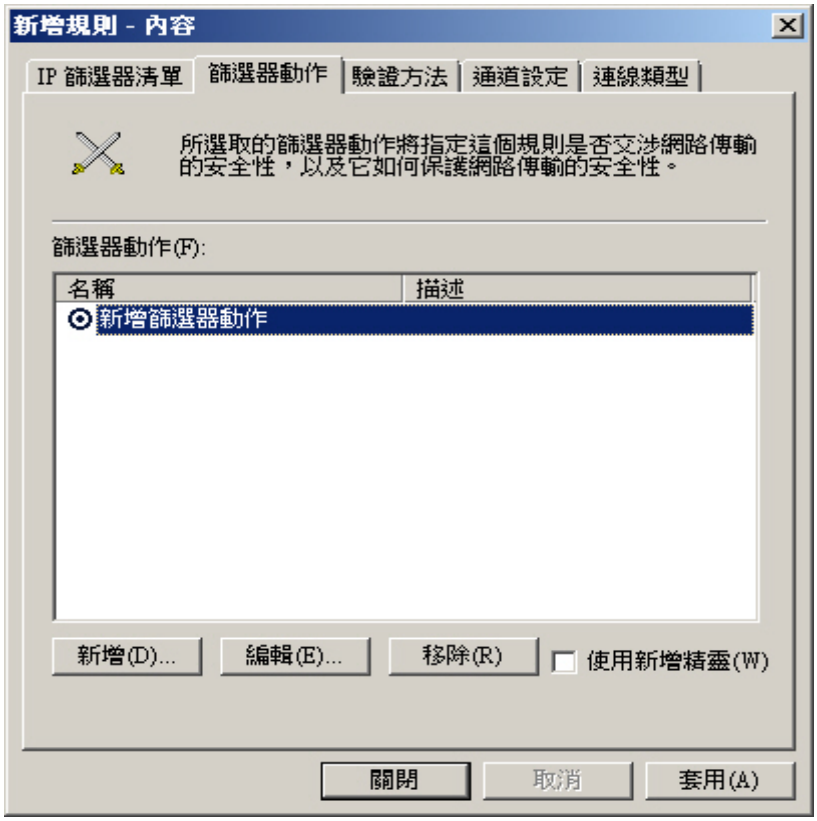


圖 11-97 篩選器動作設定

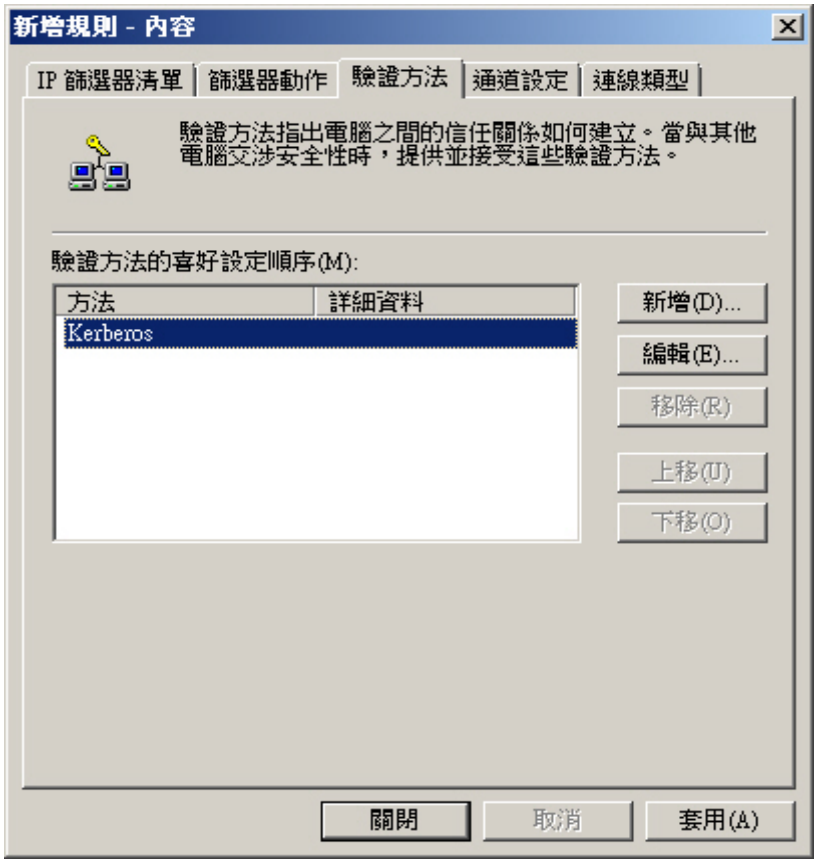


圖 11-98 編輯驗證方法

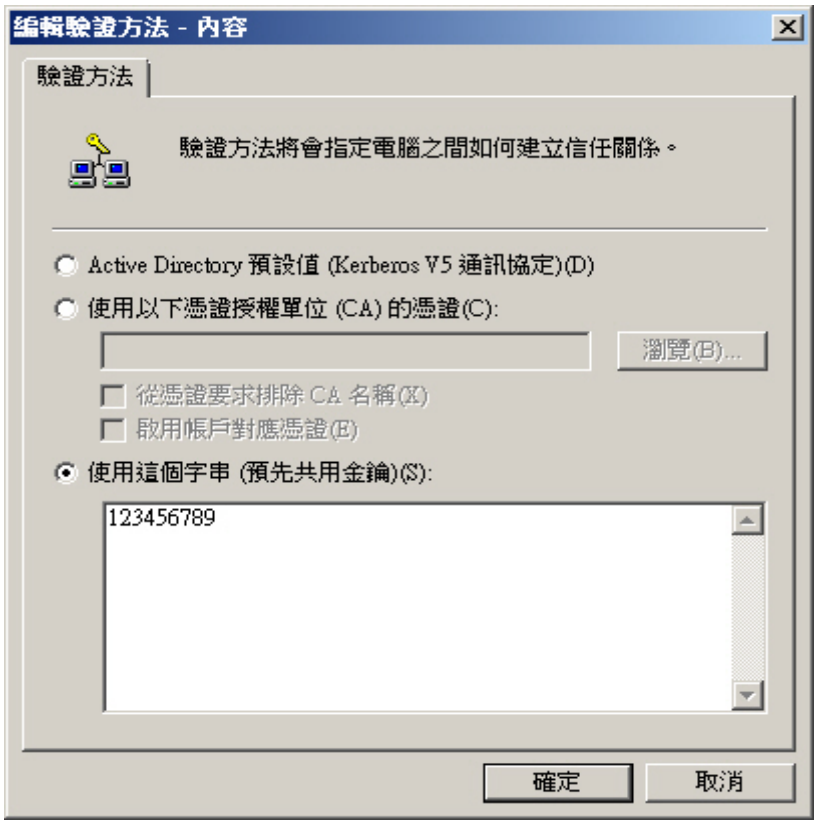


圖 11-99 設定驗證方法

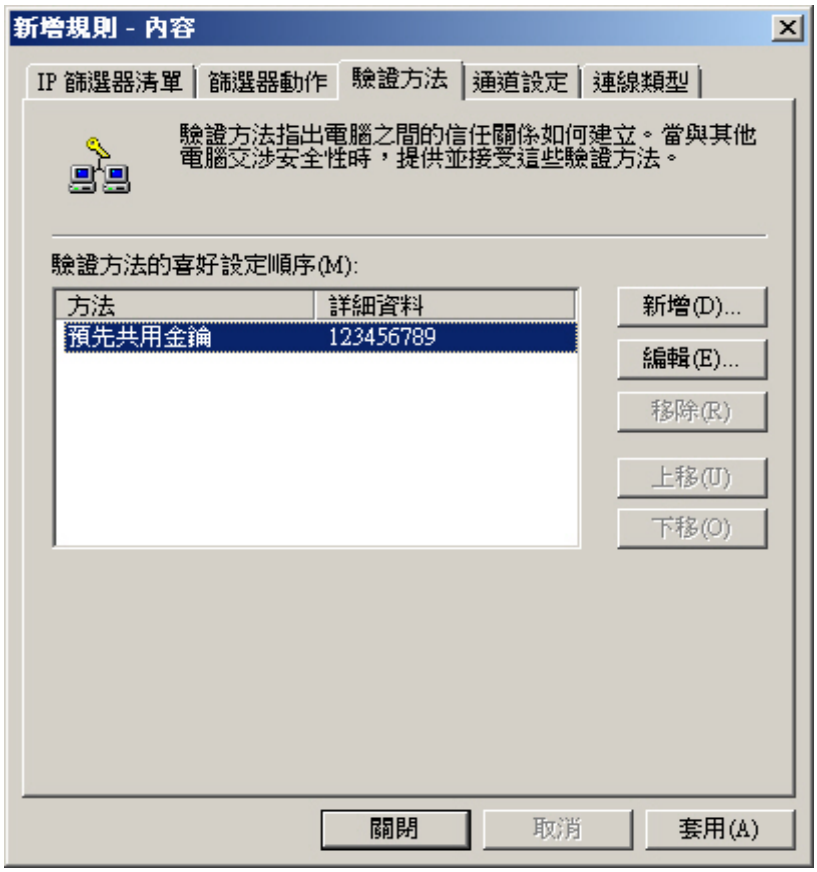


圖 11-100 完成驗證方法設定

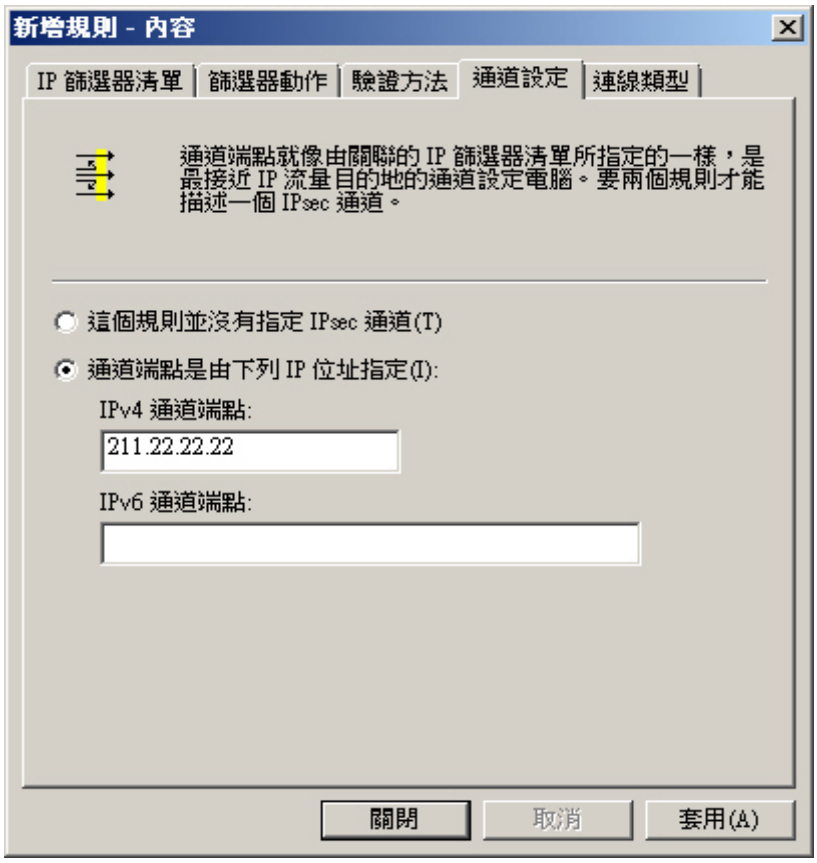


圖 11-101 通道設定

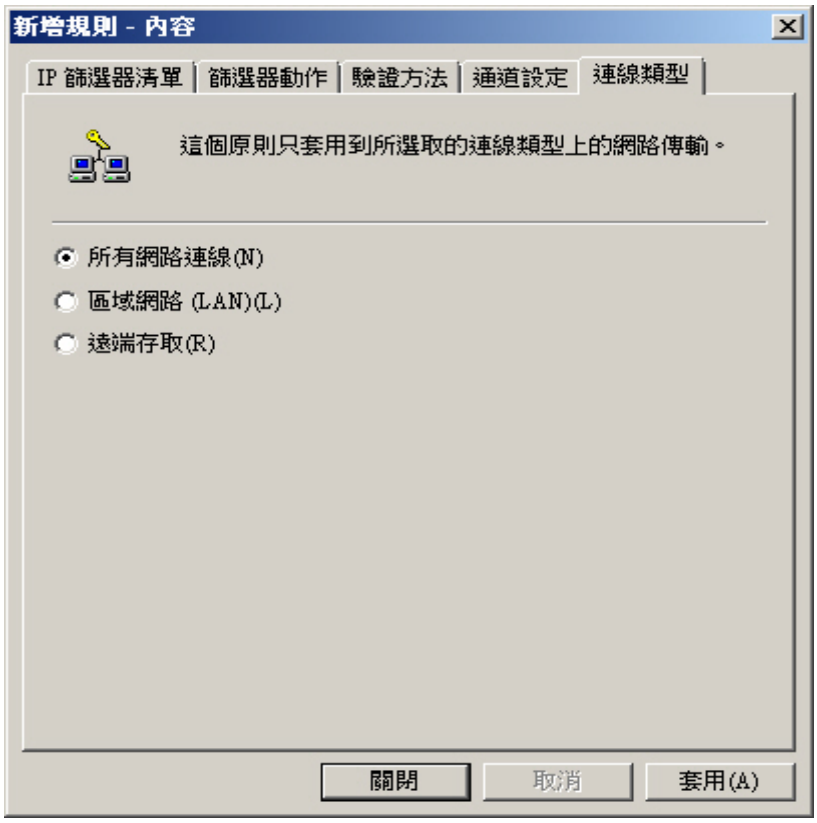


圖 11-102 連線類型設定

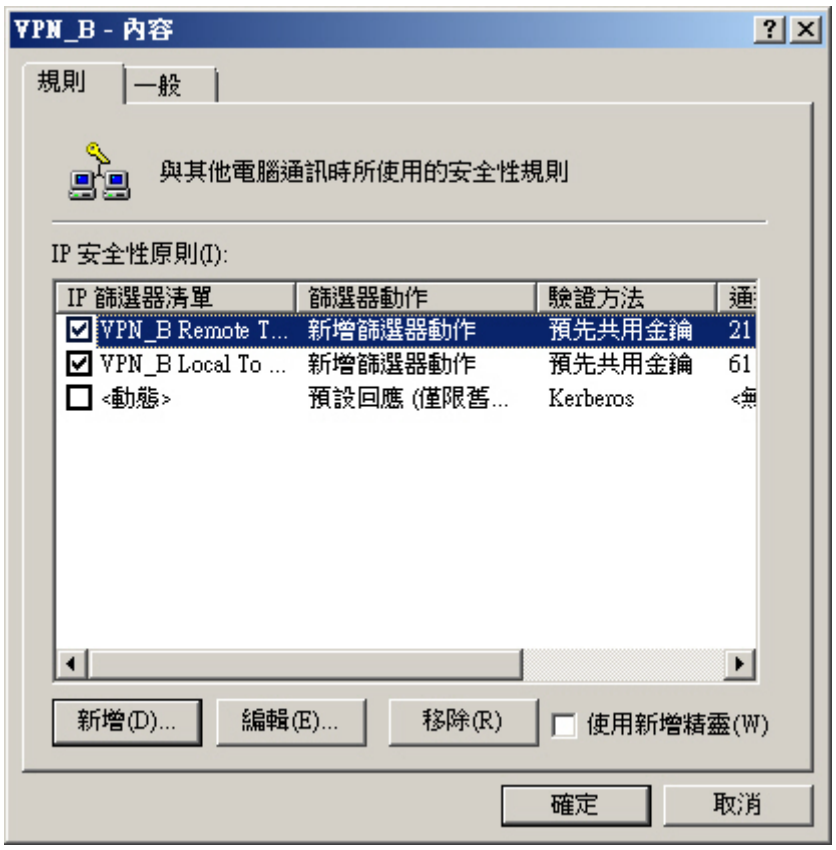


圖 11-103 完成 IP 安全性原則設定

步驟4. 在【VPN_B-內容】>【一般】視窗中：（如圖 11-104）

- 【名稱】輸入 VPN_B。
- 【檢查原則變更的間隔】輸入 180 分鐘。
- 按下【設定】鈕。
- 在【金鑰交換設定】視窗中：（如圖 11-105）
  - 勾選【主要金鑰完全正向加密（PFS）】。
  - 【驗證及產生新金鑰間隔】輸入 480 分鐘。
  - 按下【方法】鈕。
  - 在【金鑰交換安全性方法】視窗中，【安全性方法的喜好設定順序】選擇 3DES-SHA1-中(2)並按下【編輯】鈕：（如圖 11-106）
    - 在【IKE 安全性演算法】視窗中：（如圖 11-107）
      - 【完整性演算法】選擇 MD5。
      - 【加密演算法】選擇 3DES。
      - 【Diffie-Hellman 群組】選擇中(2)。
      - 按下【確定】鈕，完成設定。
    - 按下【確定】鈕。（如圖 11-108）
  - 按下【確定】鈕。
- 按下【確定】鈕，完成設定。

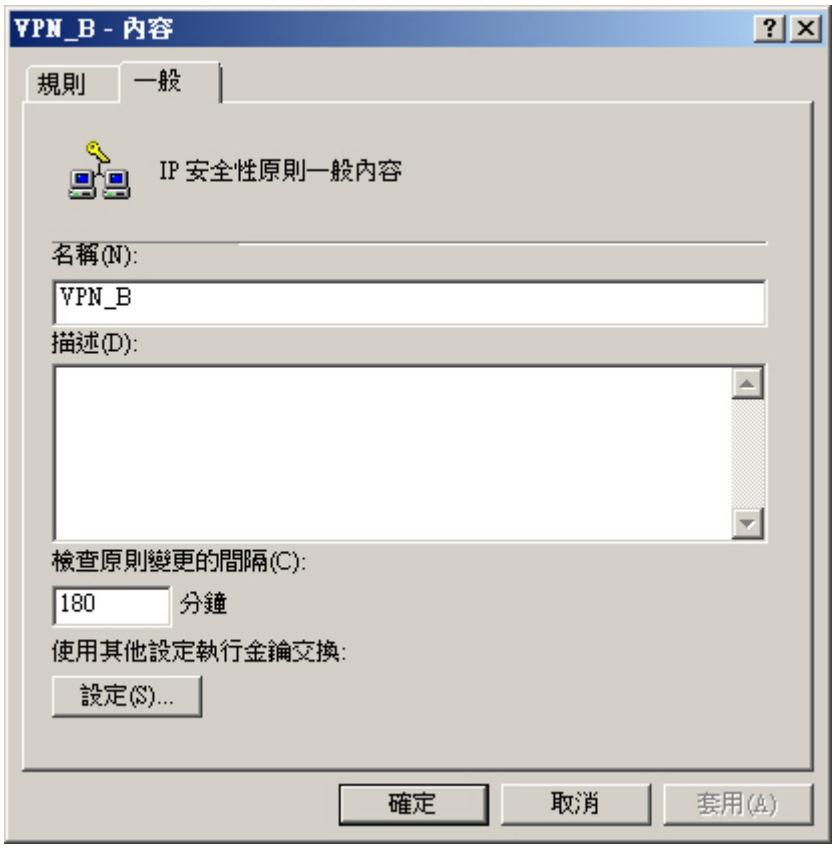


圖 11-104 設定 IP 安全性原則一般內容

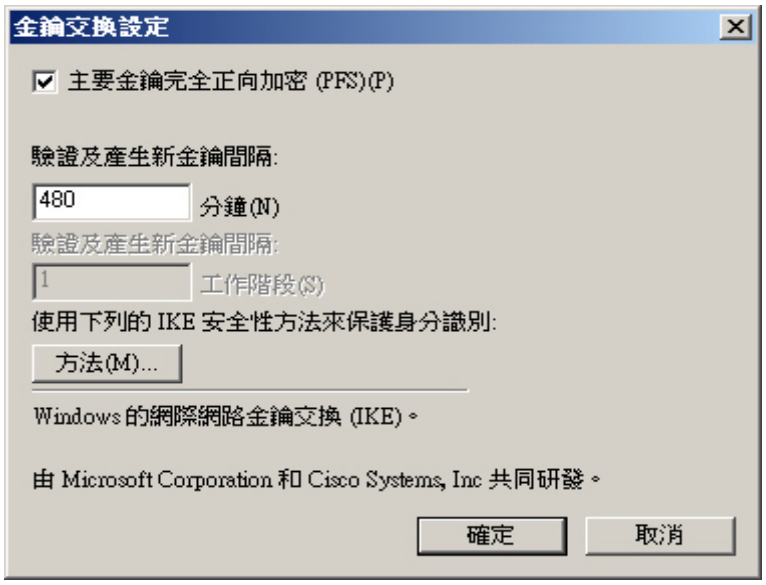


圖 11-105 金鑰交換設定

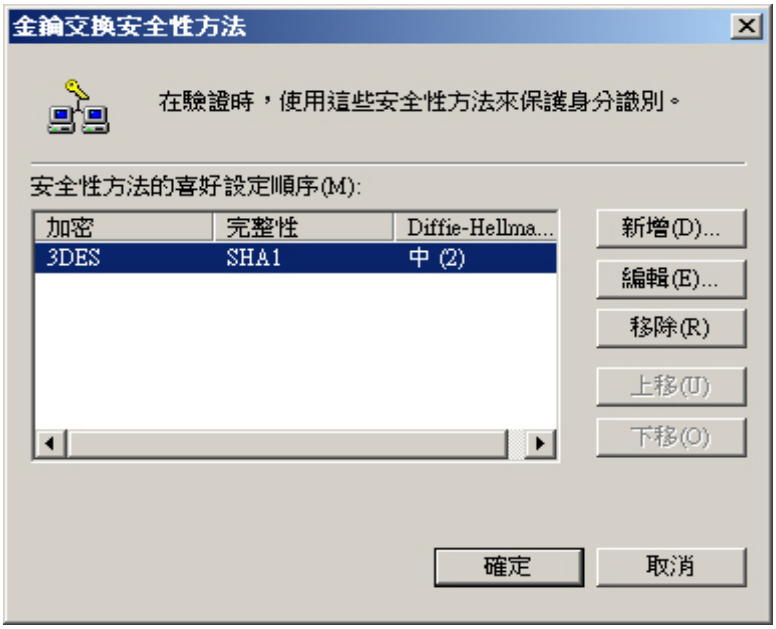


圖 11-106 編輯金鑰交換安全性方法

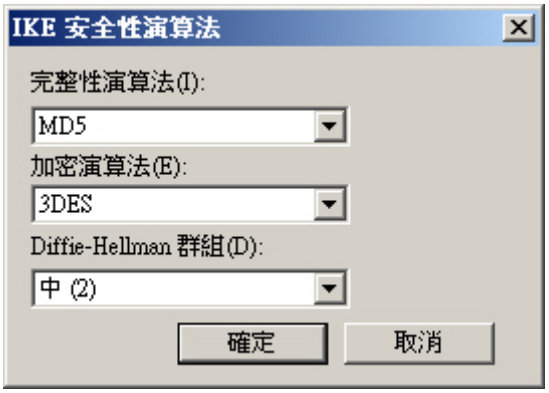


圖 11-107 IKE 安全性演算法設定

圖 11-108 完成金鑰交換安全性方法設定

步驟5. 在【Microsoft 管理主控台】視窗中，做下列設定：

- 在【主控台根目錄】>【IP 安全性原則(位置:本機電腦)】>【VPN_B】項目上，按下滑鼠右鍵並選擇【指派】。(如圖 11-109, 圖 11-110)

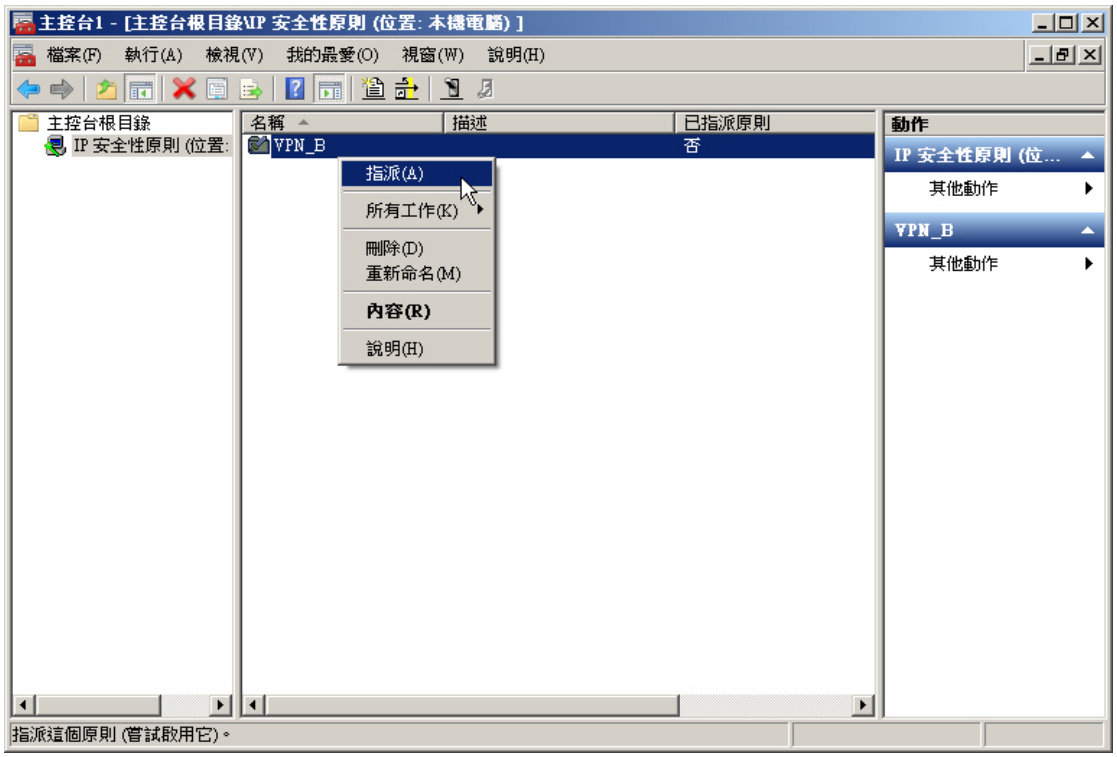


圖 11-109 指派 IP 安全性原則

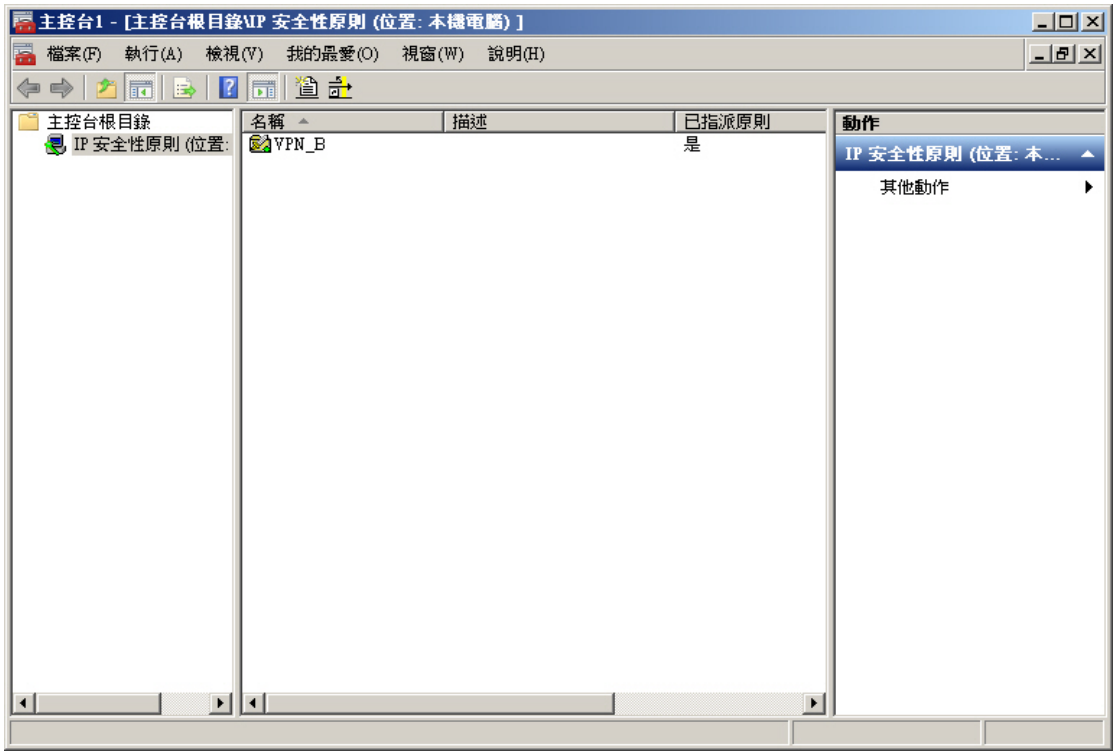


圖 11-110 完成 IP 安全性原則指派

步驟6. 在【開始】>【系統管理工具】>【服務】視窗中，做下列設定：（如圖 11-111）

- 在【服務（本機）】>【IPsec Policy Agent】項目上，按下滑鼠右鍵並選擇【重新啟動】。（如圖 11-112）

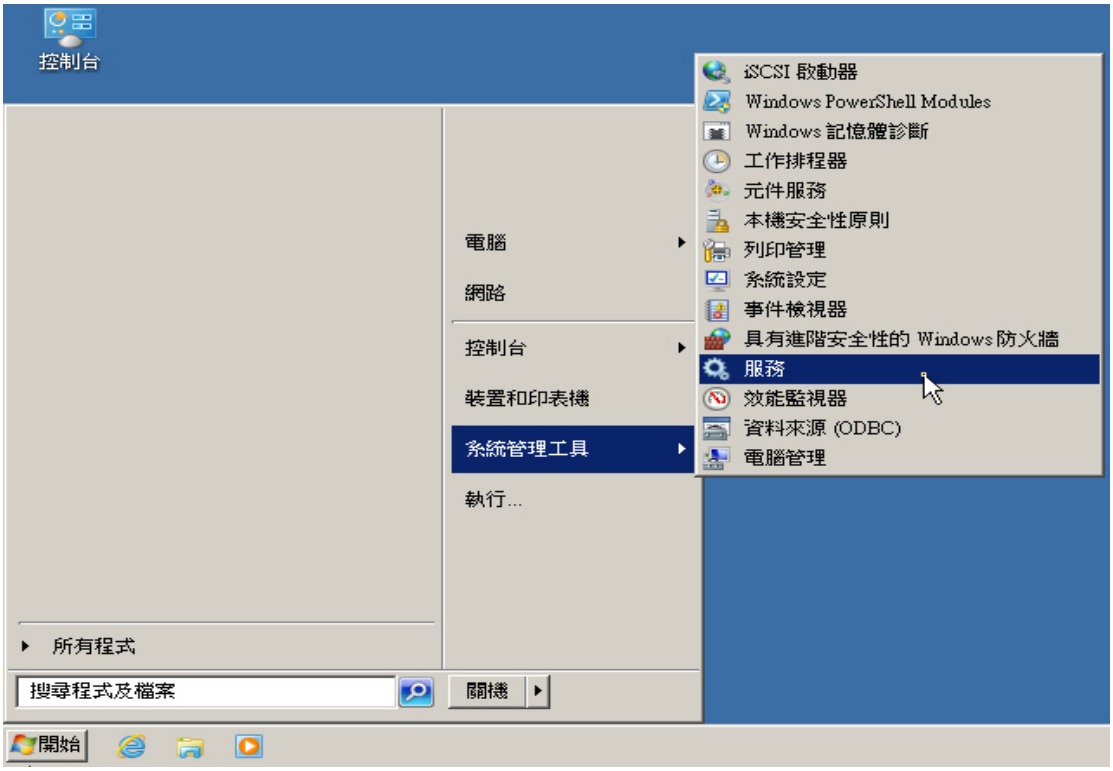


圖 11-111 開啟服務視窗

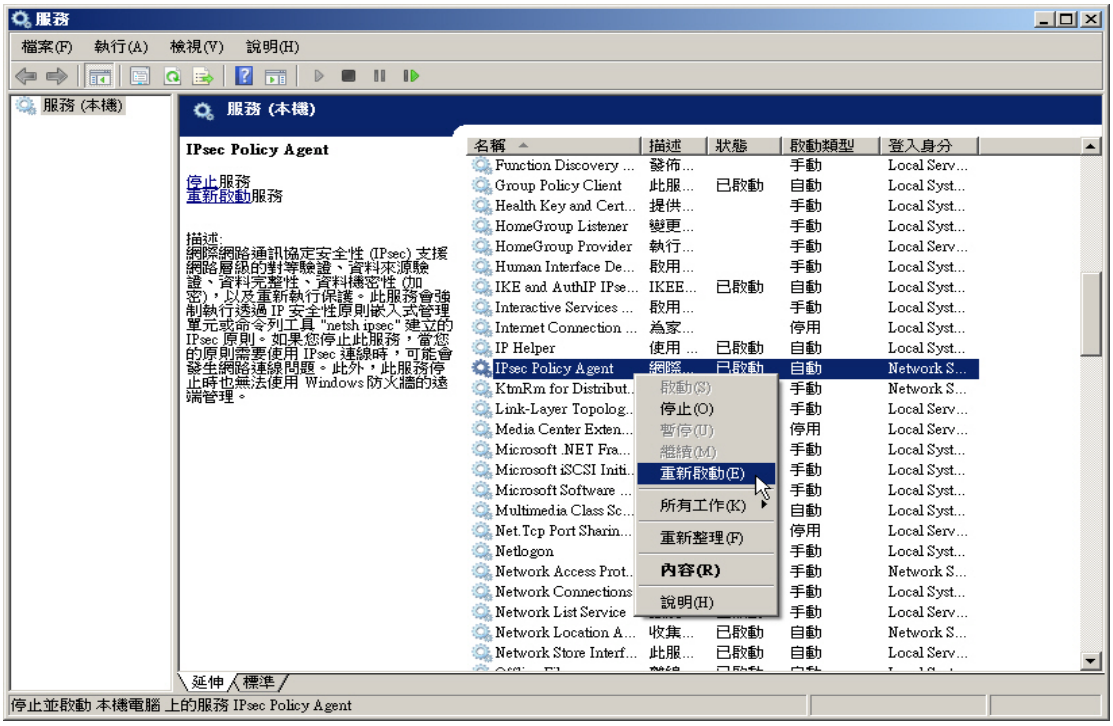


圖 11-112 重新啟動 IPsec Policy Agent 服務

注意：

1. 完成設定後，要持續 Ping 甲公司內網存在的 IP 位址（例如：192.168.10.1），若取得回應，即建起此 IPSec VPN 連線。**（如圖 11-113）**

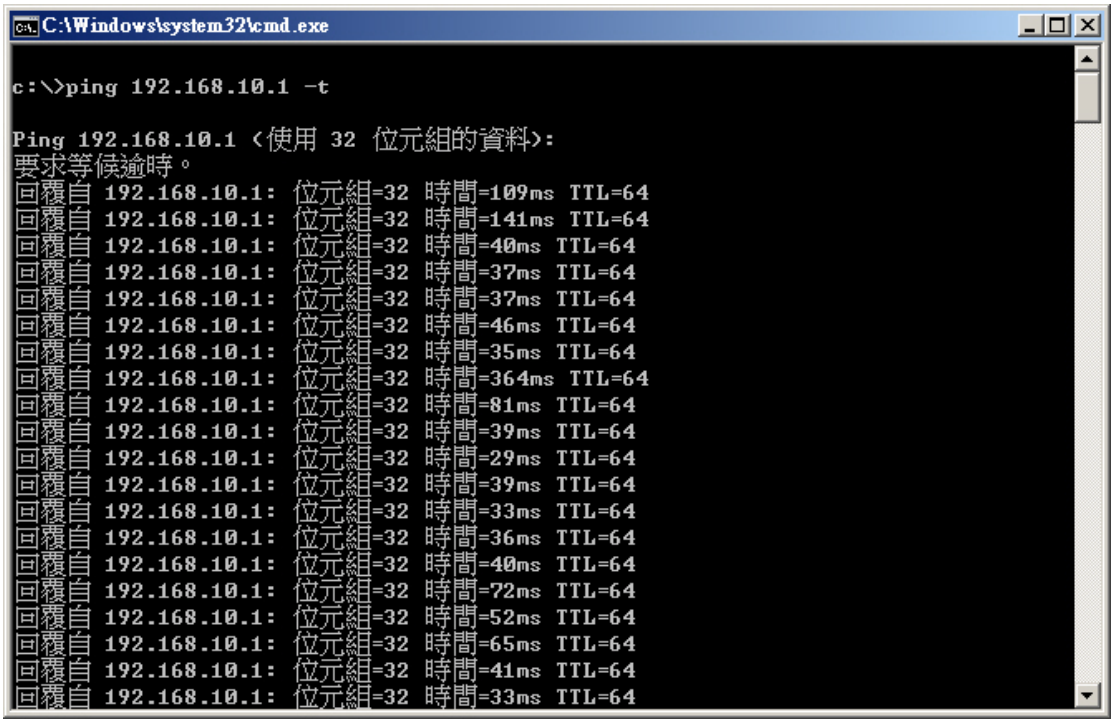


圖 11-113Ping 通甲公司內網存在的 IP 位址以建立 IPSec VPN 連線

步驟7. 完成 IPSec VPN 連線。（如圖 11-114）

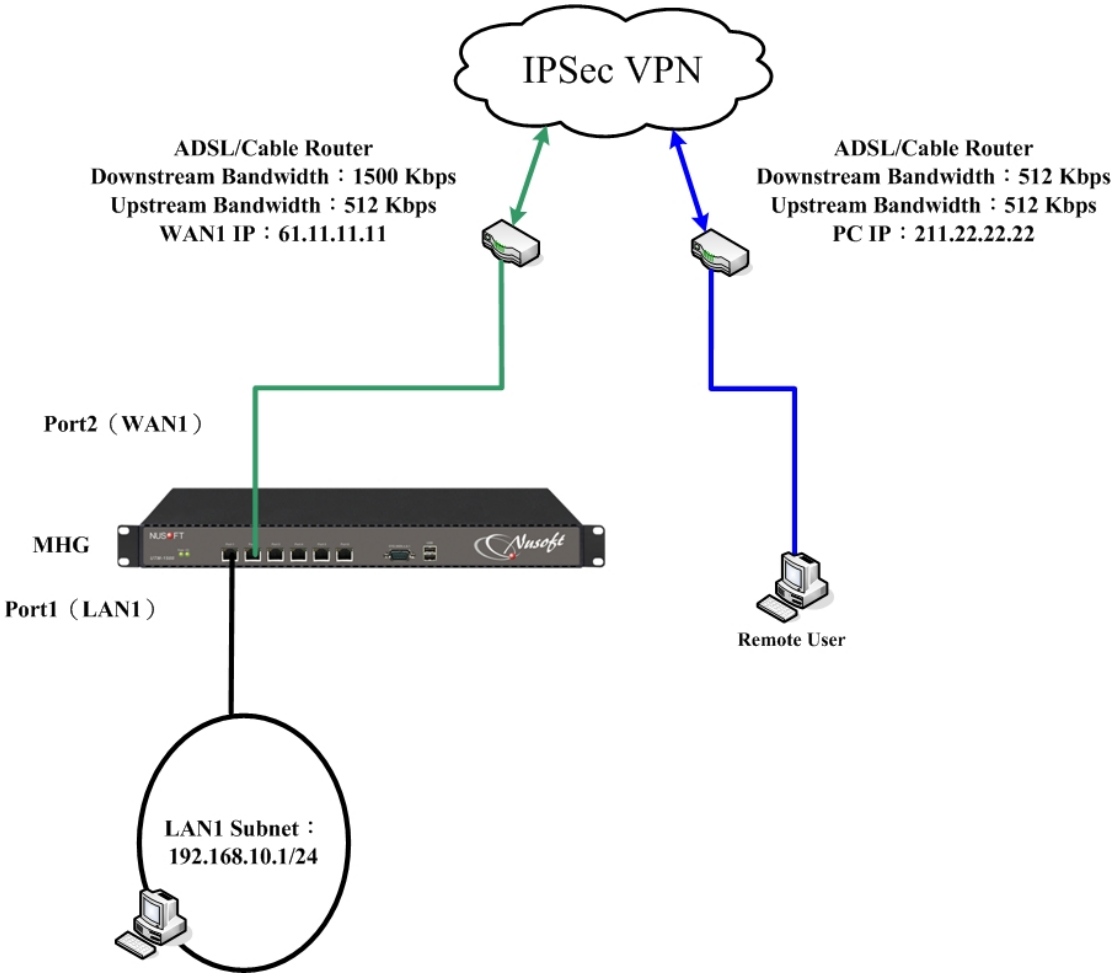


圖 11-114IPSec VPN 連線環境

11.1.3 使用兩台 MHG-2000 設定 IPSec VPN 連線的方法（連線使用 Aggressive mode 演算法）

環境設定

甲公司 Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

乙公司 Port1 設為 LAN1（192.168.20.1）為 192.168.20.x/24 網段。

Port2 設為 WAN1（211.22.22.22）和 ATU-R 對接，連上網際網路。

本範例以兩台 MHG-2000 做為平台操作，甲公司和乙公司建立 VPN（虛擬私人網路）連線以傳送資料。（連線使用 Aggressive mode 演算法）

甲公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。**（如圖 11-115）**

圖 11-115IPSec 自動加密頁面

步驟2. 【名稱】輸入 VPN_A、【連線介面】選擇 Port2（WAN1）。**（如圖 11-116）**

圖 11-116 設定 IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的乙公司閘道位址。**（如圖 11-117）**

圖 11-117 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-118）

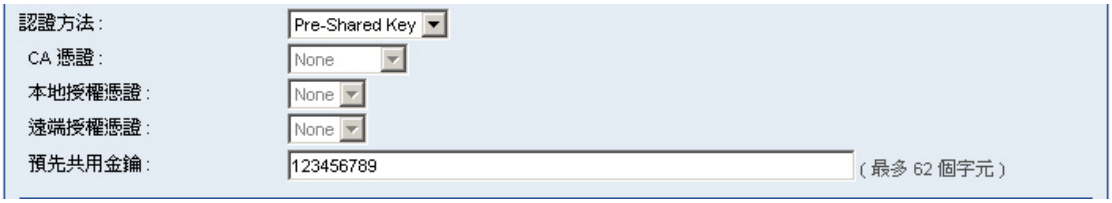


圖 11-118 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 SHA1、【群組】選擇 Diffie-Hellman 2。（如圖 11-119）

圖 11-119 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-120）

圖 11-120 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒。（如圖 11-121）

圖 11-121 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期

步驟8. 【使用模式】選擇 Aggressive mode、【本地 ID】輸入 11.11.11.11、【遠端 ID】輸入@abc123。（如圖 11-122）

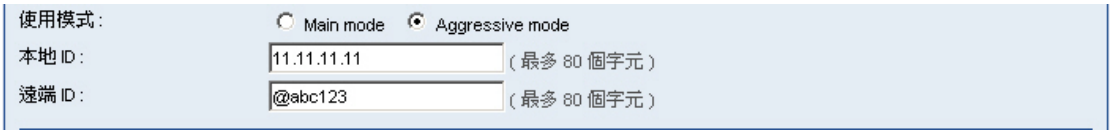


圖 11-122 設定 IPSec 使用模式

說明：

1. 本地/遠端 ID 設定為：

- 空白：會以彼此連線用的外部 IP 位址做為 ID。
- 不相同且彼此未使用的 IP 位址，例如：11.11.11.11、22.22.22.22。
- 數字或字母，前端需加@，例如：@123a、@abcd1。

步驟9. 完成 IPSec 自動加密設定。（如圖 11-123）

圖 11-123 完成 IPSec 自動加密設定

步驟10. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-124）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 將【可選取的通道】VPN_A 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-125）

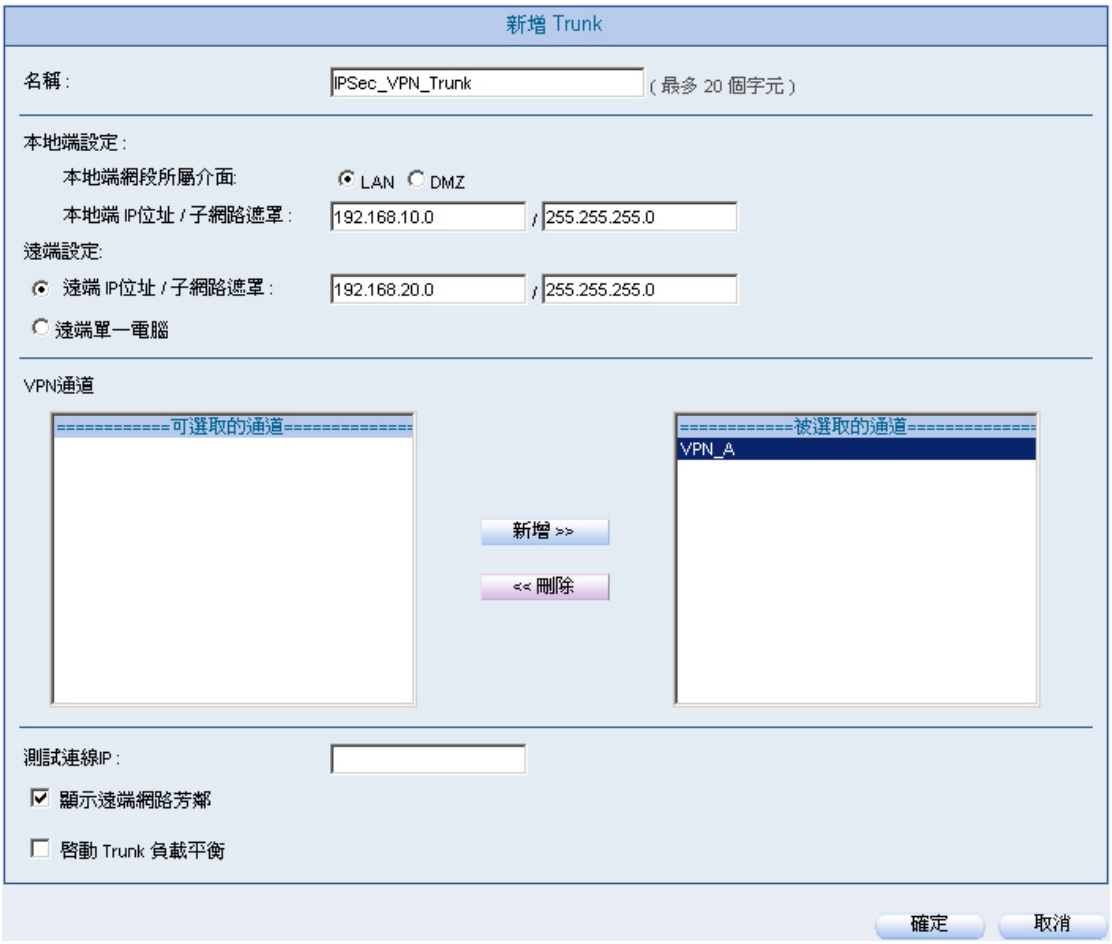


圖 11-124 設定 Trunk

圖 11-125 完成 Trunk 設定

步驟11. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-126）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-127）

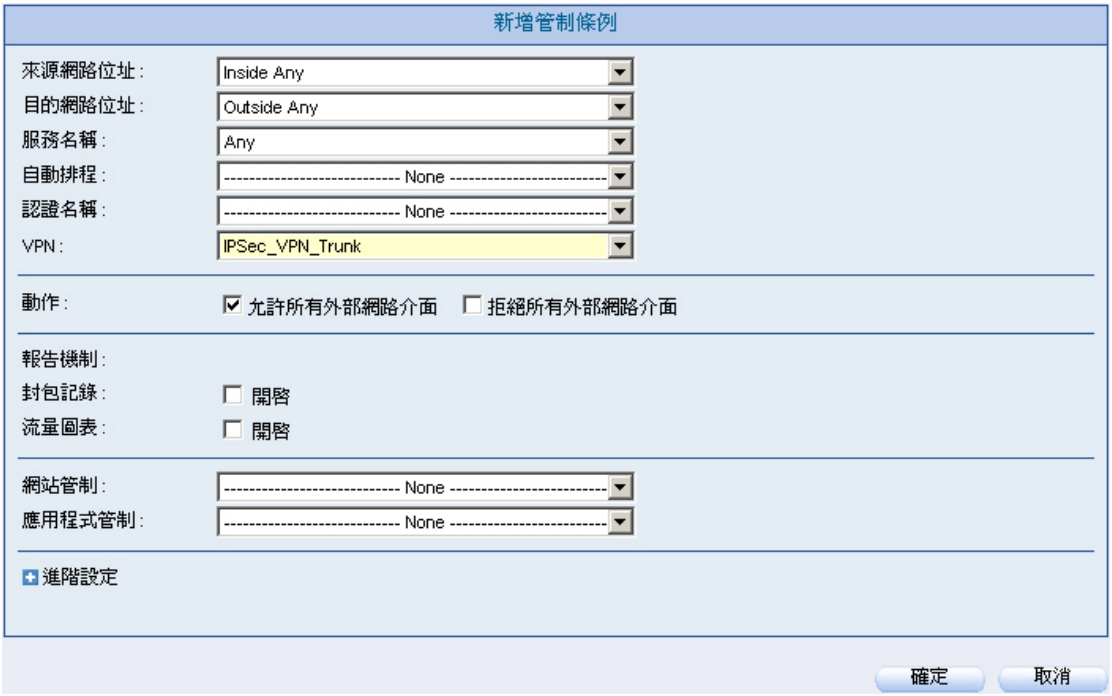


圖 11-126 設定 VPN Trunk 內部至外部之管制條例

圖 11-127 完成管制條例設定

步驟12. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-128）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-129）

圖 11-128 設定 VPN Trunk 外部至內部之管制條例

圖 11-129 完成管制條例設定

乙公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 11-130）

圖 11-130IPSec 自動加密頁面

步驟2. 【名稱】輸入 VPN_B、【連線介面】選擇 Port2（WAN1）。（如圖 11-131）

圖 11-131 設定 IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的甲公司閘道位址。（如圖 11-132）

圖 11-132 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-133）

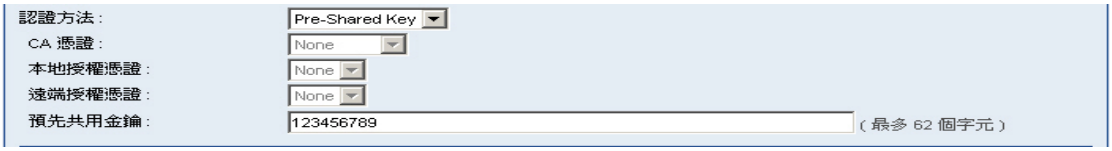


圖 11-133 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 SHA1、【群組】選擇 Diffie-Hellman 2。（如圖 11-134）

圖 11-134 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-135）

圖 11-135 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒。（如圖 11-136）

圖 11-136 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期

步驟8. 【使用模式】選擇 Aggressive mode、【本地 ID】輸入@abc123、【遠端 ID】輸入 11.11.11.11。（如圖 11-137）

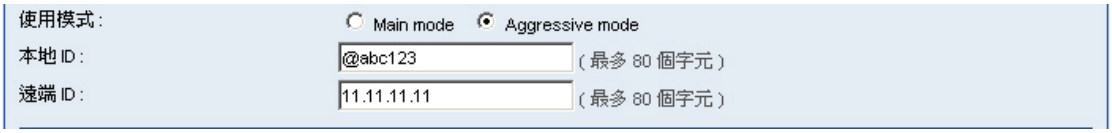


圖 11-137 設定 IPSec 使用模式

步驟9. 完成 IPSec 自動加密設定。（如圖 11-138）

圖 11-138 完成 IPSec 自動加密設定

步驟10. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-139）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 將【可選取的通道】VPN_B 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-140）

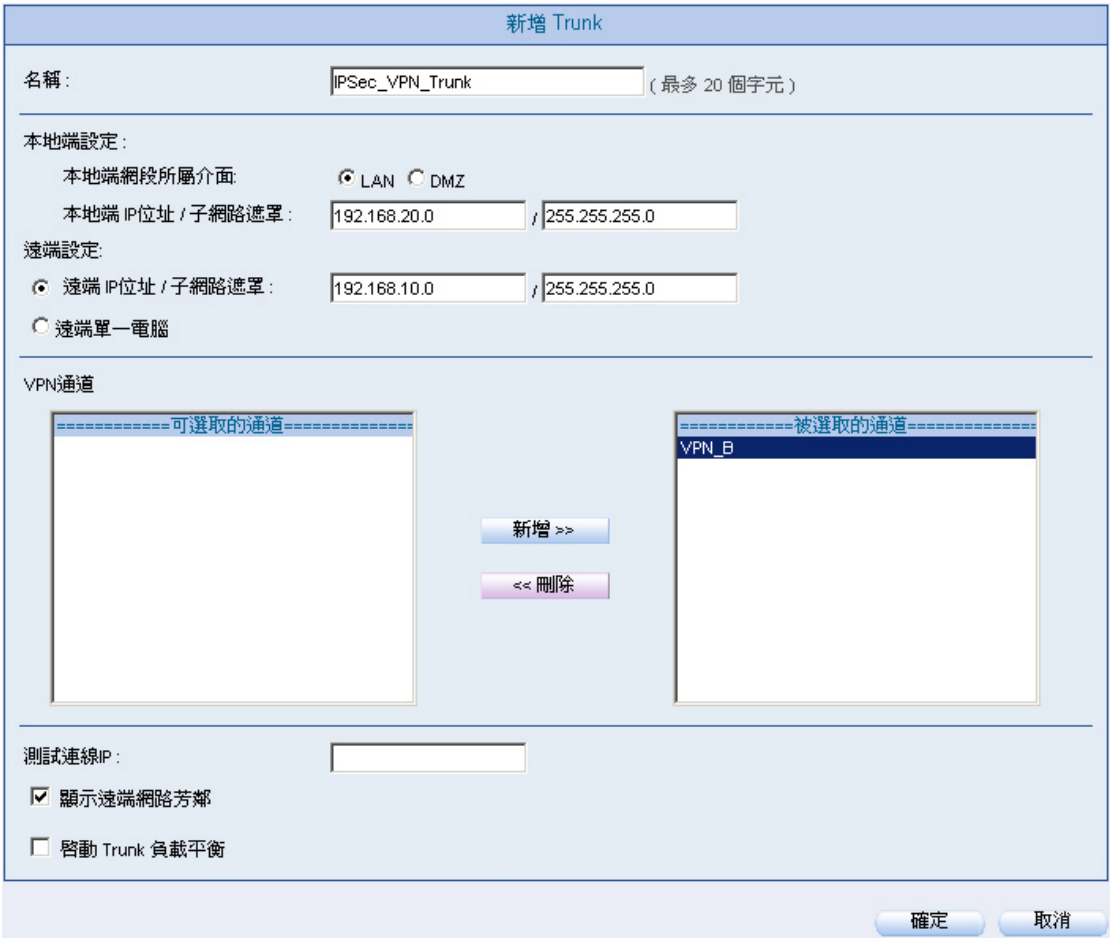


圖 11-139 設定 Trunk

圖 11-140 完成 Trunk 設定

步驟11. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-141）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-142）

圖 11-141 設定 VPN Trunk 內部至外部之管制條例

圖 11-142 完成管制條例設定

步驟12. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-143）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-144）

圖 11-143 設定 VPN Trunk 外部至內部之管制條例

圖 11-144 完成管制條例設定

步驟13. 完成 IPSec VPN 連線。（如圖 11-145）

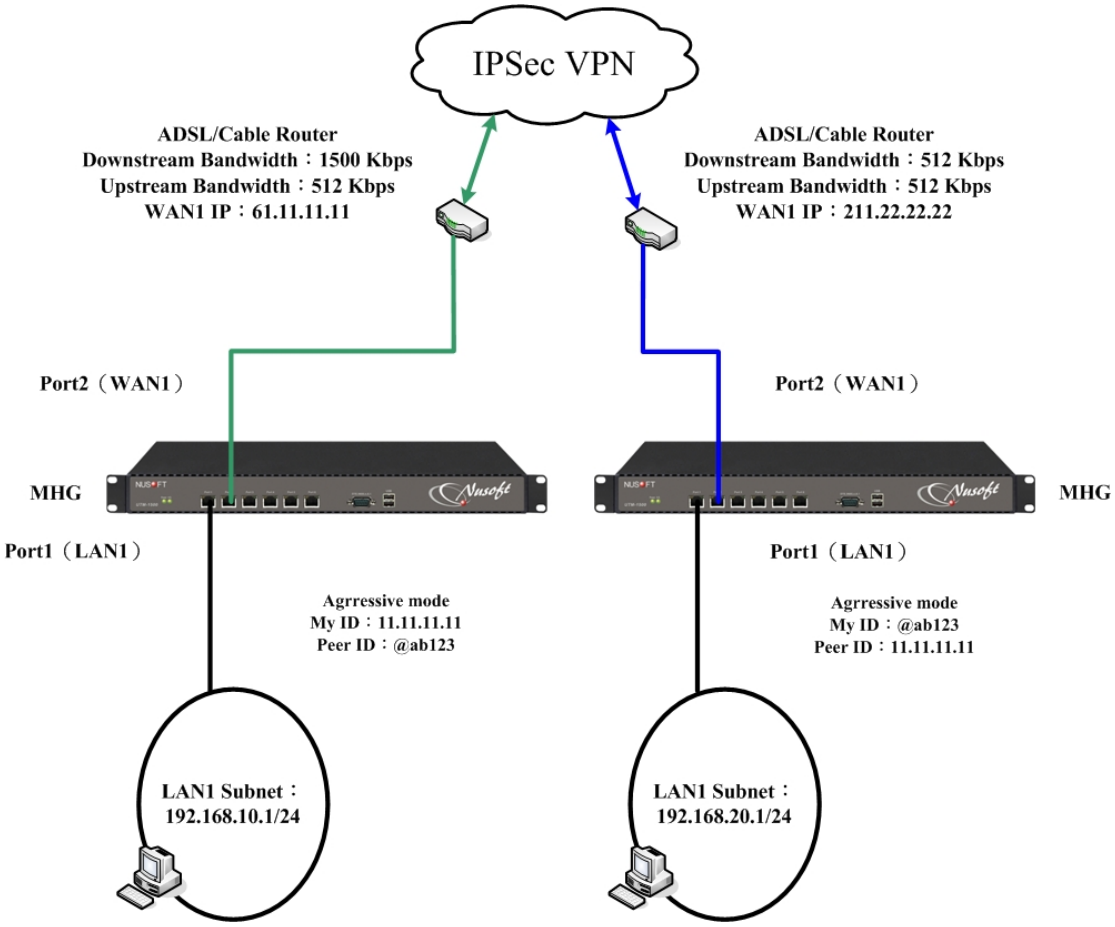


圖 11-145IPSec VPN 連線環境

11.1.4 使用兩台 MHG-2000 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）

環境設定

甲公司 Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

Port3 設為 WAN2（61.22.22.22）和 ATU-R 對接，連上網際網路。

乙公司 Port1 設為 LAN1（192.168.20.1）為 192.168.20.x/24 網段。

Port2 設為 WAN1（211.22.22.22）和 ATU-R 對接，連上網際網路。

Port3 設為 WAN2（211.33.33.33）和 ATU-R 對接，連上網際網路。

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 MHG-2000 做為平台操作，甲公司和乙公司建立 VPN（虛擬私人網路）連線以傳送資料。（連線使用 GRE/IPSec 封包封裝演算法）

甲公司的設定步驟如下：

步驟1. 在【進階功能】>【證書管理】>【遠端 CA 憑證】頁面中，做下列設定：

- 按下【匯入】鈕，進入【匯入 CA 憑證】頁面，將 CSR（Certificate Signing Request）申請簽署的 CA Server 證書（例如：CA_Server_01.pem、CA_Server_02.pem 檔）存放路徑填入【匯入 CA 證書】欄位，按下【確定】鈕，匯入 MHG-2000。**（如圖 11-146，圖 11-147，圖 11-148，圖 11-149）**

圖 11-146 匯入第一筆 CSR 申請簽署的 CA Server 證書

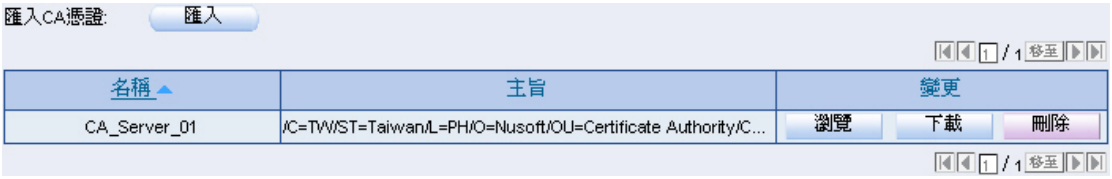


圖 11-147 第一筆 CSR 申請簽署的 CA Server 證書匯入完成

圖 11-148 匯入第二筆 CSR 申請簽署的 CA Server 證書

圖 11-149 第二筆 CSR 申請簽署的 CA Server 證書匯入完成

步驟2. 在【進階功能】>【證書管理】>【授權憑證】頁面中，做下列設定：

- 按下【新增】鈕。**（如圖 11-150）**
- 【名稱】輸入 Site_A_01。
- 【憑證公用名稱】輸入 VPN_01。
- 【國家】選擇 Taiwan。
- 【州/省】輸入 Taiwan。
- 【地區（城市）】輸入 Taipei。
- 【公司】輸入 Nusoft。
- 【單位】輸入 Support。
- 【電子郵件】輸入 support@nusoft.com.tw。
- 【金鑰長度】選擇 2048。
- 輸入指定的【有效時間】。
- 按下【確定】鈕。**（如圖 11-151）**
- 按【下載】鈕，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 11-152）**
- 按下【匯入】鈕，進入【匯入授權憑證】頁面，將本地經由 CA Server 簽署後取回之證書（例如：.pem 檔）存放路徑填入【匯入授權證書】欄位，按下【確定】鈕，匯入 MHG-2000。**（如圖 11-153, 圖 11-154）**
- 再次按下【新增】鈕。**（如圖 11-155）**
- 【名稱】輸入 Site_B_01。
- 【憑證公用名稱】輸入 VPN_01。
- 【國家】選擇 Great Britain (UK)。
- 【州/省】輸入 Great Britain。
- 【地區（城市）】輸入 London。
- 【公司】輸入 Nusoft_Branch_Office。
- 【單位】輸入 Support。
- 【電子郵件】輸入 support@nusoft.com.uk。
- 【金鑰長度】選擇 2048。
- 輸入指定的【有效時間】。
- 按下【確定】鈕。**（如圖 11-156）**
- 按【下載】鈕，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 11-157）**
- 按下【匯入】鈕，進入【匯入授權憑證】頁面，將本地經由 CA Server 簽署後取回之證書（例如：.pem 檔）存放路徑填入【匯入授權證書】欄位，按下【確定】鈕，匯入 MHG-2000。**（如圖 11-158, 圖 11-159）**

- 將乙公司經由 CA Server（CA_Server_01）簽署後取回之證書（例如：.pem 檔），匯入 MHG-2000。**（如圖 11-160，圖 11-161）**
- 將乙公司經由 CA Server（CA_Server_02）簽署後取回之證書（例如：.pem 檔），匯入 MHG-2000。**（如圖 11-162，圖 11-163）**

圖 11-150 設定第一筆 CSR

圖 11-151 完成第一筆 CSR 設定

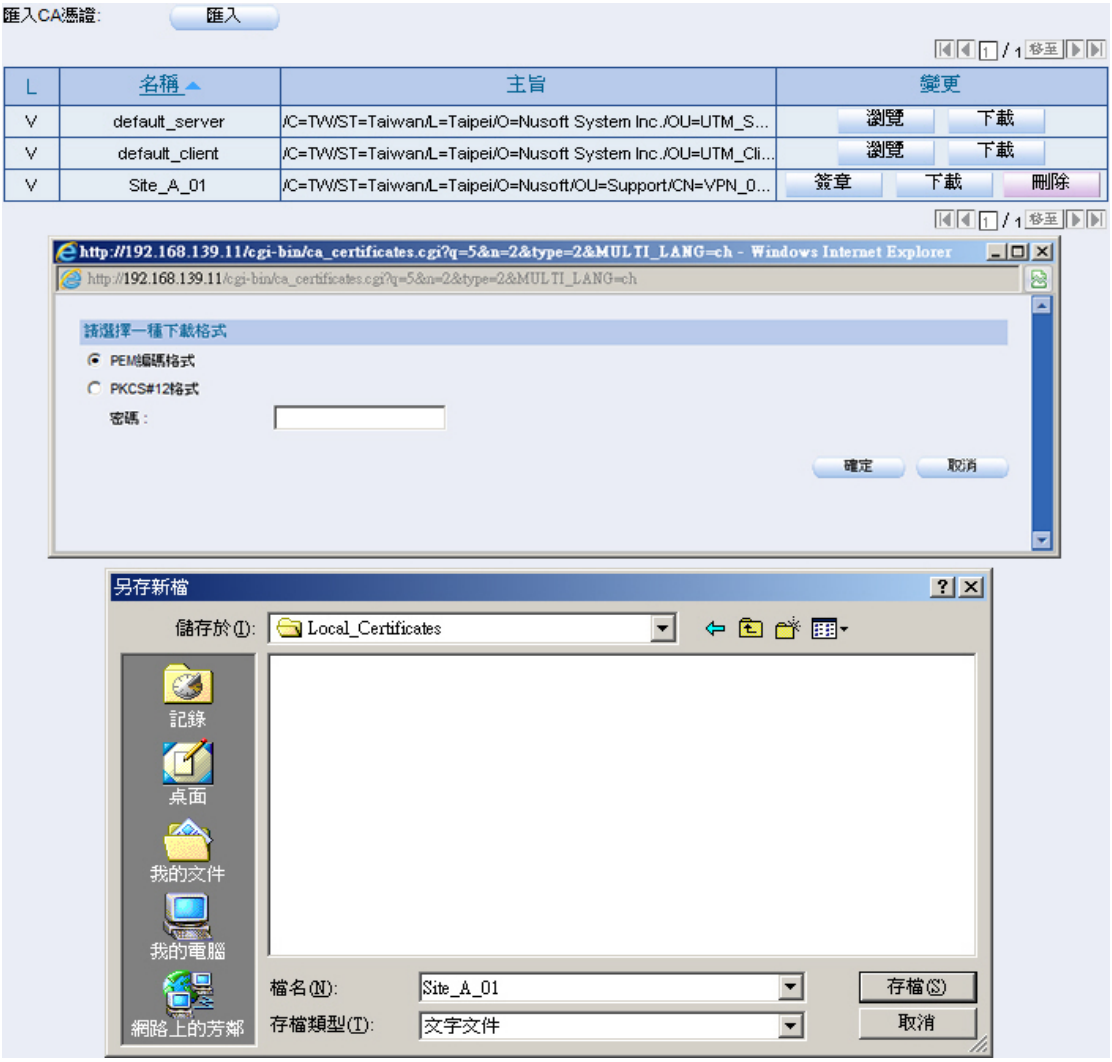


圖 11-152 下載第一筆 CSR 檔案

圖 11-153 匯入第一筆授權證書

圖 11-154 第一筆授權證書匯入完成

圖 11-155 設定第二筆 CSR

圖 11-156 完成第二筆 CSR 設定

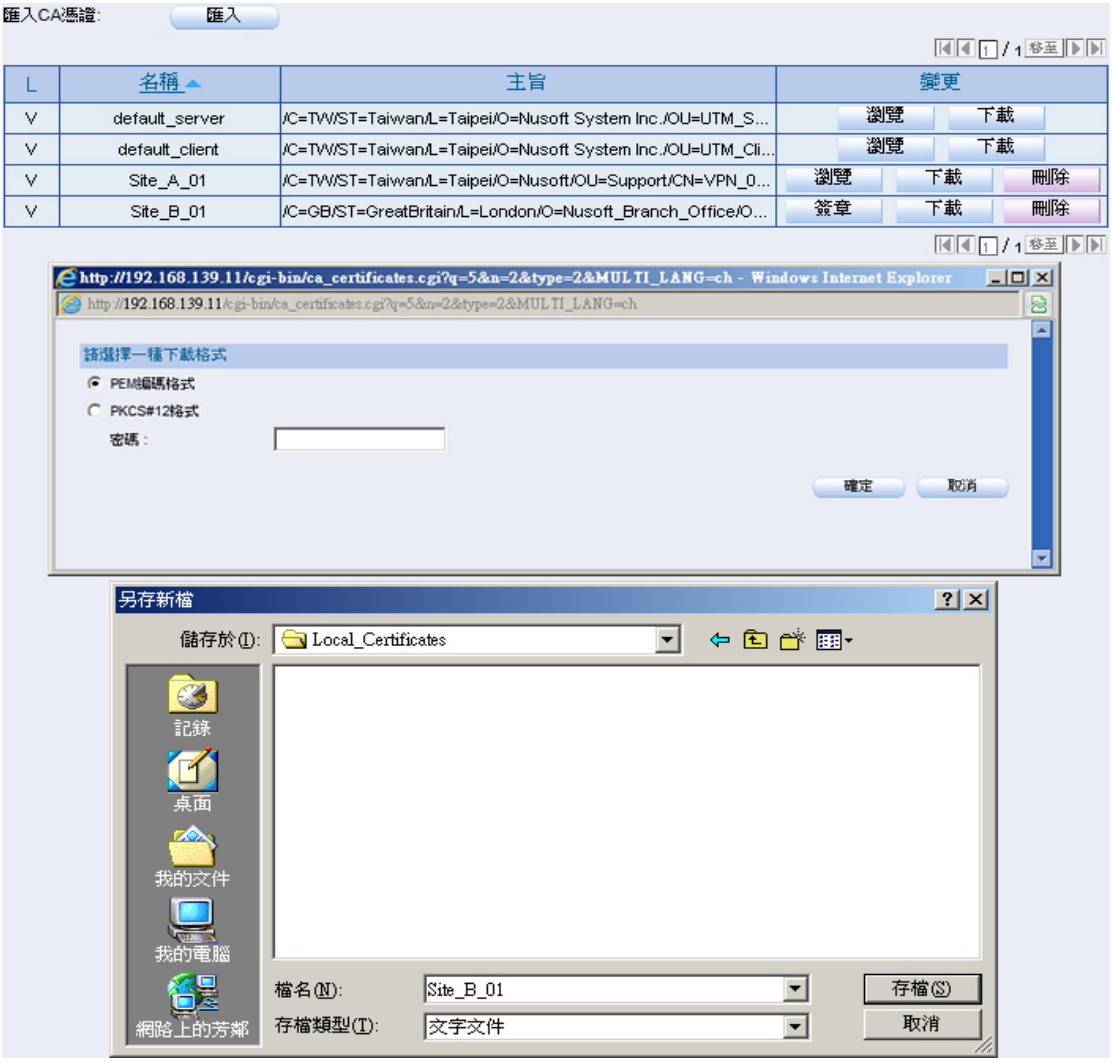


圖 11-157 下載第二筆 CSR 檔案

圖 11-158 匯入第二筆授權證書

圖 11-159 第二筆授權證書匯入完成

圖 11-160 上傳第一筆乙公司證書

圖 11-161 第一筆乙公司證書上傳完成

圖 11-162 上傳第二筆乙公司證書

圖 11-163 第二筆乙公司證書上傳完成

步驟3. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 11-164）

圖 11-164IPSec 自動加密頁面

步驟4. 【名稱】輸入 VPN_01、【連線介面】選擇 Port2（WAN1）。（如圖 11-165）

圖 11-165 設定 IPSec 名稱和外部網路介面

步驟5. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的乙公司閘道 WAN1 IP 位址。（如圖 11-166）

圖 11-166 設定 IPSec 到目的位址

步驟6. 【認證方法】選擇 RSA Signature、【CA 憑證】選擇 CA_Server_01、【本地授權憑證】選擇 Site_A_01、【遠端授權憑證】選擇 Site_A_02。（如圖 11-167）

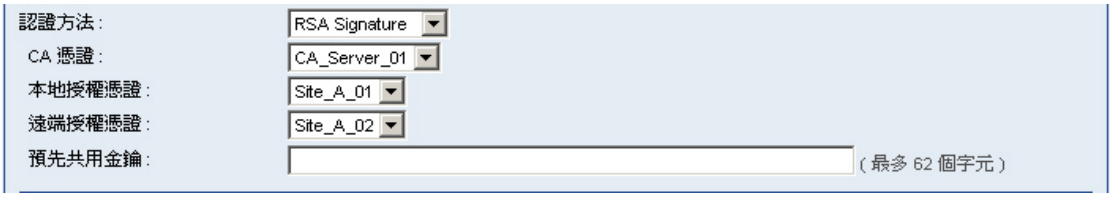


圖 11-167 設定 IPSec 認證方法

步驟7. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-168）

圖 11-168 設定 ISAKMP 演算法

步驟8. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-169）

圖 11-169 設定 IPSec 演算法

步驟9. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-170）

圖 11-170 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟10. 在【GRE/IPSec】欄位中，【GRE 本地端 IP】輸入 192.168.50.100、【GRE 遠端 IP】輸入 192.168.50.200。（如圖 11-171）

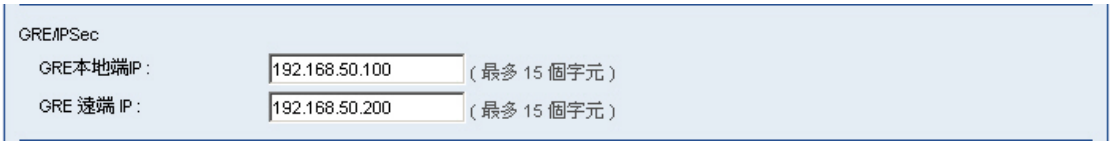


圖 11-171 設定 GRE/IPSec

說明：

1. 【GRE 本地端 IP】和【GRE 遠端 IP】需為未被使用的同一 C Class 網段之 IP。

步驟11. 完成 VPN_01 IPSec 自動加密設定。（如圖 11-172）

圖 11-172 完成 VPN_01 IPSec 自動加密設定

步驟12. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，再次按下【新增】鈕。（如圖 11-173）

圖 11-173IPSec 自動加密頁面

步驟13. 【名稱】輸入 VPN_02、【連線介面】選擇 Port3（WAN2）。（如圖 11-174）

圖 11-174 設定 IPSec 名稱和外部網路介面

步驟14. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的乙公司閘道 WAN2 IP 位址。（如圖 11-175）

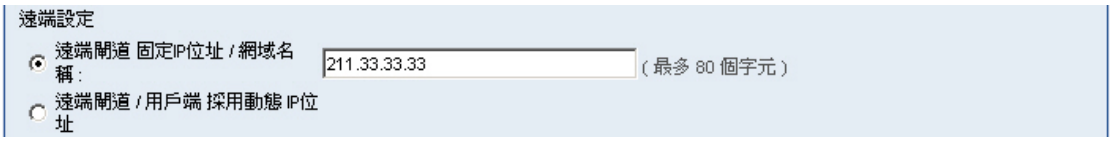


圖 11-175 設定 IPSec 到目的位址

步驟15. 【認證方法】選擇 RSA Signature、【CA 憑證】選擇 CA_Server_02、【本地授權憑證】選擇 Site_B_01、【遠端授權憑證】選擇 Site_B_02。（如圖 11-176）

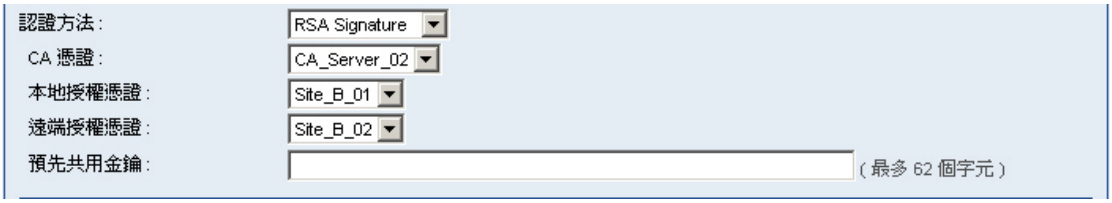


圖 11-176 設定 IPSec 認證方法

步驟16. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-177）

圖 11-177 設定 ISAKMP 演算法

步驟17. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-178）

圖 11-178 設定 IPSec 演算法

步驟18. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-179）

圖 11-179 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟19. 在【GRE/IPSec】欄位中，【GRE 本地端 IP】輸入 192.168.60.100、【GRE 遠端 IP】輸入 192.168.60.200。（如圖 11-180）

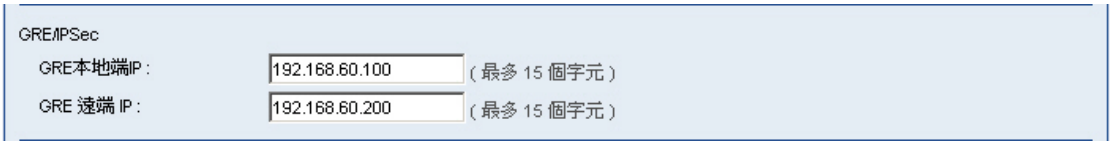


圖 11-180 設定 GRE/IPSec

步驟20. 完成 VPN_02 IPSec 自動加密設定。（如圖 11-181）

圖 11-181 完成 VPN_02 IPSec 自動加密設定

步驟21. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-182）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 將【可選取的通道】VPN_01、VPN_02 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-183）

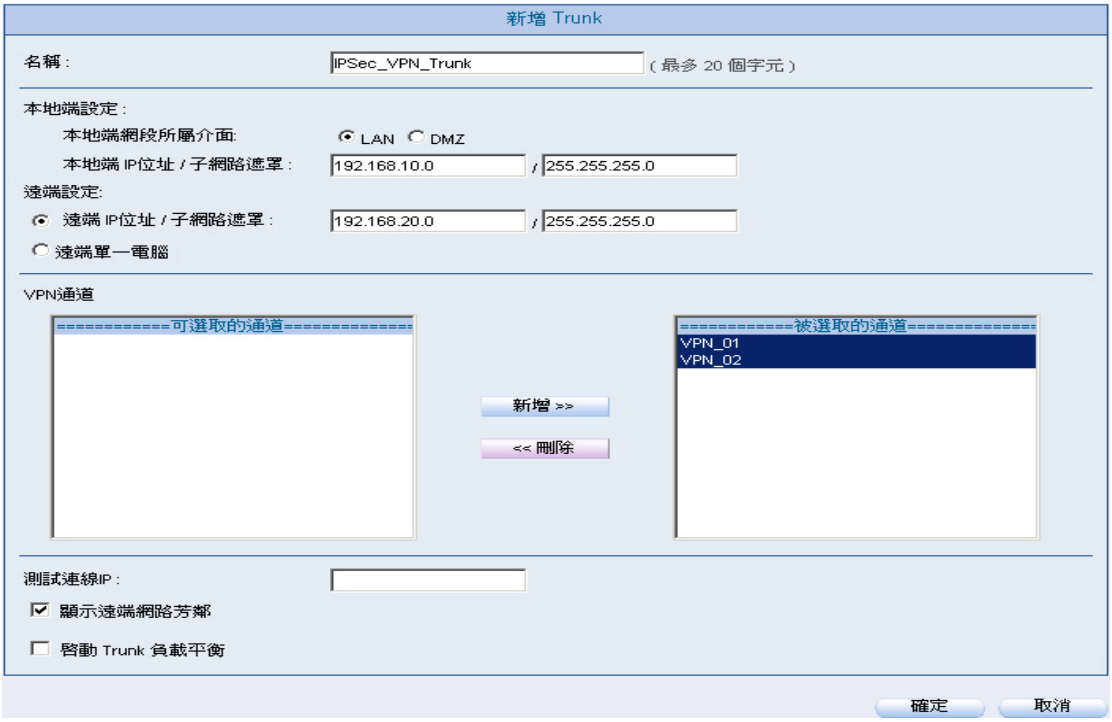


圖 11-182 設定 Trunk

圖 11-183 完成 Trunk 設定

步驟22. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-184）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-185）

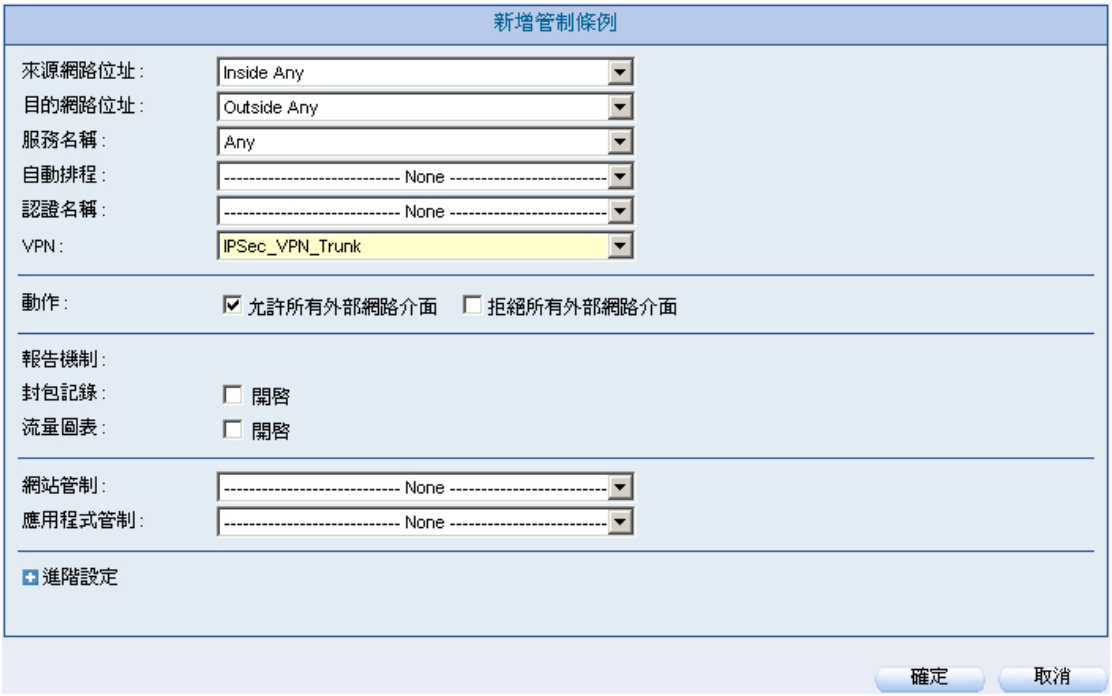


圖 11-184 設定 VPN Trunk 內部至外部之管制條例

圖 11-185 完成管制條例設定

步驟23. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-186）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-187）

圖 11-186 設定 VPN Trunk 外部至內部之管制條例

圖 11-187 完成管制條例設定

乙公司的設定步驟如下：

步驟1. 在【進階功能】>【證書管理】>【遠端 CA 憑證】頁面中，做下列設定：

- 按下【匯入】鈕，進入【匯入 CA 憑證】頁面，將 CSR（Certificate Signing Request）申請簽署的 CA Server 證書（例如：CA_Server_01.pem、CA_Server_02.pem 檔）存放路徑填入【匯入 CA 證書】欄位，按下【確定】鈕，匯入 MHG-2000。**（如圖 11-188，圖 11-189，圖 11-190，圖 11-191）**

圖 11-188 匯入第一筆 CSR 申請簽署的 CA Server 證書

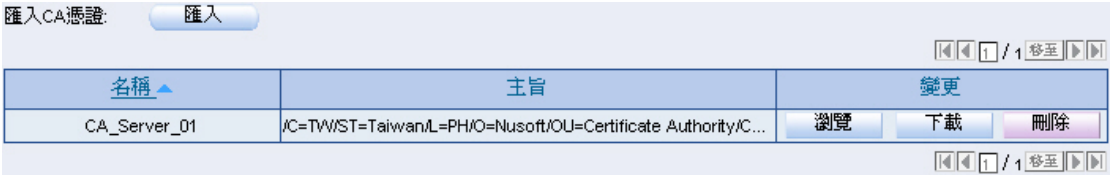


圖 11-189 第一筆 CSR 申請簽署的 CA Server 證書匯入完成

圖 11-190 匯入第二筆 CSR 申請簽署的 CA Server 證書

圖 11-191 第二筆 CSR 申請簽署的 CA Server 證書匯入完成

步驟2. 在【進階功能】>【證書管理】>【授權憑證】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 11-192）
- 【名稱】輸入 Site_A_02。
- 【憑證公用名稱】輸入 VPN_02。
- 【國家】選擇 Taiwan。
- 【州/省】輸入 Taiwan。
- 【地區（城市）】輸入 Taipei。
- 【公司】輸入 Nusoft。
- 【單位】輸入 Sales。
- 【電子郵件】輸入 sales@nusoft.com.tw。
- 【金鑰長度】選擇 2048。
- 輸入指定的【有效時間】。
- 按下【確定】鈕。（如圖 11-193）
- 按【下載】鈕，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 11-194）
- 按下【匯入】鈕，進入【匯入授權憑證】頁面，將本地經由 CA Server 簽署後取回之證書（例如：.pem 檔）存放路徑填入【匯入授權證書】欄位，按下【確定】鈕，匯入 MHG-2000。（如圖 11-195, 圖 11-196）
- 再次按下【新增】鈕。（如圖 11-197）
- 【名稱】輸入 Site_B_02。
- 【憑證公用名稱】輸入 VPN_02。
- 【國家】選擇 Great Britain (UK)。
- 【州/省】輸入 Great Britain。
- 【地區（城市）】輸入 London。
- 【公司】輸入 Nusoft_Branch_Office。
- 【單位】輸入 Sales。
- 【電子郵件】輸入 sales@nusoft.com.uk。
- 【金鑰長度】選擇 2048。
- 輸入指定的【有效時間】。
- 按下【確定】鈕。（如圖 11-198）
- 按【下載】鈕，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 11-199）
- 按下【匯入】鈕，進入【匯入授權憑證】頁面，將本地經由 CA Server 簽署後取回之證書（例如：.pem 檔）存放路徑填入【匯入授權證書】欄位，按下【確定】鈕，匯入 MHG-2000。（如圖 11-200, 圖 11-201）

- 將甲公司經由 CA Server（CA_Server_01）簽署後取回之證書（例如：.pem 檔），匯入 MHG-2000。**（如圖 11-202, 圖 11-203）**
- 將甲公司經由 CA Server（CA_Server_02）簽署後取回之證書（例如：.pem 檔），匯入 MHG-2000。**（如圖 11-204, 圖 11-205）**

圖 11-192 設定第一筆 CSR

圖 11-193 完成第一筆 CSR 設定

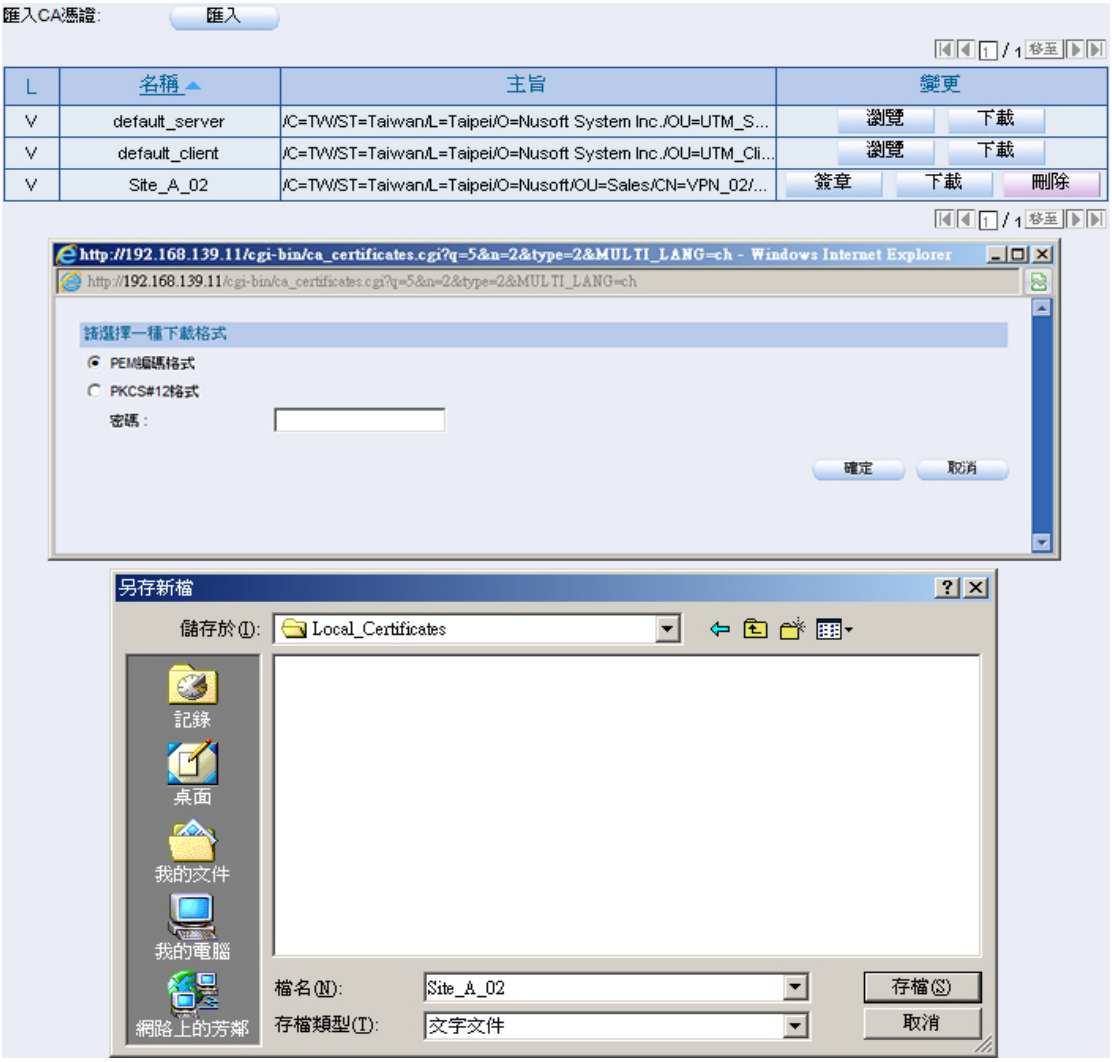


圖 11-194 下載第一筆 CSR 檔案

圖 11-195 匯入第一筆授權證書

圖 11-196 第一筆授權證書匯入完成

圖 11-197 設定第二筆 CSR

圖 11-198 完成第二筆 CSR 設定

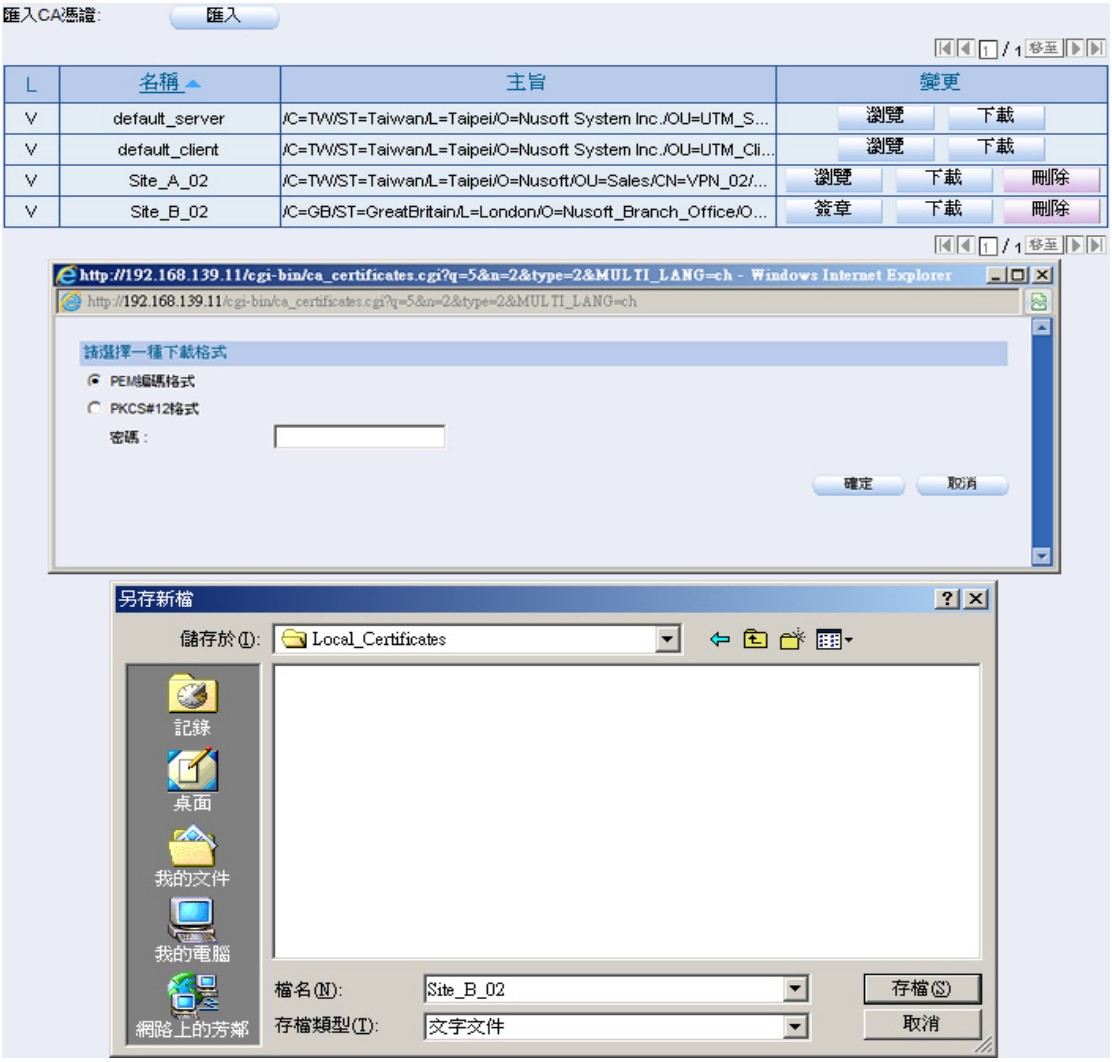


圖 11-199 下載第二筆 CSR 檔案

圖 11-200 匯入第二筆授權證書

圖 11-201 第二筆授權證書匯入完成

圖 11-202 上傳第一筆甲公司證書

圖 11-203 第一筆甲公司證書上傳完成

圖 11-204 上傳第二筆甲公司證書

圖 11-205 第二筆甲公司證書上傳完成

步驟3. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 11-206）

圖 11-206IPSec 自動加密頁面

步驟4. 【名稱】輸入 VPN_01、【連線介面】選擇 Port2（WAN1）。（如圖 11-207）

圖 11-207 設定 IPSec 名稱和外部網路介面

步驟5. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的甲公司閘道 WAN1 IP 位址。（如圖 11-208）

圖 11-208 設定 IPSec 到目的位址

步驟6. 【認證方法】選擇 RSA Signature、【CA 憑證】選擇 CA_Server_01、【本地授權憑證】選擇 Site_A_02、【遠端授權憑證】選擇 Site_A_01。（如圖 11-209）

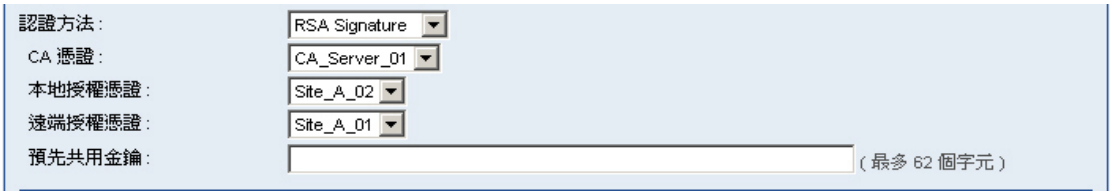


圖 11-209 設定 IPSec 認證方法

步驟7. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-210）

圖 11-210 設定 ISAKMP 演算法

步驟8. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-211）

圖 11-211 設定 IPSec 演算法

步驟9. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-212）

圖 11-212 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟10. 在【GRE/IPSec】欄位中，【GRE 本地端 IP】輸入 192.168.50.200、【GRE 遠端 IP】輸入 192.168.50.100。（如圖 11-213）

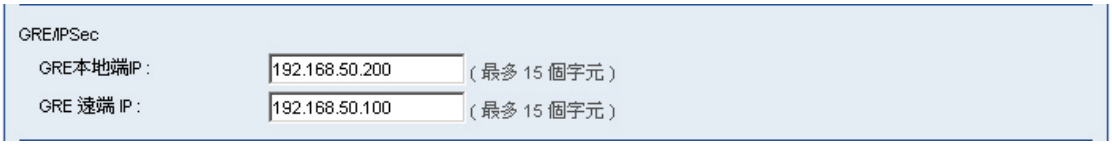


圖 11-213 設定 GRE/IPSec

步驟11. 完成 VPN_01 IPSec 自動加密設定。（如圖 11-214）

圖 11-214 完成 VPN_01 IPSec 自動加密設定

步驟12. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，再次按下【新增】鈕。（如圖 11-215）

圖 11-215IPSec 自動加密頁面

步驟13. 【名稱】輸入 VPN_02、【連線介面】選擇 Port3（WAN2）。（如圖 11-216）

圖 11-216 設定 IPSec 名稱和外部網路介面

步驟14. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的甲公司閘道 WAN2 IP 位址。（如圖 11-217）

圖 11-217 設定 IPSec 到目的位址

步驟15. 【認證方法】選擇 RSA Signature、【CA 憑證】選擇 CA_Server_02、【本地授權憑證】選擇 Site_B_02、【遠端授權憑證】選擇 Site_B_01。（如圖 11-218）

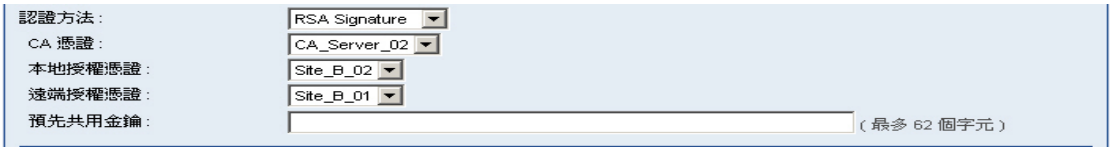


圖 11-218 設定 IPSec 認證方法

步驟16. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-219）

圖 11-219 設定 ISAKMP 演算法

步驟17. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-220）

圖 11-220 設定 IPSec 演算法

步驟18. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-221）

圖 11-221 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟19. 在【GRE/IPSec】欄位中，【GRE 本地端 IP】輸入 192.168.60.200、【GRE 遠端 IP】輸入 192.168.60.100。（如圖 11-222）

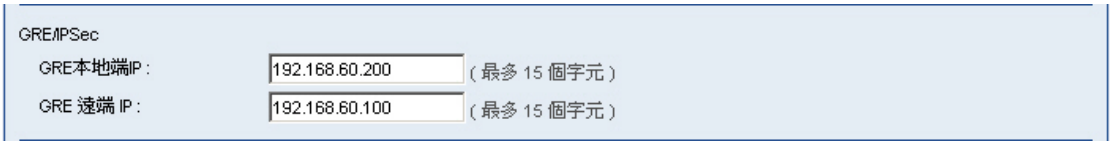


圖 11-222 設定 GRE/IPSec

步驟20. 完成 VPN_02 IPSec 自動加密設定。（如圖 11-223）

圖 11-223 完成 VPN_02 IPSec 自動加密設定

步驟21. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-224）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 將【可選取的通道】VPN_01、VPN_02 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-225）

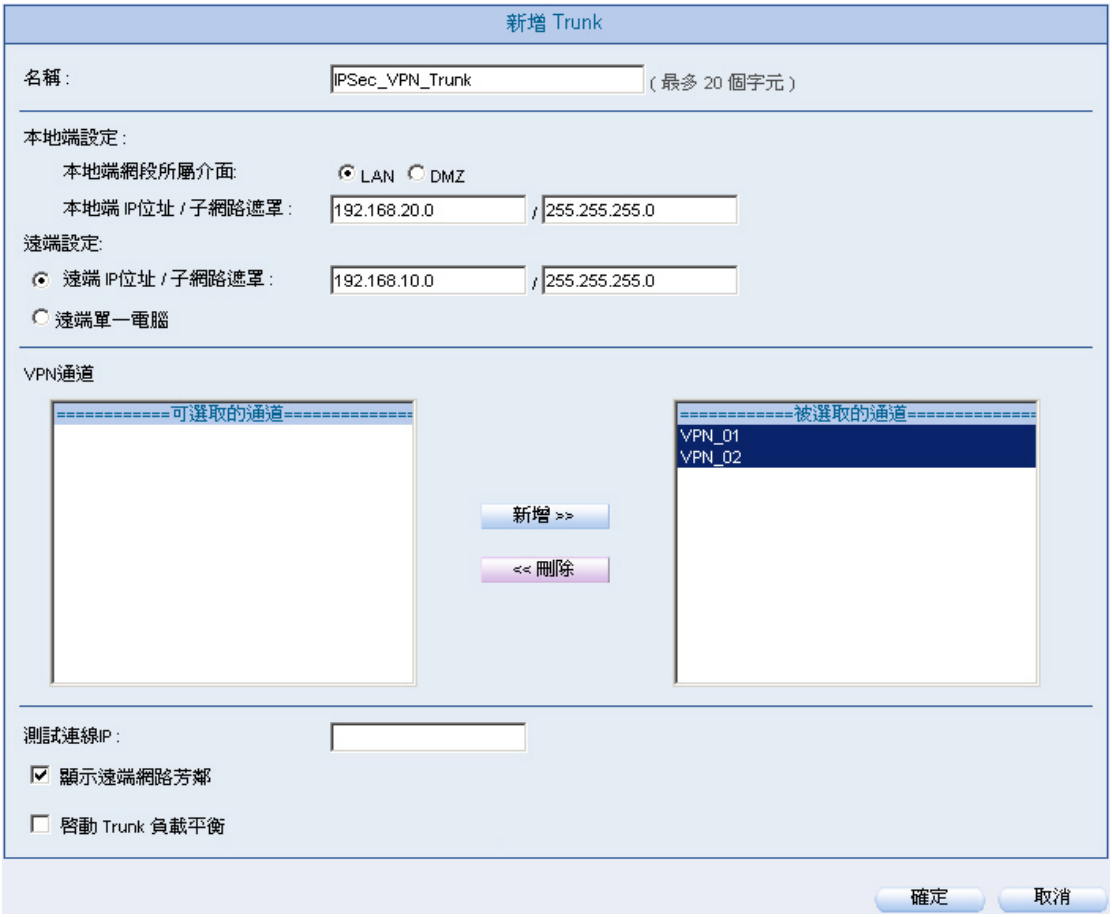


圖 11-224 設定 Trunk

圖 11-225 完成 Trunk 設定

步驟22. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-226）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-227）

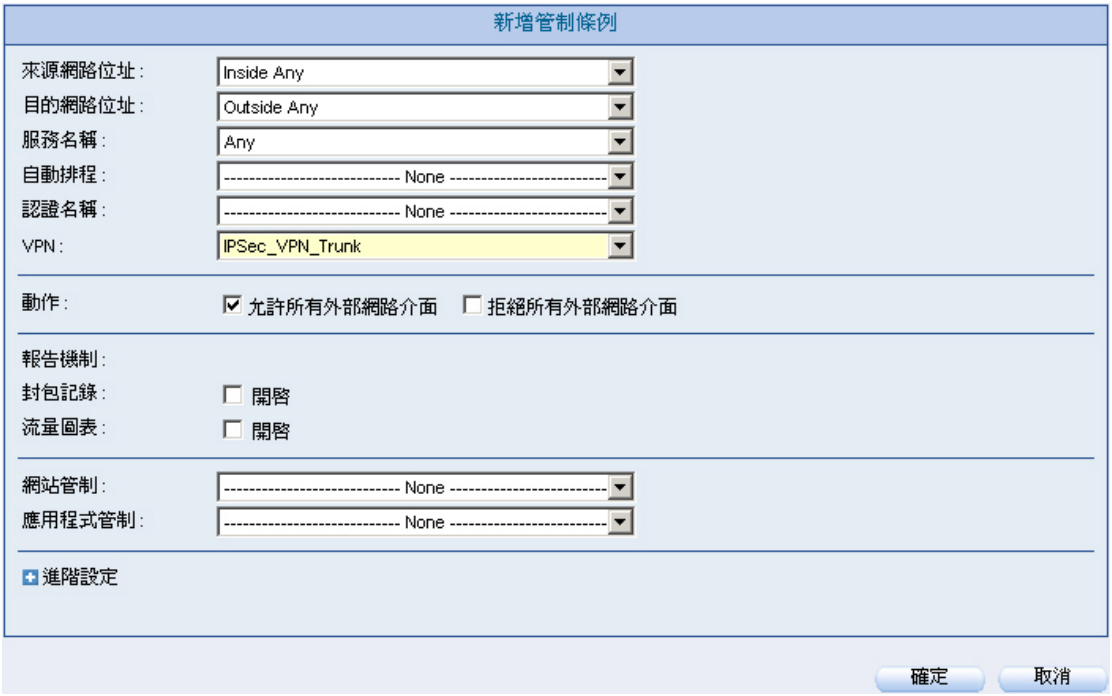


圖 11-226 設定 VPN Trunk 內部至外部之管制條例

圖 11-227 完成管制條例設定

步驟23. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-228）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-229）

圖 11-228 設定 VPN Trunk 外部至內部之管制條例

圖 11-229 完成管制條例設定

步驟24. 完成 IPSec VPN 連線。（如圖 11-230）

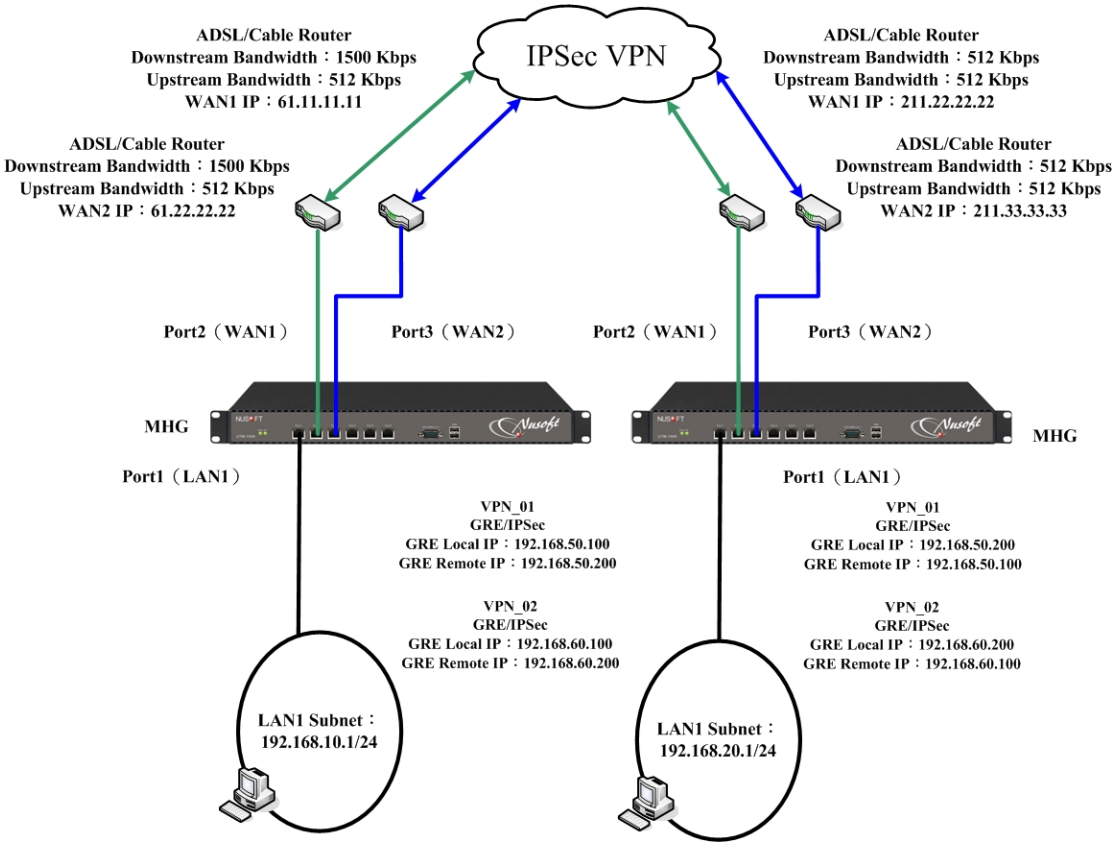


圖 11-230IPSec VPN 連線環境

11.1.5 使用三台 MHG-2000 設定 IPSec VPN Hub 連線的方法

環境設定

甲公司 Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

乙公司 Port1 設為 LAN1（192.168.20.1）為 192.168.20.x/24 網段。

Port2 設為 WAN1（211.22.22.22）和 ATU-R 對接，連上網際網路。

丙公司 Port1 設為 LAN1（192.168.30.1）為 192.168.30.x/24 網段。

Port2 設為 WAN1（121.33.33.33）和 ATU-R 對接，連上網際網路。

本範例以三台 MHG-2000 做為平台操作，乙公司和丙公司透過與甲公司建立的 VPN（虛擬私人網路）連線彼此互傳資料。

甲公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 11-231）

圖 11-231IPSec 自動加密頁面

步驟2. 【名稱】輸入 VPN_01、【連線介面】選擇 Port2（WAN1）。（如圖 11-232）

圖 11-232 設定 IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的乙公司閘道位址。（如圖 11-233）

圖 11-233 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-234）

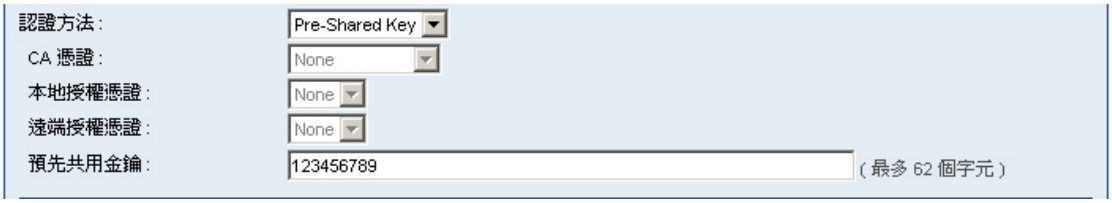


圖 11-234 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-235）

圖 11-235 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-236）

圖 11-236 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-237）

圖 11-237 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟8. 完成 VPN_01 IPSec 自動加密設定。（如圖 11-238）

圖 11-238 完成 VPN_01 IPSec 自動加密設定

步驟9. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-239）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.0.0/255.255.0.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 將【可選取的通道】VPN_01 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-240）

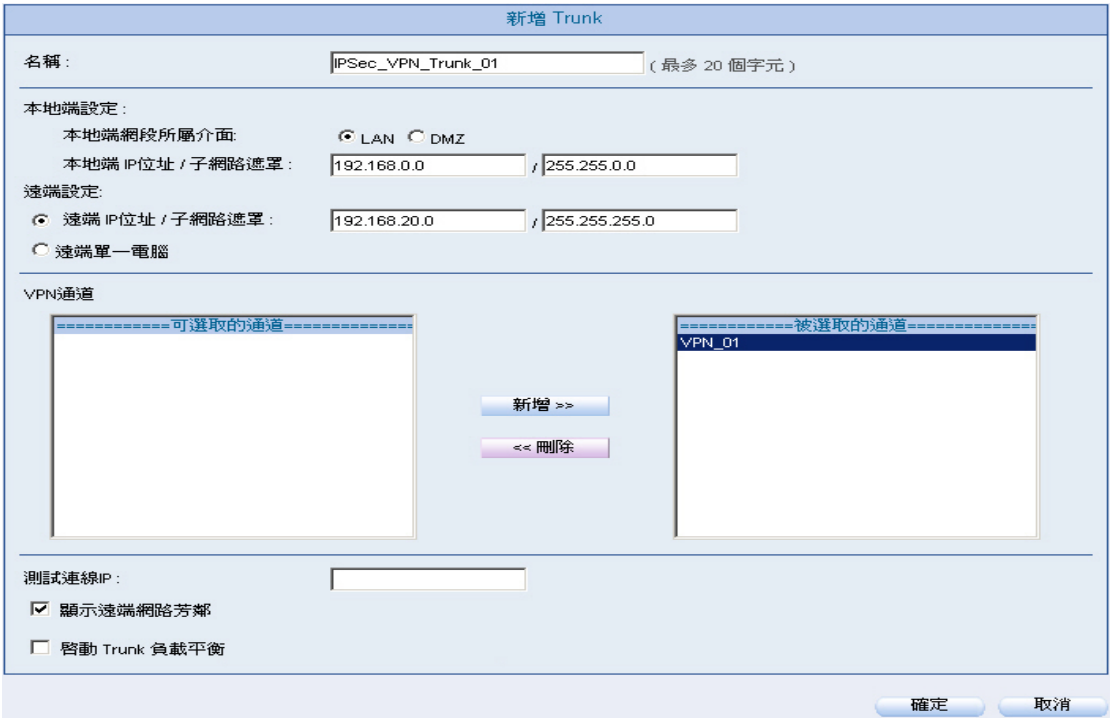


圖 11-239 設定第一筆 Trunk

圖 11-240 完成第一筆 Trunk 設定

步驟10. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，再次按下【新增】鈕。（如圖 11-241）

圖 11-241IPSec 自動加密頁面

步驟11. 【名稱】輸入 VPN_02、【連線介面】選擇 Port2（WAN1）。（如圖 11-242）

圖 11-242 設定 IPSec 名稱和外部網路介面

步驟12. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的丙公司閘道位址。（如圖 11-243）

圖 11-243 設定 IPSec 到目的位址

步驟13. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-244）

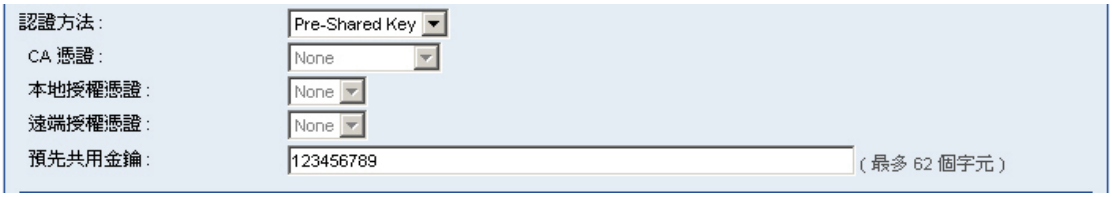


圖 11-244 設定 IPSec 認證方法

步驟14. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-245）

圖 11-245 設定 ISAKMP 演算法

步驟15. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-246）

圖 11-246 設定 IPSec 演算法

步驟16. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-247）

圖 11-247 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟17. 完成 VPN_02 IPSec 自動加密設定。（如圖 11-248）

圖 11-248 完成 VPN_02 IPSec 自動加密設定

步驟18. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-249）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.0.0/255.255.0.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入丙公司的子網路 192.168.30.0/255.255.255.0。
- 將【可選取的通道】VPN_02 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-250）

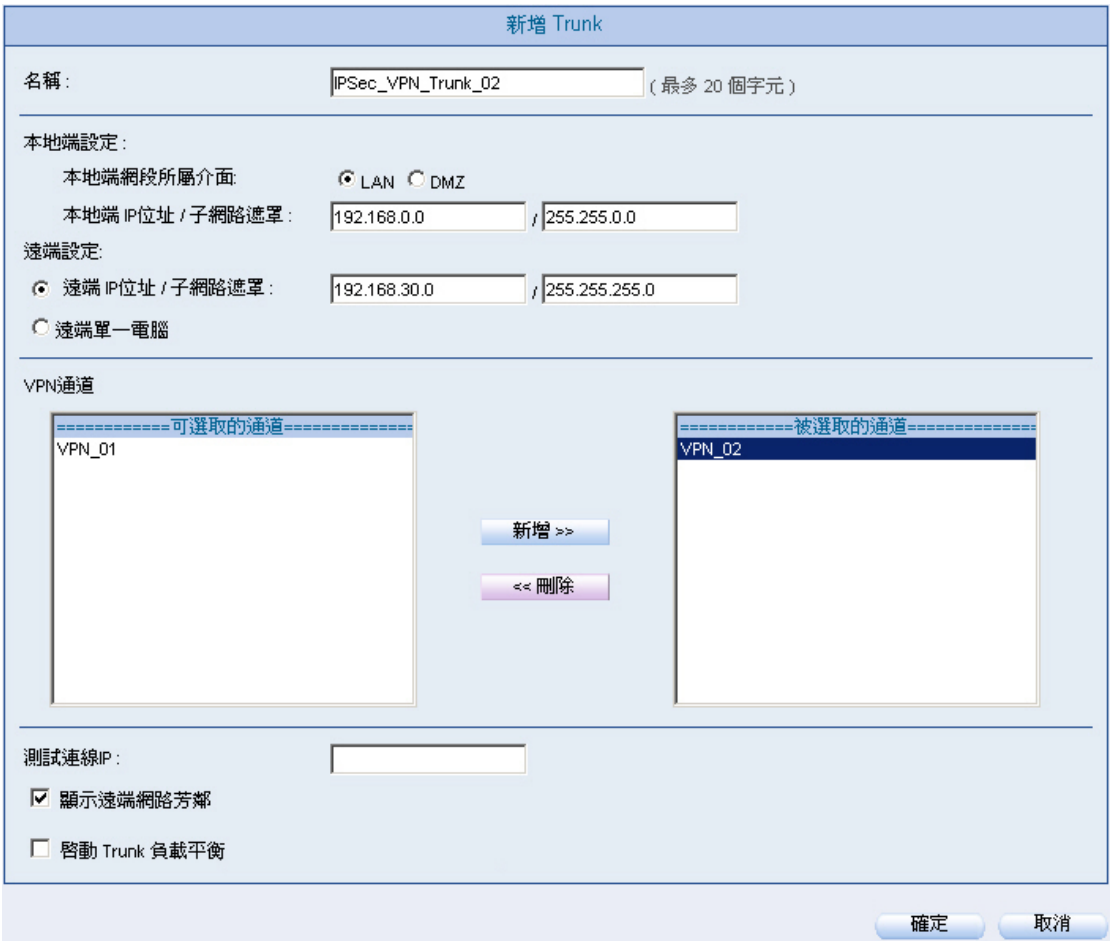


圖 11-249 設定第二筆 Trunk

圖 11-250 完成第二筆 Trunk 設定

步驟19. 在【管制條例選項】>【VPN】>【Trunk 群組】頁面中，做下列設定：（如圖 11-251）

- 輸入所指定的 Trunk 群組【名稱】。
- 將【可選取的 Trunk】IPSec_VPN_Trunk_01（LAN）、IPSec_VPN_Trunk_02（LAN）新增至【被選取的 Trunk】清單中。
- 按下【確定】鈕，完成設定。（如圖 11-252）

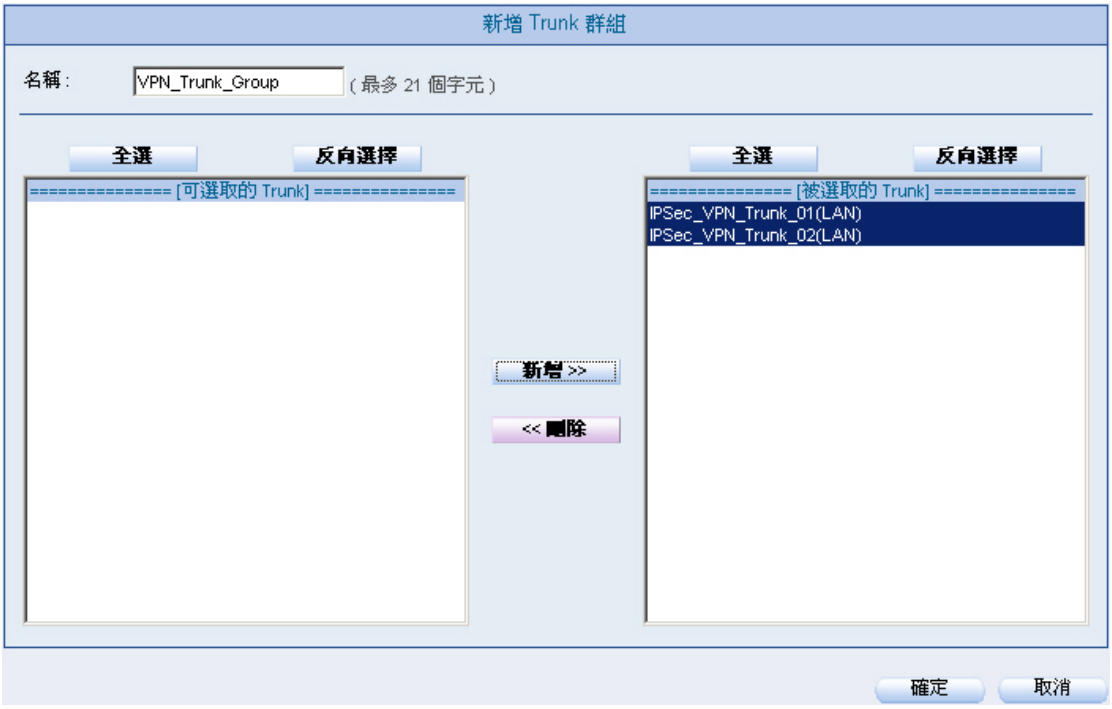


圖 11-251 設定 Trunk 群組

圖 11-252 完成 Trunk 群組設定

注意：

1. 在進行【管制條例選項】>【VPN】>【Trunk】設定時，做為 VPN Hub（甲公司）的網段要包含到各分點（乙公司、丙公司）的網段。

步驟20. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-253）

- 【VPN】選擇所設定的 Trunk 群組規則。
- 按下【確定】鈕，完成設定。（如圖 11-254）

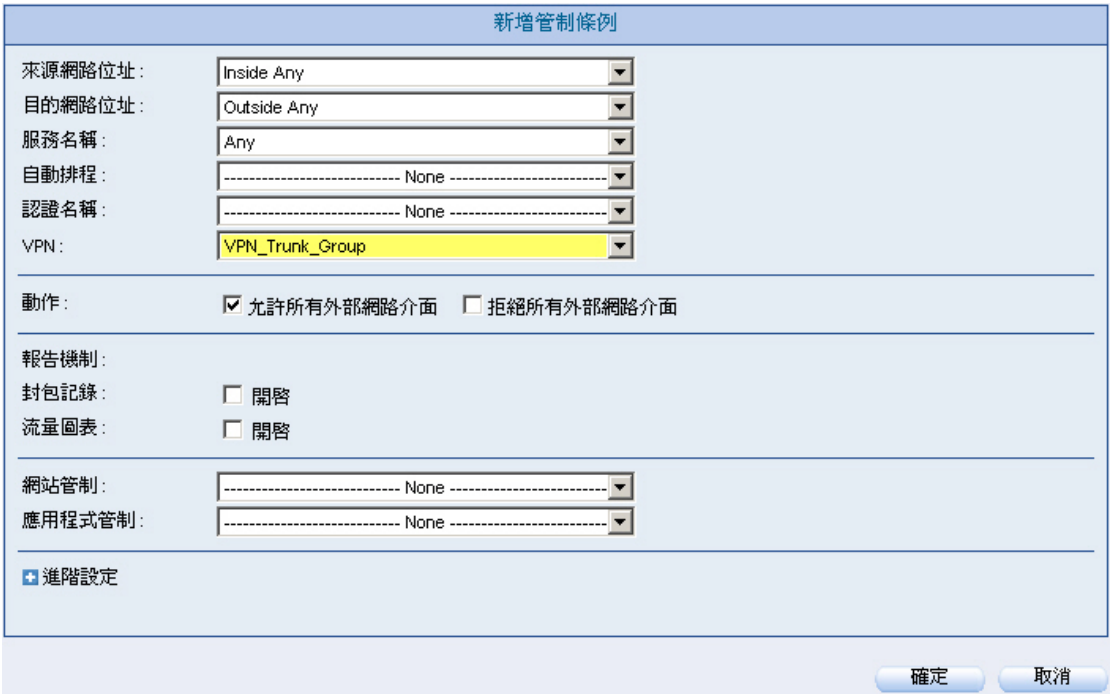


圖 11-253 設定 VPN Trunk 群組內部至外部之管制條例

圖 11-254 完成管制條例設定

步驟21. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-255）

- 【VPN】選擇所設定的 Trunk 群組規則。
- 按下【確定】鈕，完成設定。（如圖 11-256）

圖 11-255 設定 VPN Trunk 群組外部至內部之管制條例

圖 11-256 完成管制條例設定

乙公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 11-257）

圖 11-257IPSec 自動加密頁面

步驟2. 【名稱】輸入 VPN_01、【連線介面】選擇 Port2（WAN1）。（如圖 11-258）

圖 11-258 設定 IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的甲公司閘道位址。（如圖 11-259）

圖 11-259 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-260）

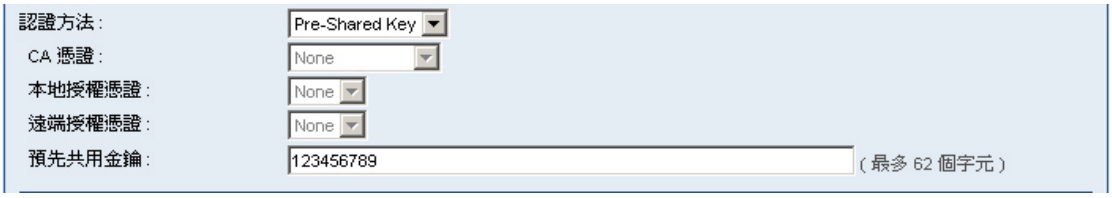


圖 11-260 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-261）

圖 11-261 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-262）

圖 11-262 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-263）

圖 11-263 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟8. 完成 IPSec 自動加密設定。（如圖 11-264）

圖 11-264 完成 IPSec 自動加密設定

步驟9. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-265）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲公司的子網路 192.168.0.0/255.255.0.0。
- 將【可選取的通道】VPN_01 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-266）

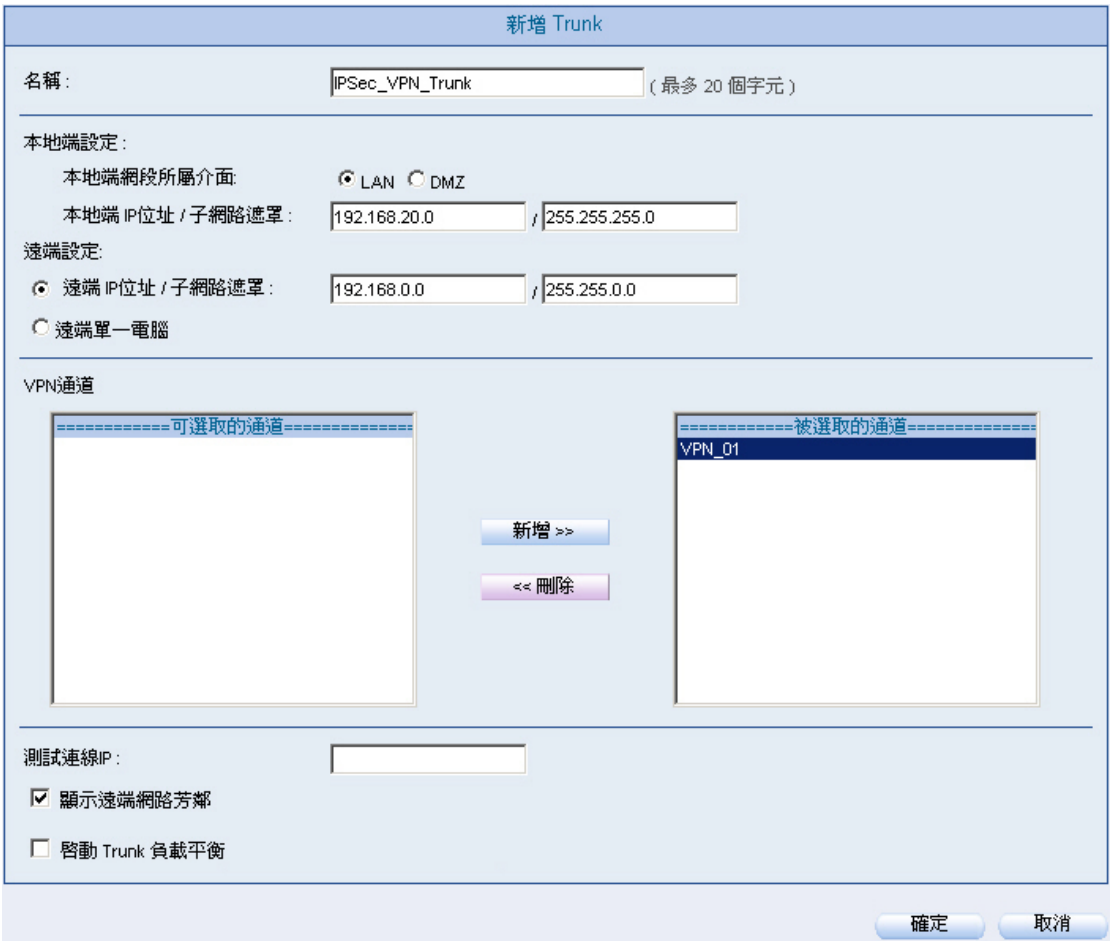


圖 11-265 設定 Trunk

圖 11-266 完成 Trunk 設定

步驟10. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-267）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-268）

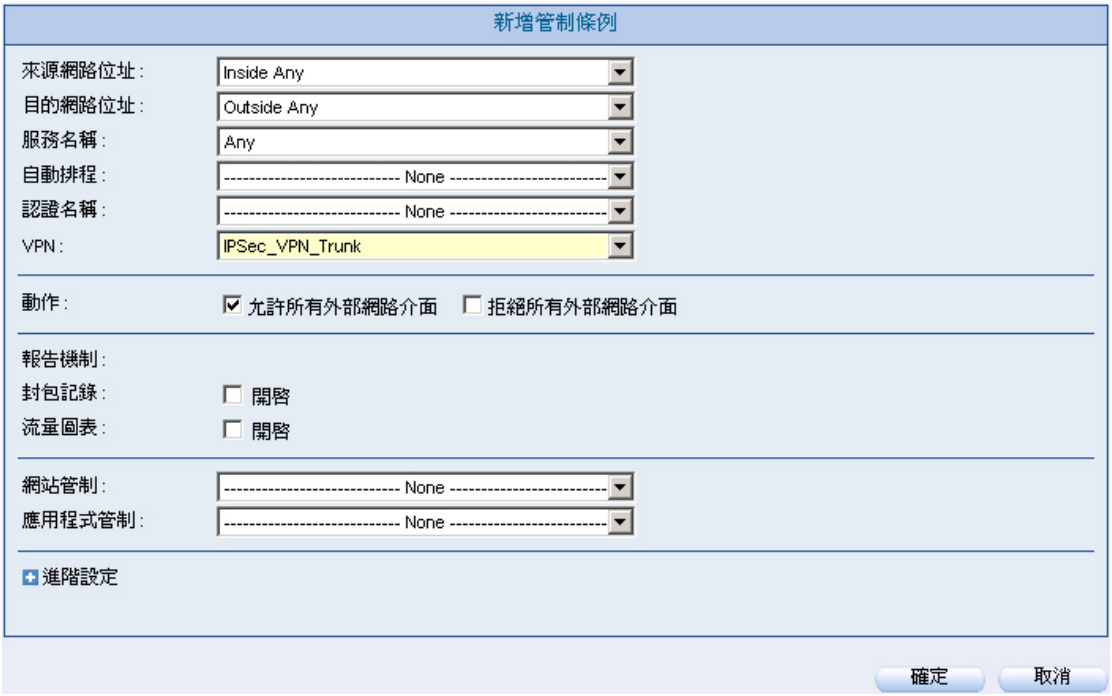


圖 11-267 設定 VPN Trunk 內部至外部之管制條例

圖 11-268 完成管制條例設定

步驟11. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-269）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-270）

圖 11-269 設定 VPN Trunk 外部至內部之管制條例

圖 11-270 完成管制條例設定

丙公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 11-271）

圖 11-271IPSec 自動加密頁面

步驟2. 【名稱】輸入 VPN_02、【連線介面】選擇 Port2（WAN1）。（如圖 11-272）

圖 11-272 設定 IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的甲公司閘道位址。（如圖 11-273）

圖 11-273 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 11-274）

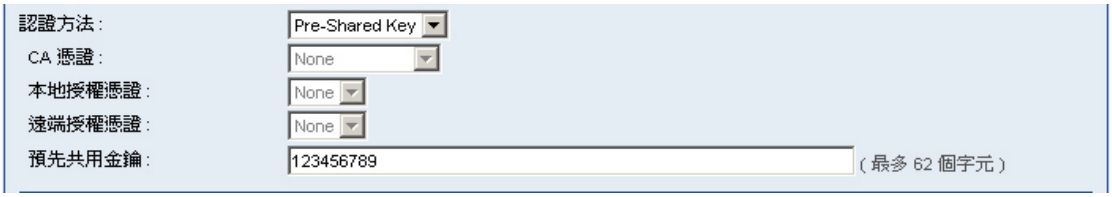


圖 11-274 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 11-275）

圖 11-275 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。（如圖 11-276）

圖 11-276 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。（如圖 11-277）

圖 11-277 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟8. 完成 IPSec 自動加密設定。（如圖 11-278）

圖 11-278 完成 IPSec 自動加密設定

步驟9. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-279）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入丙公司的子網路 192.168.30.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲公司的子網路 192.168.0.0/255.255.0.0。
- 將【可選取的通道】VPN_02 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-280）

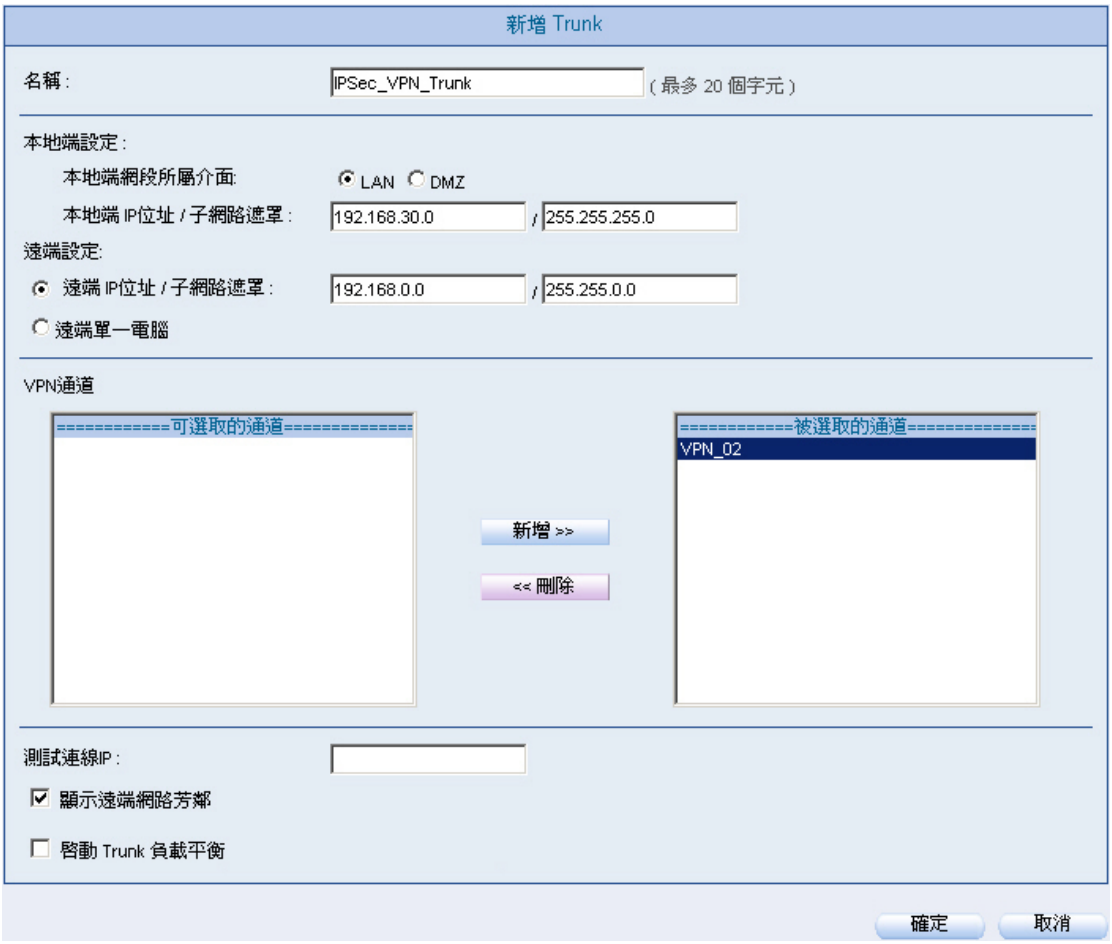


圖 11-279 設定 Trunk

圖 11-280 完成 Trunk 設定

步驟10. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-281）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-282）

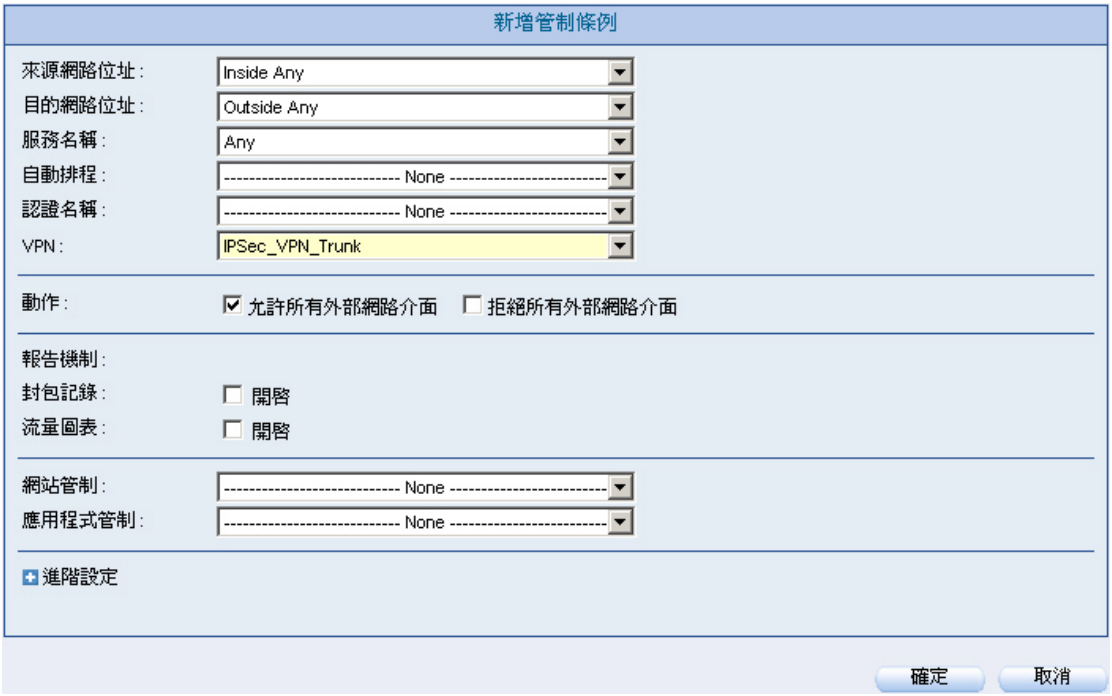


圖 11-281 設定 VPN Trunk 內部至外部之管制條例

圖 11-282 完成管制條例設定

步驟11. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-283）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-284）

圖 11-283 設定 VPN Trunk 外部至內部之管制條例

圖 11-284 完成管制條例設定

步驟12. 完成 IPSec VPN 連線。（如圖 11-285）

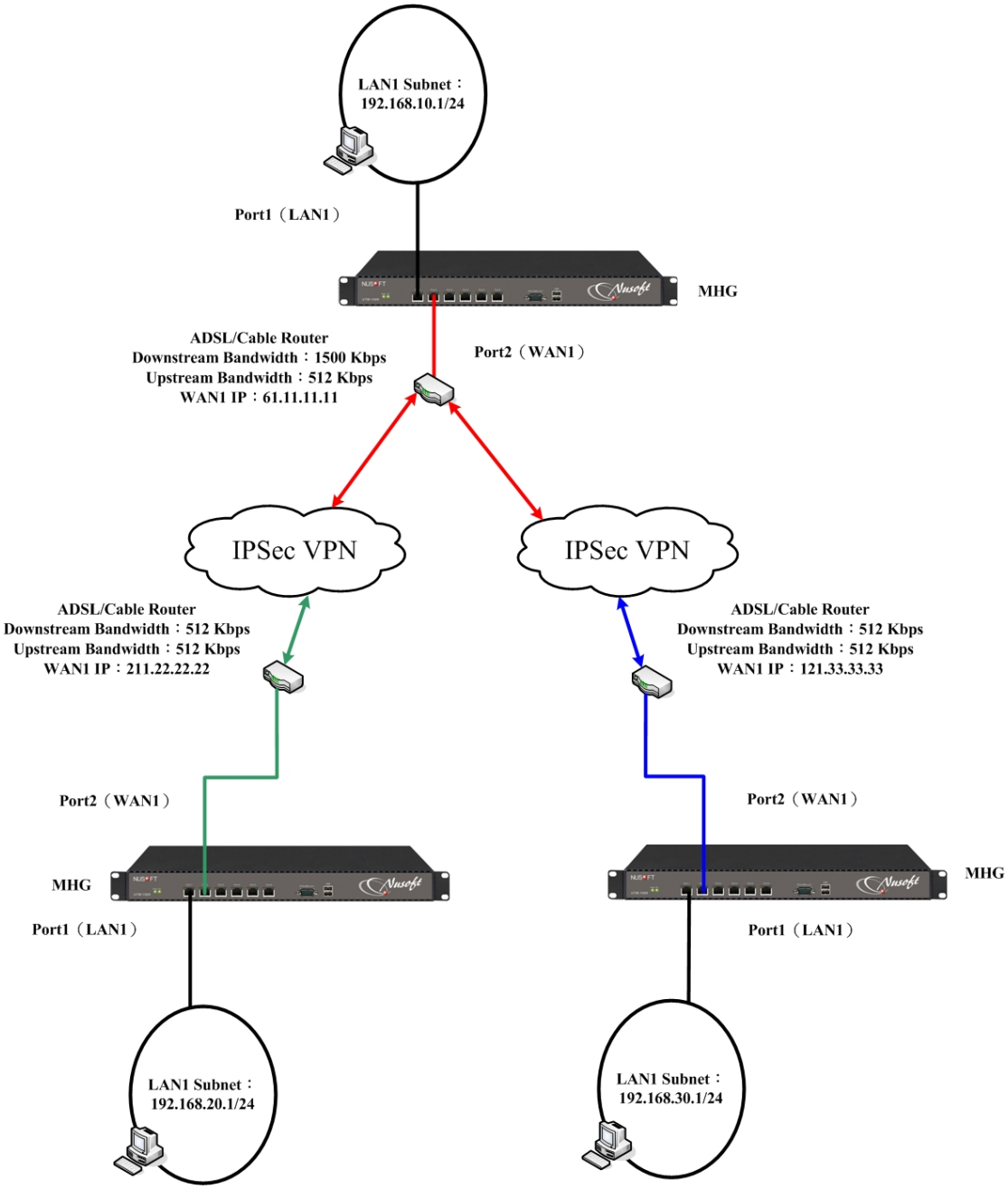


圖 11-285IPSec VPN 連線環境

11.1.6 使用兩台 MHG-2000 設定 PPTP VPN 的 OutBound Load Balance 連線方法

環境設定

甲公司 Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

Port3 設為 WAN2（61.22.22.22）和 ATU-R 對接，連上網際網路。

乙公司 Port1 設為 LAN1（192.168.20.1）為 192.168.20.x/24 網段。

Port2 設為 WAN1（211.22.22.22）和 ATU-R 對接，連上網際網路。

Port3 設為 WAN2（211.33.33.33）和 ATU-R 對接，連上網際網路。

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

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

本範例以兩台 MHG-2000 做為平台操作，甲公司和乙公司建立 VPN（虛擬私人網路）連線以傳送資料。

甲公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【PPTP 伺服器】頁面中，做下列設定：（如圖 11-286）

- 按下【修改】鈕。
- 勾選【啟動 PPTP 伺服器】。
- 勾選【加密認證】。
- 勾選允許 PPTP 用戶端連上網際網路的外部網路介面。
- 【閒置】時間輸入 0。
- 輸入指定的用戶端連線 IP 配發範圍。
- 按下【確定】鈕，完成設定。

圖 11-286 啟動 PPTP 伺服器

說明：

1. 管理員可開放或限制外部使用者，在和 MHG-2000 PPTP 伺服器建立 VPN 連線時，透過 MHG-2000 連上網際網路。
2. 【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）。
3. 透過RADIUS伺服器（設定方式可參照 第 8 章 RADIUS認證功能使用範例）進行PPTP VPN連線認證，要於【管制條例選項】>【VPN】>【PPTP伺服器】新增一條【連線驗證帳戶類型】為RADIUS伺服器的連線規則，以供用戶端認證連線。

步驟2. 在【管制條例選項】>【VPN】>【PPTP 伺服器】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 11-287）
- 【連線驗證帳戶類型】選擇本地端。
- 輸入指定的【使用者名稱】輸入 PPTP_01。
- 【密碼】輸入 123456789。
- 【用戶端連線時所配發的 IP 位址】選擇使用配給的 IP 範圍。
- 按下【確定】鈕。（如圖 11-288）
- 再次按下【新增】鈕。（如圖 11-289）
- 【連線驗證帳戶類型】選擇本地端。
- 【使用者名稱】輸入 PPTP_02。
- 【密碼】輸入 987654321。
- 【用戶端連線時所配發的 IP 位址】選擇使用配給的 IP 範圍。
- 按下【確定】鈕，完成設定。（如圖 11-290）

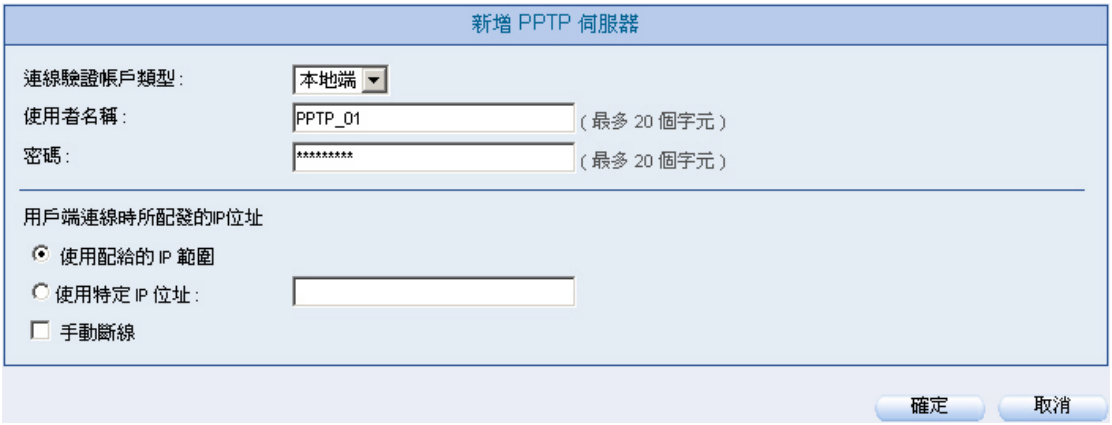


圖 11-287 設定第一條 PPTP 伺服器連線規則

圖 11-288 完成第一條 PPTP 伺服器連線規則設定

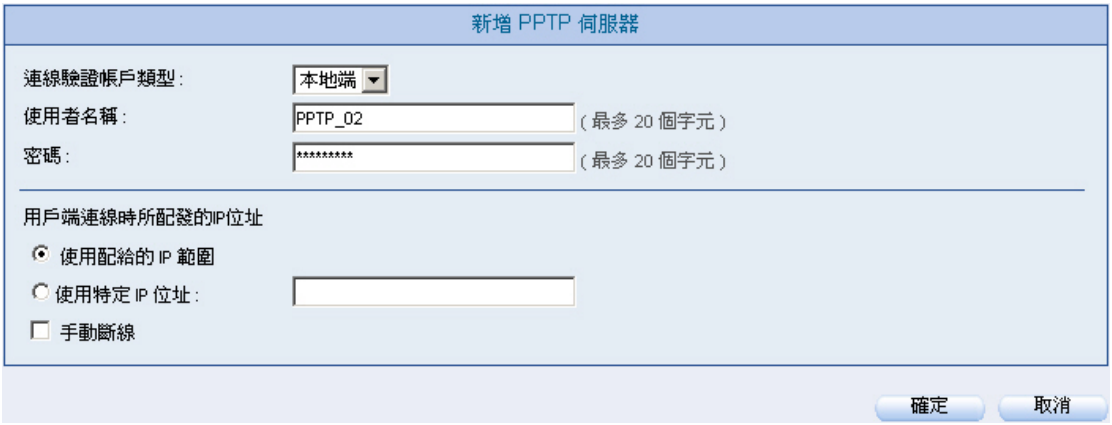


圖 11-289 設定第二條 PPTP 伺服器連線規則

圖 11-290 完成第二條 PPTP 伺服器連線規則設定

說明：

1. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 MHG-2000【PPTP 伺服器】使用者設定錯亂時，可清除清單內容重新【匯入】。

步驟3. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-291）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 將【可選取的通道】PPTP_Server_PPTP_01 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-292）

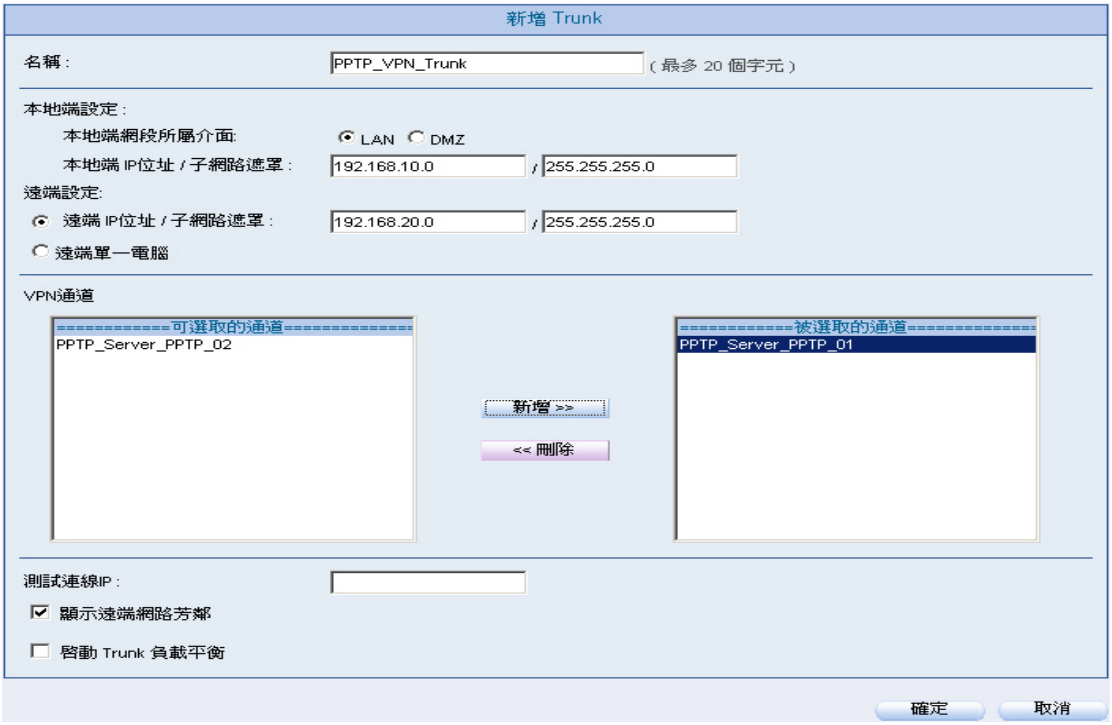


圖 11-291 設定 Trunk

圖 11-292 完成 Trunk 設定

說明：

1. 當【遠端設定】選擇遠端 IP 位址/子網路遮罩時，僅需新增一條 PPTP_Server 通道，即可達到 PPTP VPN Trunk 的連線需求。

步驟4. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-293）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-294）

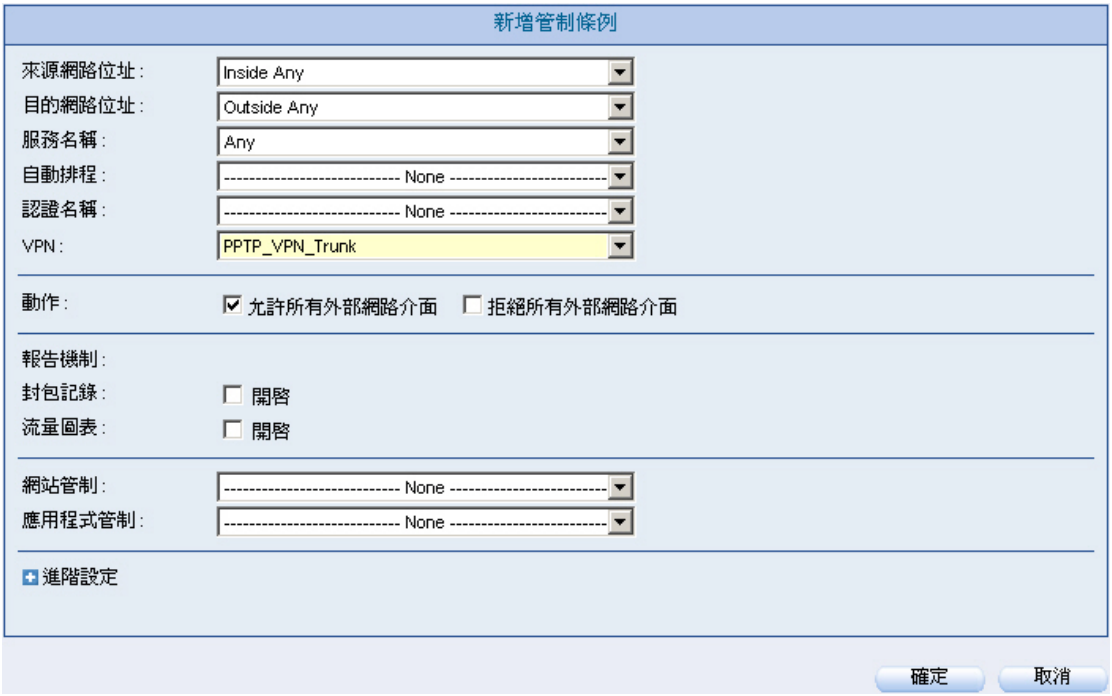


圖 11-293 設定 VPN Trunk 內部至外部之管制條例

圖 11-294 完成管制條例設定

步驟5. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-295）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-296）

圖 11-295 設定 VPN Trunk 外部至內部之管制條例

圖 11-296 完成管制條例設定

乙公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【PPTP 用戶端】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 11-297）
- 【使用者名稱】輸入 PPTP_01。
- 【密碼】輸入 123456789。
- 【伺服器 IP 位址 / 網域名稱】輸入所要連線的甲公司閘道 WAN1 IP 位址。
- 勾選【加密認證】。
- 【連線介面】選擇 Port2（WAN1）。
- 按下【確定】鈕。（如圖 11-298）
- 再次按下【新增】鈕。（如圖 11-299）
- 【使用者名稱】輸入 PPTP_02。
- 【密碼】輸入 987654321。
- 【伺服器 IP 位址 / 網域名稱】輸入所要連線的甲公司閘道 WAN2 IP 位址。
- 勾選【加密認證】。
- 【連線介面】選擇 Port3（WAN2）。
- 按下【確定】鈕，完成設定。（如圖 11-300）

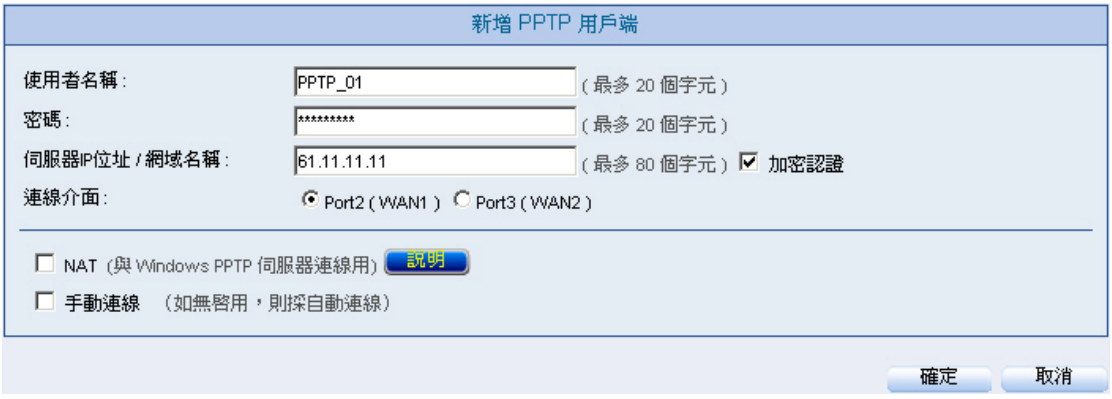


圖 11-297 設定第一條 PPTP 用戶端連線規則

圖 11-298 完成第一條 PPTP 用戶端連線規則設定

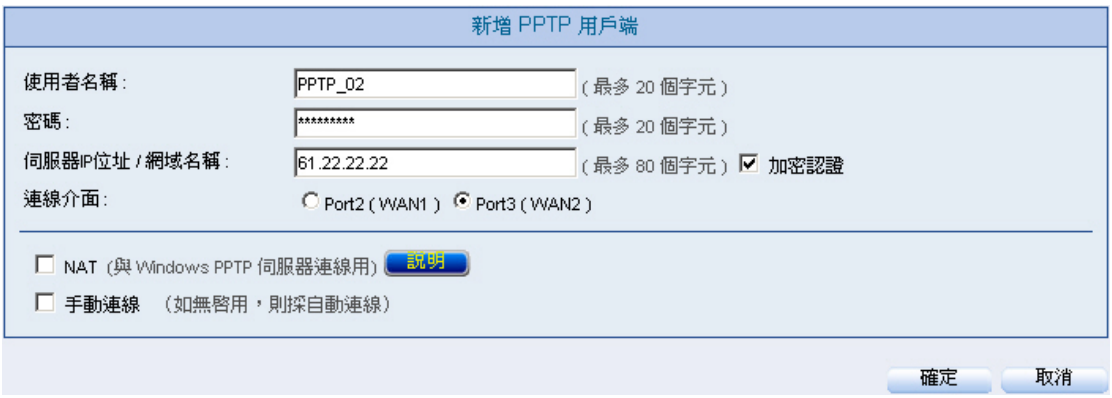


圖 11-299 設定第二條 PPTP 用戶端連線規則

圖 11-300 完成第二條 PPTP 用戶端連線規則設定

說明：

1. 從 MHG-2000 之 PPTP 用戶端欲透過 MHG-2000 之 PPTP 伺服器連線至網際網路、其所建立的 IPSec VPN 網段時，要勾選【NAT(與 Windows PPTP 伺服器連線用)】，將 PPTP 用戶端內部 PC 之 IP 位址轉為 PPTP 伺服器所配發的特定網段 IP 位址。

步驟2. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-301）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 將【可選取的通道】PPTP_Client_PPTP_01（61.11.11.11）、PPTP_Client_PPTP_02（61.22.22.22）新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-302）

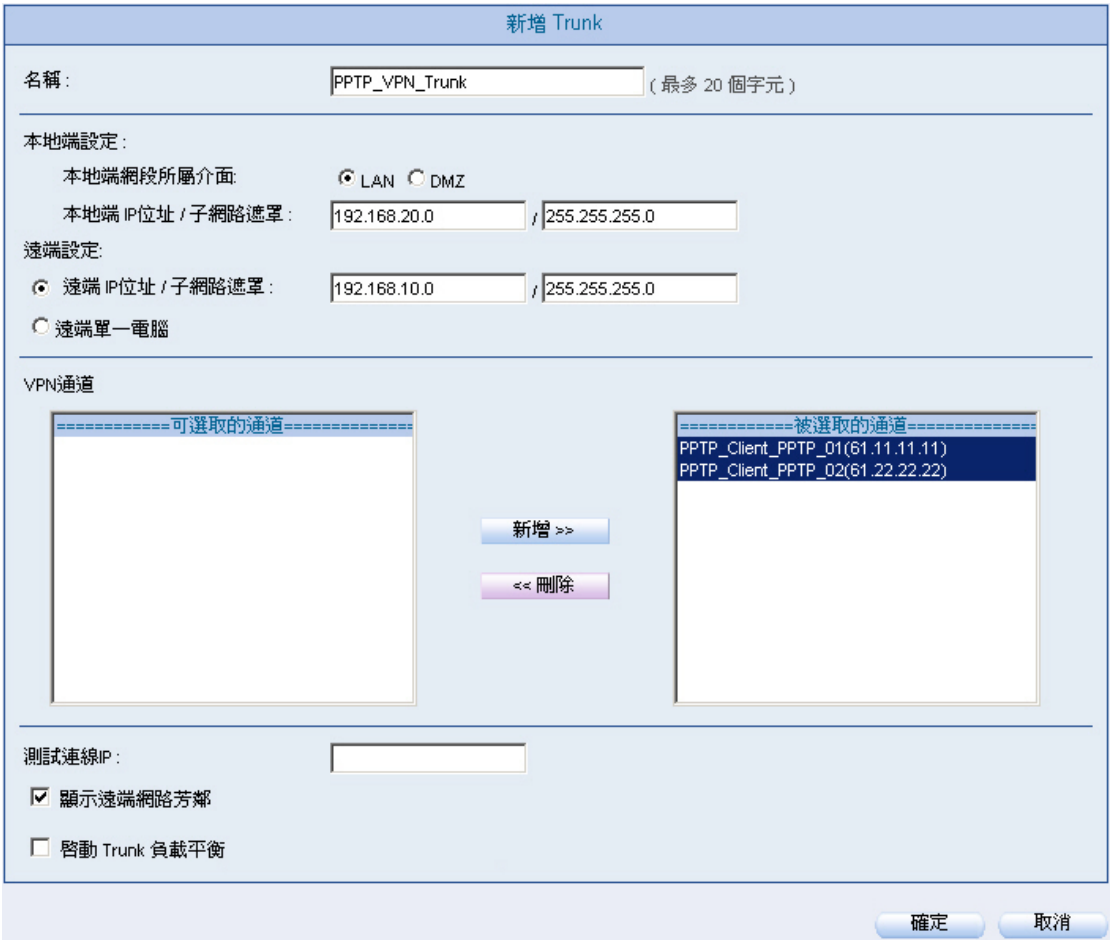


圖 11-301 設定 Trunk

圖 11-302 完成 Trunk 設定

說明：

1. 當【遠端設定】選擇遠端 IP 位址/子網路遮罩時，依照外部網路介面數，決定可新增的 PPTP_Client 通道數，以達到 PPTP VPN Trunk 的連線需求。

步驟3. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-303）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-304）

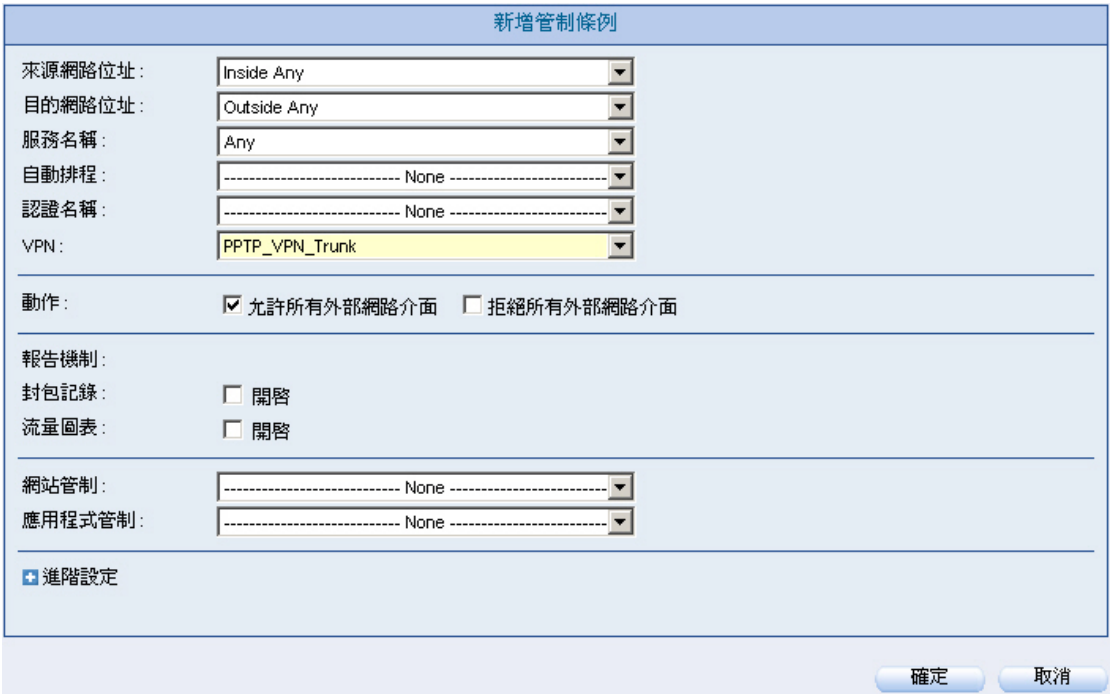


圖 11-303 設定 VPN Trunk 內部至外部之管制條例

圖 11-304 完成管制條例設定

步驟4. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-305）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-306）

圖 11-305 設定 VPN Trunk 外部至內部之管制條例

圖 11-306 完成管制條例設定

步驟5. 完成 PPTP VPN 連線。（如圖 11-307）

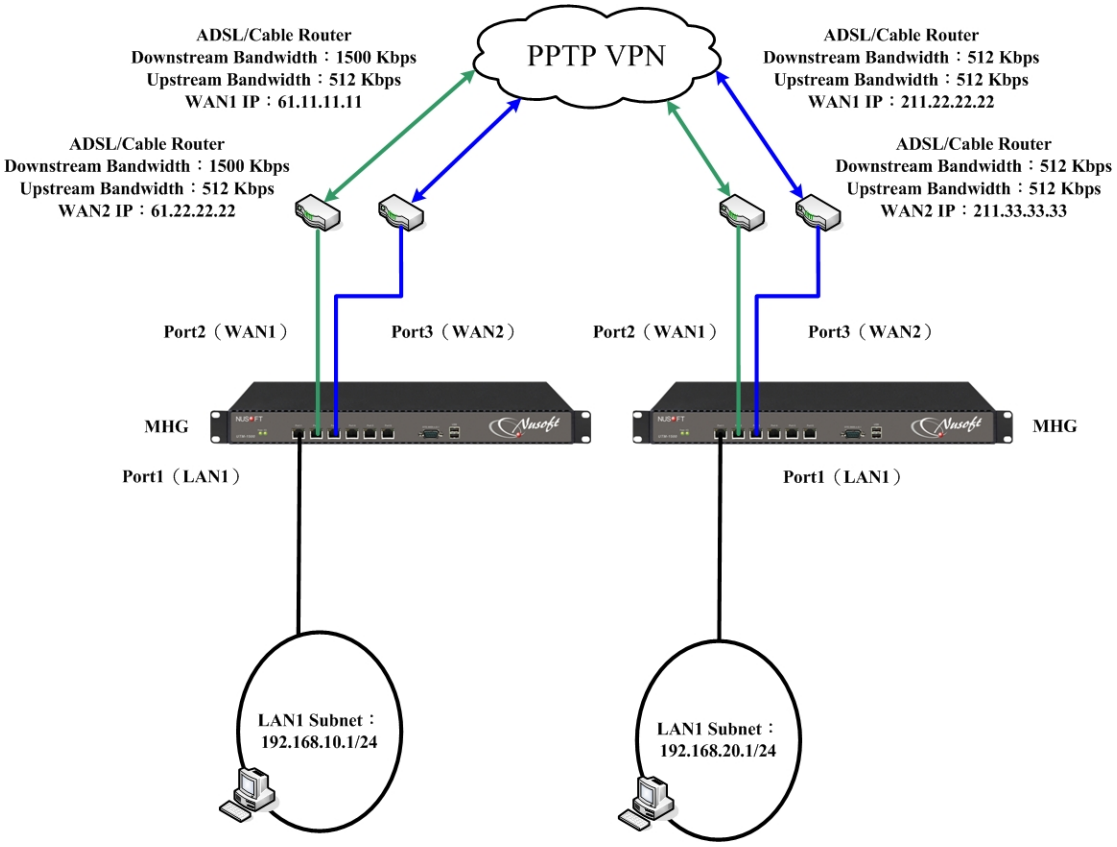


圖 11-307PPTP VPN 連線環境

11.1.7 使用兩台 MHG-2000 設定 PPTP VPN 用戶端透過伺服器端連上網際網路的方法

環境設定

甲公司 Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

乙公司 Port1 設為 LAN1（192.168.20.1）為 192.168.20.x/24 網段。

Port2 設為 WAN1（211.22.22.22）和 ATU-R 對接，連上網際網路。

本範例以兩台 MHG-2000 做為平台操作，乙公司（客戶端）透過和甲公司（伺服器端）建立的 VPN（虛擬私人網路）連線連上網際網路。

甲公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【PPTP 伺服器】頁面中，做下列設定：（如圖 11-308）

- 按下【修改】鈕。
- 勾選【啟動 PPTP 伺服器】。
- 勾選【加密認證】。
- 勾選允許 PPTP 用戶端連上網際網路的外部網路介面。
- 【閒置】時間輸入 0。
- 輸入指定的用戶端連線 IP 配發範圍。
- 按下【確定】鈕，完成設定。

圖 11-308 啟動 PPTP 伺服器

步驟2. 在【管制條例選項】>【VPN】>【PPTP 伺服器】頁面中，做下列設定：（如圖 11-309）

- 【連線驗證帳戶類型】選擇本地端。
- 【使用者名稱】輸入 PPTP_Connection。
- 【密碼】輸入 123456789。
- 【用戶端連線時所配發的 IP 位址】選擇使用配給的 IP 範圍。
- 按下【確定】鈕，完成設定。（如圖 11-310）

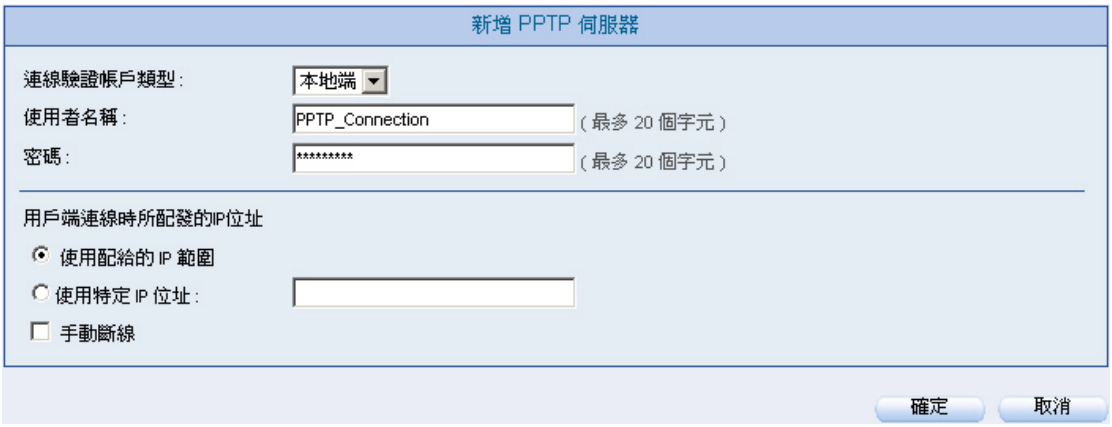


圖 11-309 設定 PPTP 伺服器連線規則

圖 11-310 完成 PPTP 伺服器連線規則設定

乙公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【PPTP 用戶端】頁面中，做下列設定：（如圖 11-311）

- 【使用者名稱】輸入 PPTP_Connection。
- 【密碼】輸入 123456789。
- 【伺服器 IP 位址 / 網域名稱】輸入所要連線的甲公司閘道 WAN1 IP 位址。
- 勾選【加密認證】。
- 【連線介面】選擇 Port2（WAN1）。
- 勾選【NAT（與 Windows PPTP 伺服器連線用）】。
- 按下【確定】鈕，完成設定。（如圖 11-312）

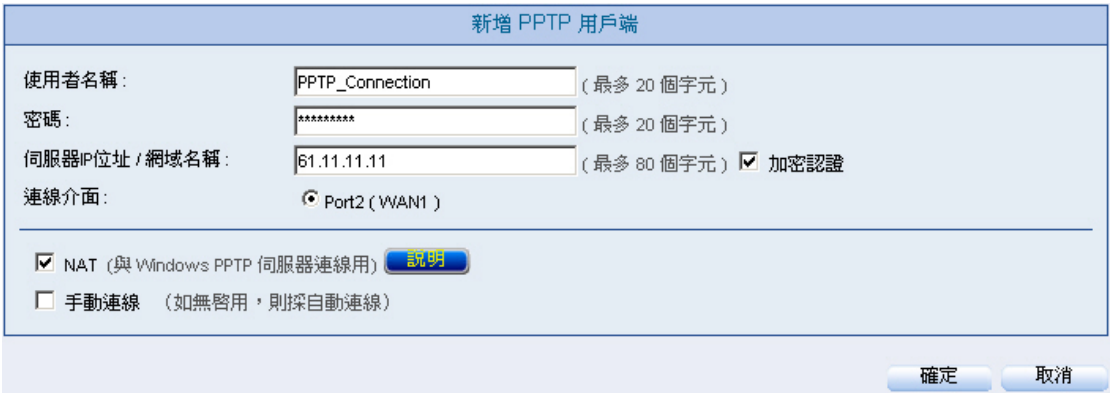


圖 11-311 設定 PPTP 用戶端連線規則

圖 11-312 完成 PPTP 用戶端連線規則設定

說明：

1. 從 MHG-2000 之 PPTP 用戶端建立 VPN 連線至 MHG-2000 之 PPTP 伺服器端時，要勾選【NAT(與 Windows PPTP 伺服器連線用)】，才可使 MHG-2000 之 PPTP 用戶端透過 MHG-2000 之 PPTP 伺服器端連上網際網路。

步驟2. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-313）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入乙公司的子網路 192.168.20.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲公司的子網路 0.0.0.0/0.0.0.0。
- 將【可選取的通道】PPTP_Client_PPTP_Connection(61.11.11.11)新增至【被選取的通道】清單中。
- 按下【確定】鈕，完成設定。（如圖 11-314）

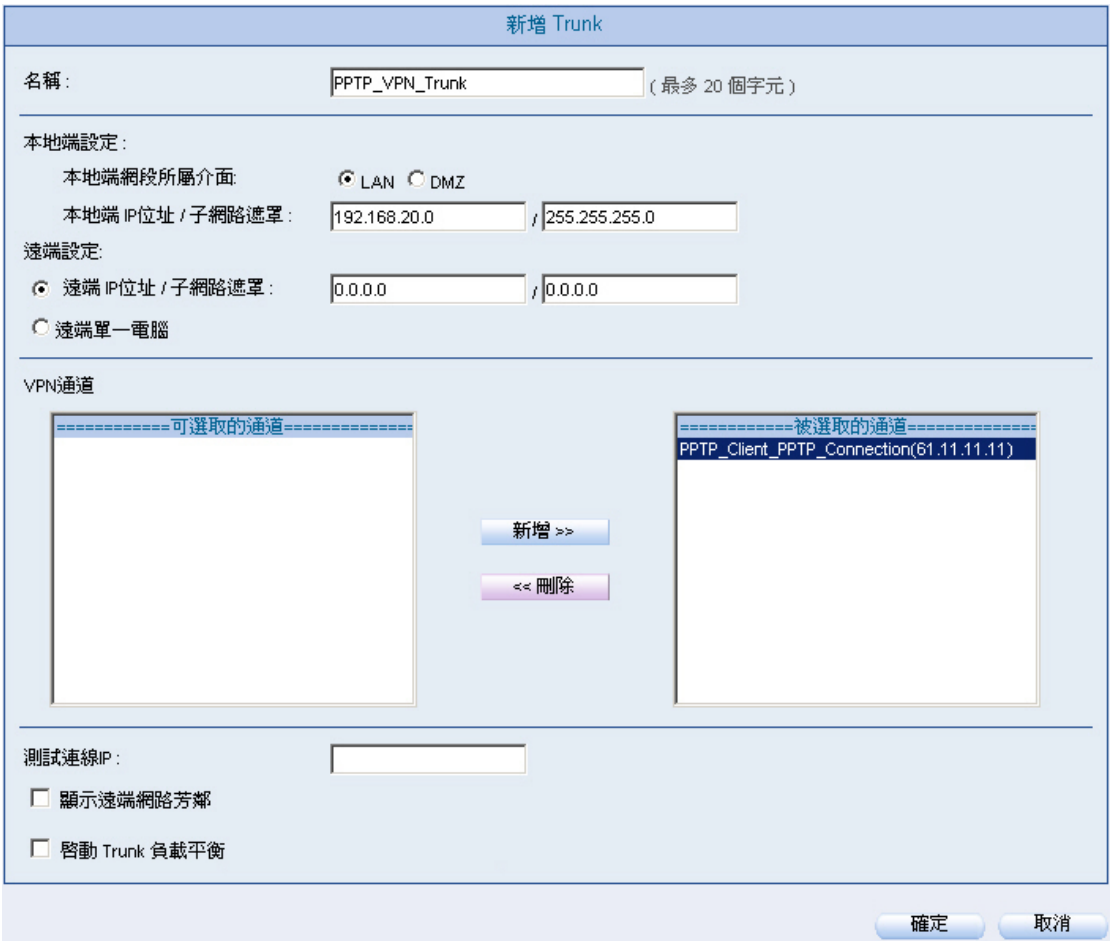


圖 11-313 設定 Trunk

圖 11-314 完成 Trunk 設定

步驟3. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-315）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-316）

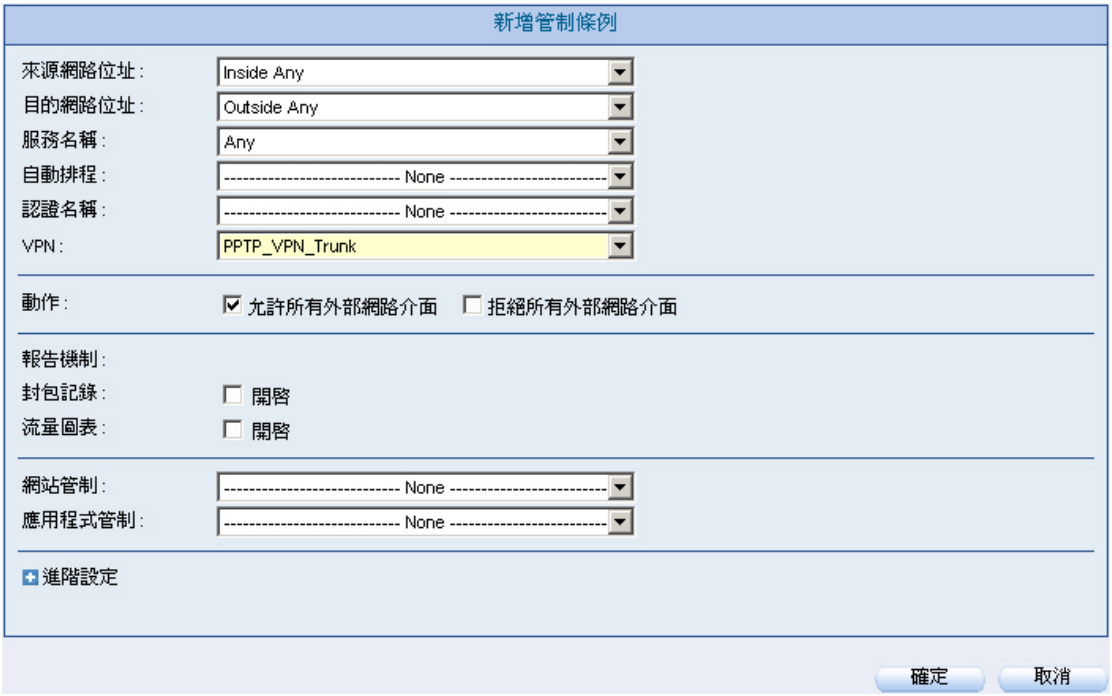


圖 11-315 設定 VPN Trunk 內部至外部之管制條例

圖 11-316 完成管制條例設定

說明：

1. 此時本地端（乙公司）的【Trunk】設定僅需套用至【管制條例】>【內部至外部】。

步驟4. 完成 PPTP VPN 連線。**（如圖 11-317）**

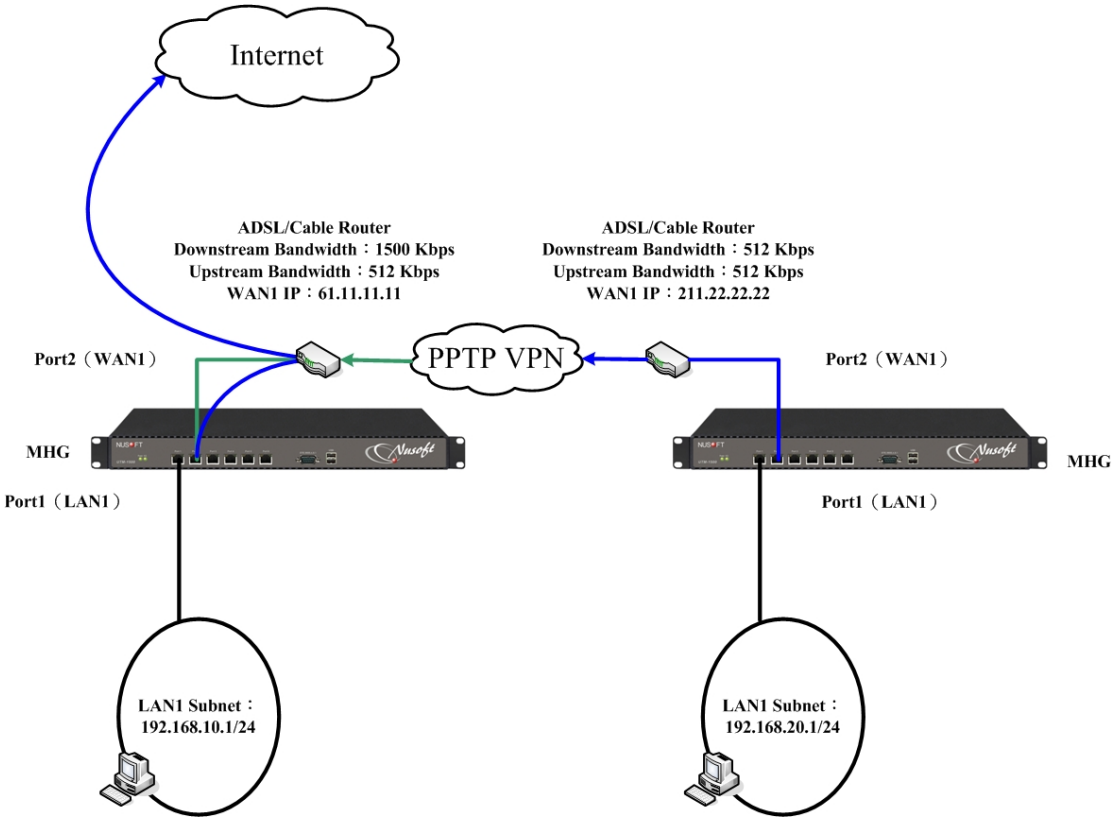


圖 11-317PPTP VPN 連線環境

11.1.8 使用一台 MHG-2000 與 Windows 7 設定 PPTP VPN 連線的方法

環境設定

甲公司使用 MHG-2000。

Port1 設為 LAN1（192.168.10.1）為 192.168.10.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接，連上網際網路。

乙公司使用以 Windows 7 作業之單一 PC，IP 位址為 211.22.22.22。

本範例以一台 MHG-2000 及 Windows 7 作業的 PC 做為平台操作，甲公司和乙公司建立 VPN（虛擬私人網路）連線以傳送資料。

甲公司的設定步驟如下：

步驟1. 在【管制條例選項】>【VPN】>【PPTP 伺服器】頁面中，做下列設定：（如圖 11-318）

- 按下【修改】鈕。
- 勾選【啟動 PPTP 伺服器】。
- 勾選【加密認證】。
- 勾選允許 PPTP 用戶端連上網際網路的外部網路介面。
- 【閒置】時間輸入 0。
- 輸入指定的用戶端連線 IP 配發範圍。
- 按下【確定】鈕，完成設定。

圖 11-318 啟動 PPTP 伺服器

說明：

1. 管理員可開放或限制外部使用者，在和 MHG-2000 PPTP 伺服器建立 VPN 連線時，透過 MHG-2000 連上網際網路。
2. 【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）。
3. 若外部使用者欲透過 PPTP VPN 連線至 MHG-2000 已建立的 IPSec VPN 網段，用戶端連線 IP 配發範圍必須設定和內部網路介面（LAN1）同網段(192.168.10.x/24)且未被使用的 IP；同時，外部使用者必須透過 IPSec VPN 建立連線的介面位址，和 MHG-2000 建立 PPTP VPN 連線。

步驟2. 在【管制條例選項】>【VPN】>【PPTP 伺服器】頁面中，做下列設定：（如圖 11-319）

- 【連線驗證帳戶類型】選擇本地端。
- 【使用者名稱】輸入 PPTP_Connection。
- 【密碼】輸入 123456789。
- 【用戶端連線時所配發的 IP 位址】選擇使用配給的 IP 範圍。
- 按下【確定】鈕，完成設定。（如圖 11-320）

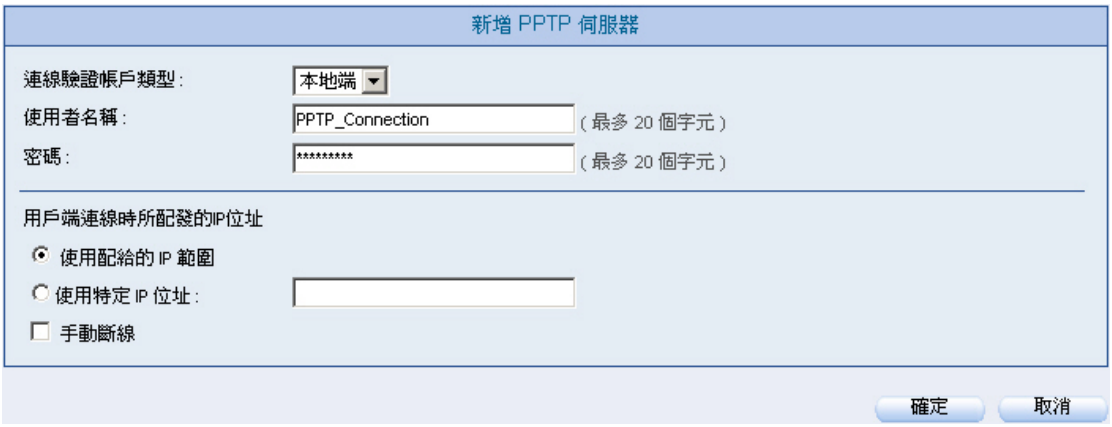


圖 11-319 設定 PPTP 伺服器連線規則

圖 11-320 完成 PPTP 伺服器連線規則設定

步驟3. 在【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 11-321）

- 輸入所指定的 Trunk【名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲公司的子網路 192.168.10.0/255.255.255.0。
- 【遠端設定】選擇遠端單一電腦。
- 將【可選取的通道】PPTP_Server_PPTP_Connection 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 11-322）

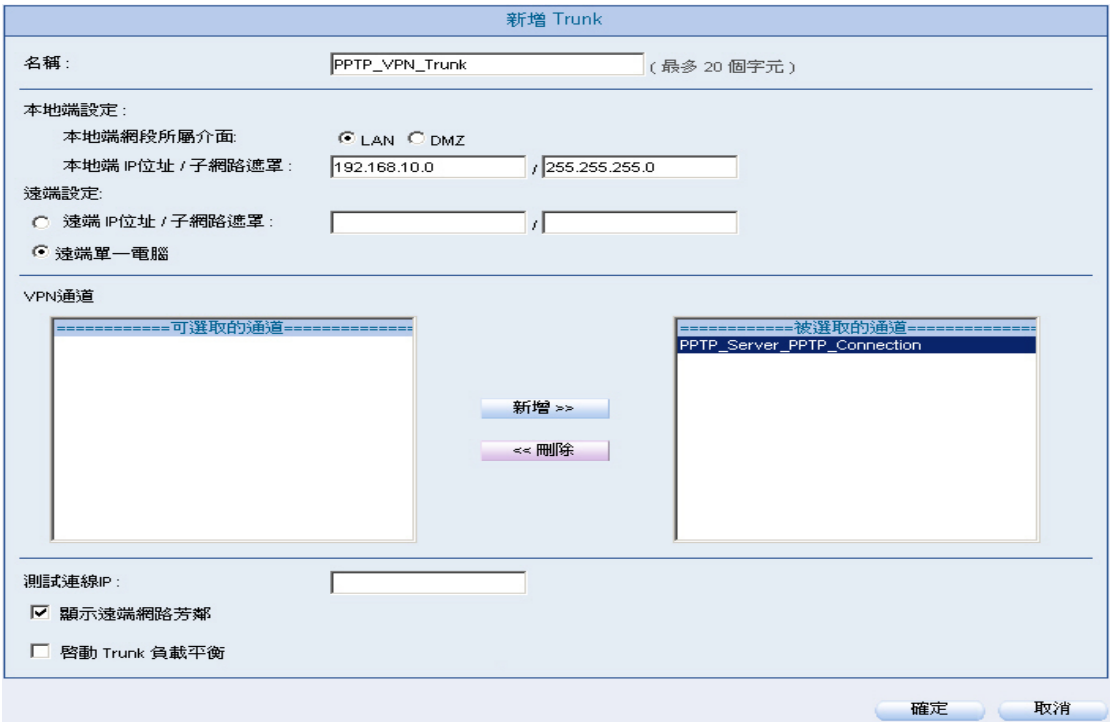


圖 11-321 設定 Trunk

圖 11-322 完成 Trunk 設定

說明：

1. 若外部使用者欲透過 PPTP VPN 連線至 MHG-2000 已建立的 IPSec VPN 網段，本地端 IP 位址/子網路遮罩必須設定為 IPSec VPN 網段。

步驟4. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-323）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-324）

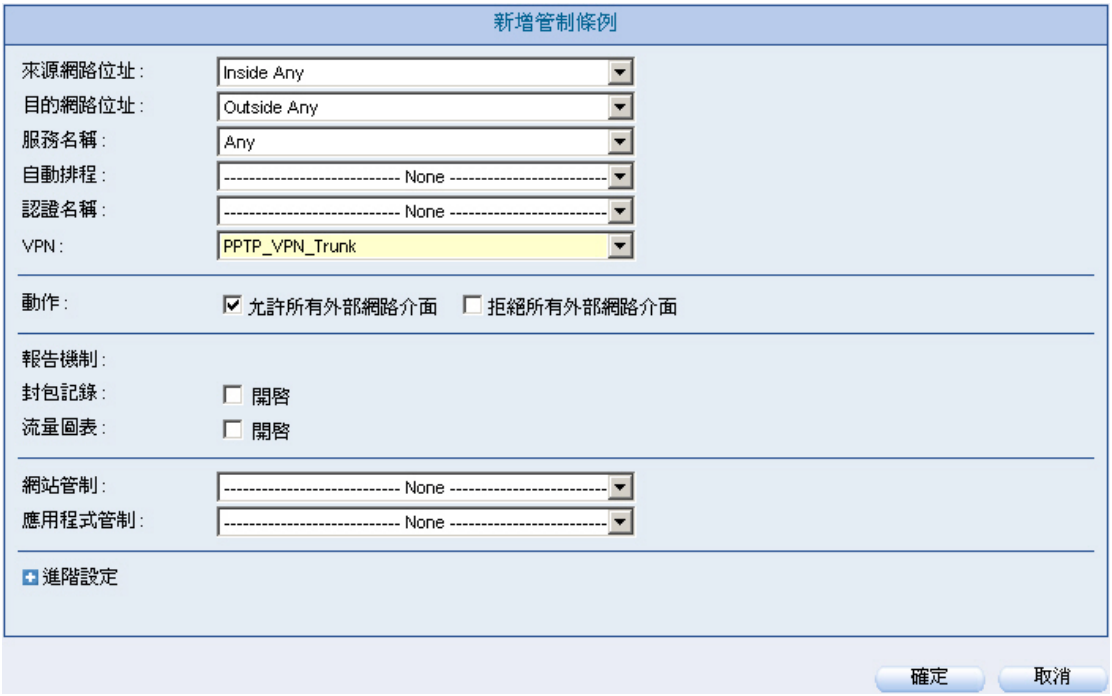


圖 11-323 設定 VPN Trunk 內部至外部之管制條例

圖 11-324 完成管制條例設定

步驟5. 在【管制條例】>【外部至內部】功能中，做下列設定：（如圖 11-325）

- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 11-326）

圖 11-325 設定 VPN Trunk 外部至內部之管制條例

圖 11-326 完成管制條例設定

乙公司的設定步驟如下：

步驟1. 在【開始】>【控制台】>【網路和共用中心】視窗中，做下列設定：（如圖 11-327）

- 點選【設定新的連線或網路】連結。（如圖 11-328）
- 在【設定連線或網路】視窗中：
  - 選擇【連線到工作地點】。
  - 按【下一步】鈕。（如圖 11-329）
- 在【連線到工作地點】視窗中：
  - 按下【使用我的網際網路連線(VPN)】鈕。（如圖 11-330）
  - 【網際網路位址】輸入 61.11.11.11。
  - 輸入指定【目的地名稱】。
  - 勾選【不要立即連線；先設定好，我稍後再連線】。
  - 按【下一步】鈕。（如圖 11-331）
  - 【使用者名稱】輸入 PPTP_Connection。
  - 【密碼】輸入 123456789。
  - 勾選【記住這個密碼】。
  - 按下【建立】鈕。（如圖 11-332）
  - 按下【關閉】鈕。（如圖 11-333）
- 點選【變更介面卡設定】連結。（如圖 11-334）
- 在【網路連線】視窗中：
  - 在【VPN 連線】項目上，按下滑鼠右鍵並選擇【連線】。（如圖 11-335）
  - 在【連線到 VPN 連線】視窗中：
    - 按下【連線】鈕。（如圖 11-336, 圖 11-337）
  - 完成連線。（如圖 11-338）

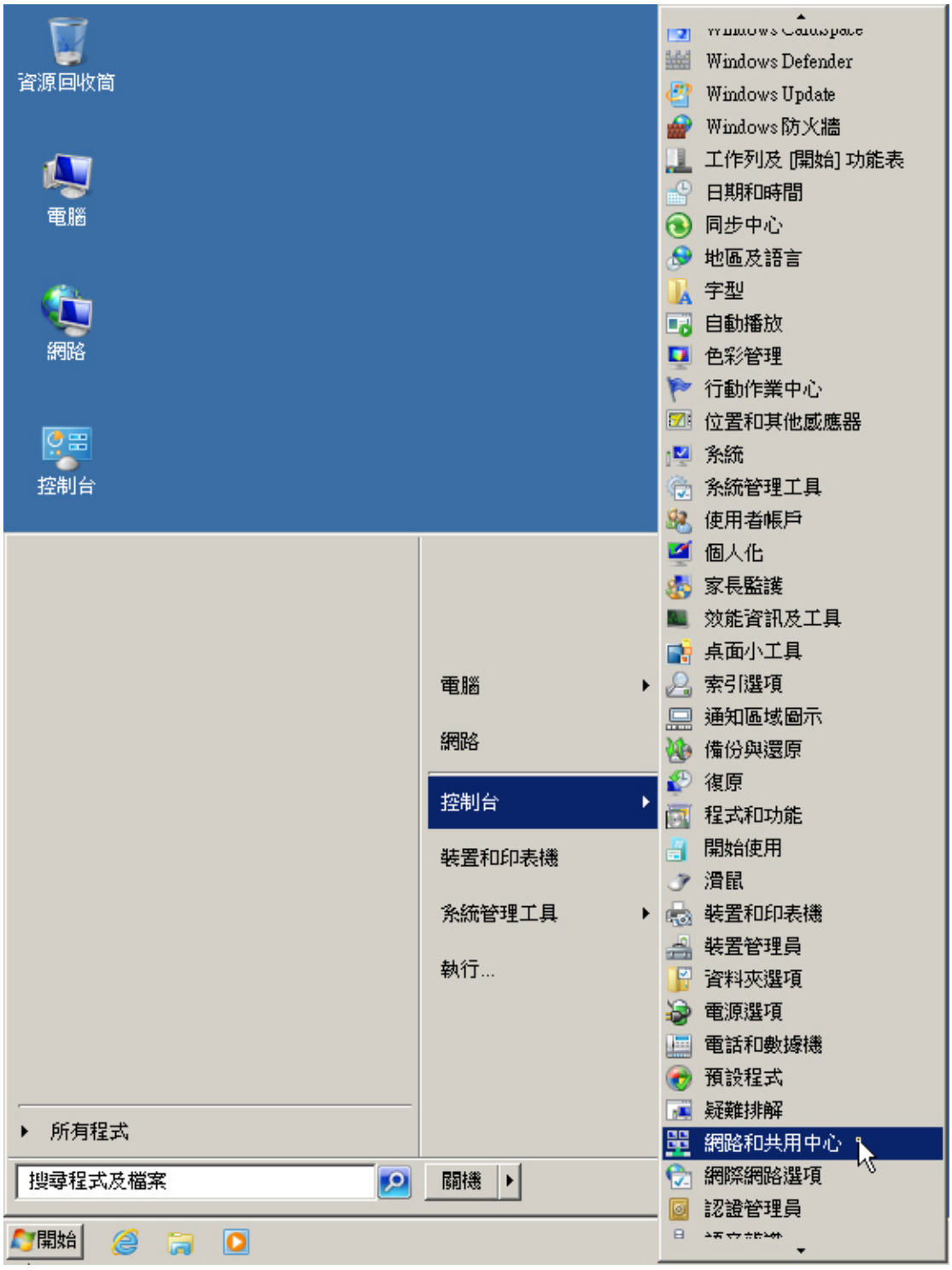


圖 11-327 開啟網路和共用中心視窗

圖 11-328 開啟設定連線或網路視窗

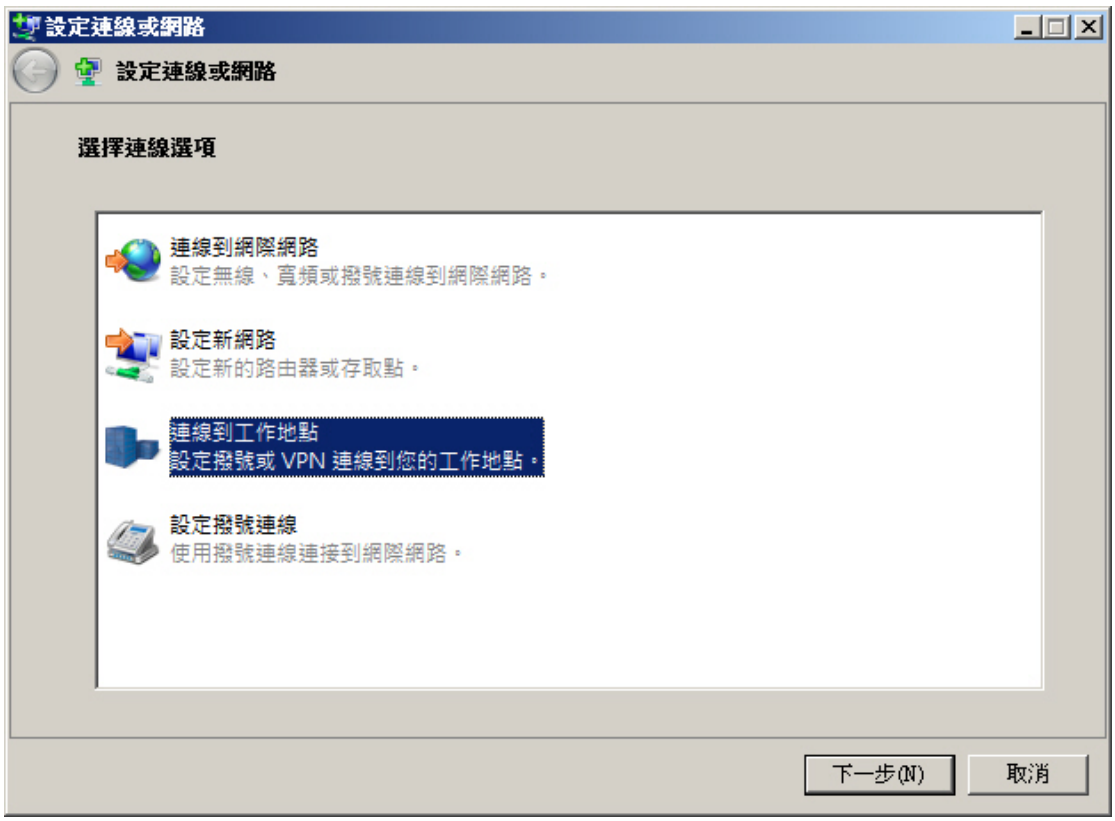


圖 11-329 開啟連線到工作地點視窗

圖 11-330 選擇連線模式

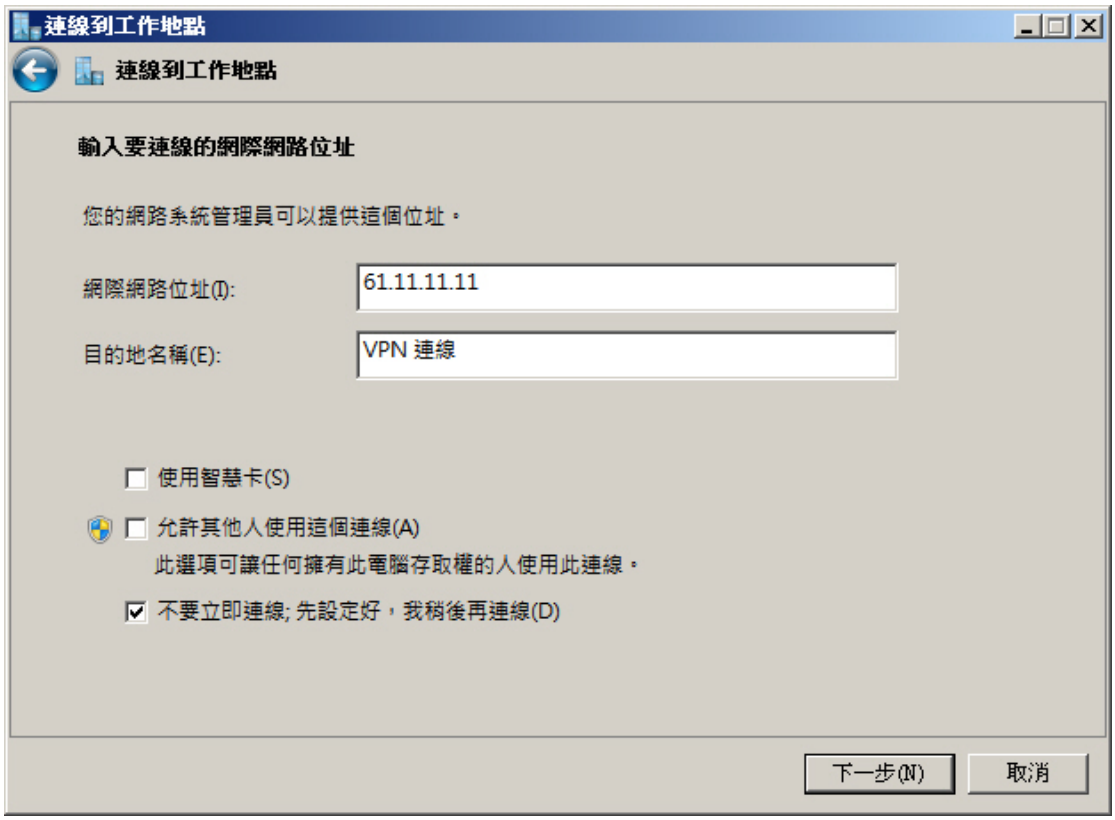


圖 11-331 網際網路位址設定

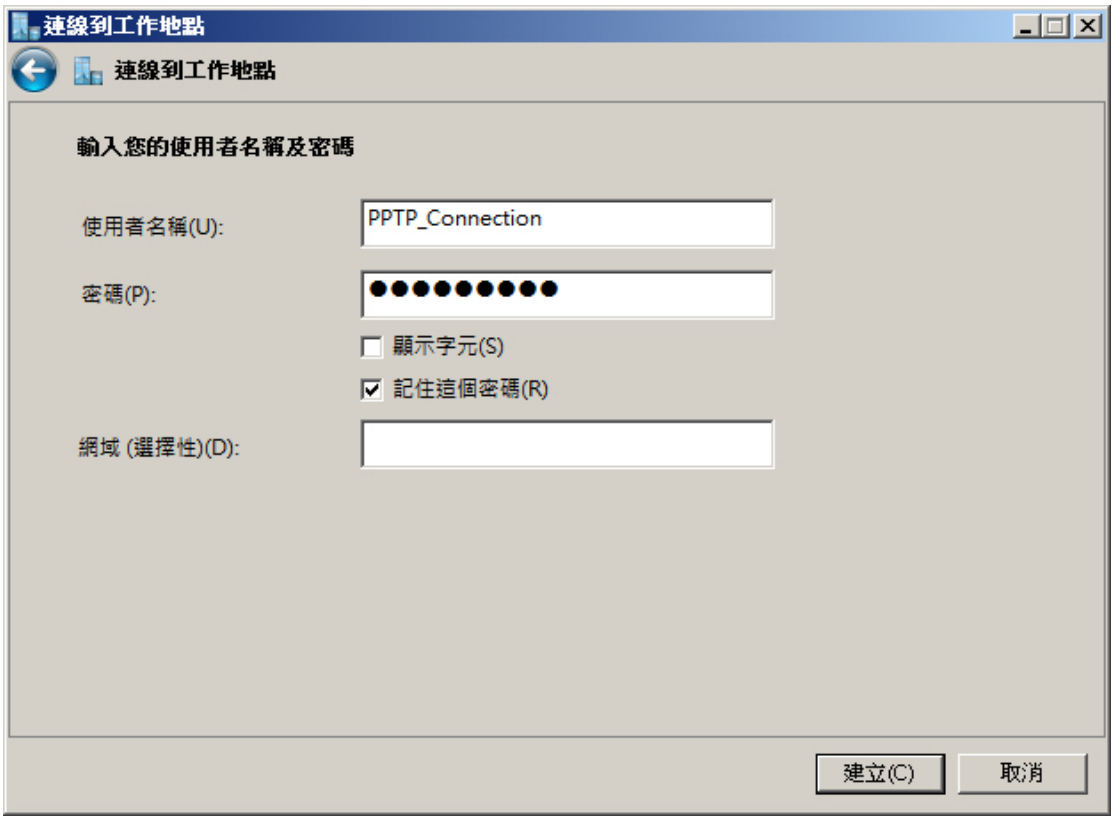


圖 11-332 連線驗證帳密設定

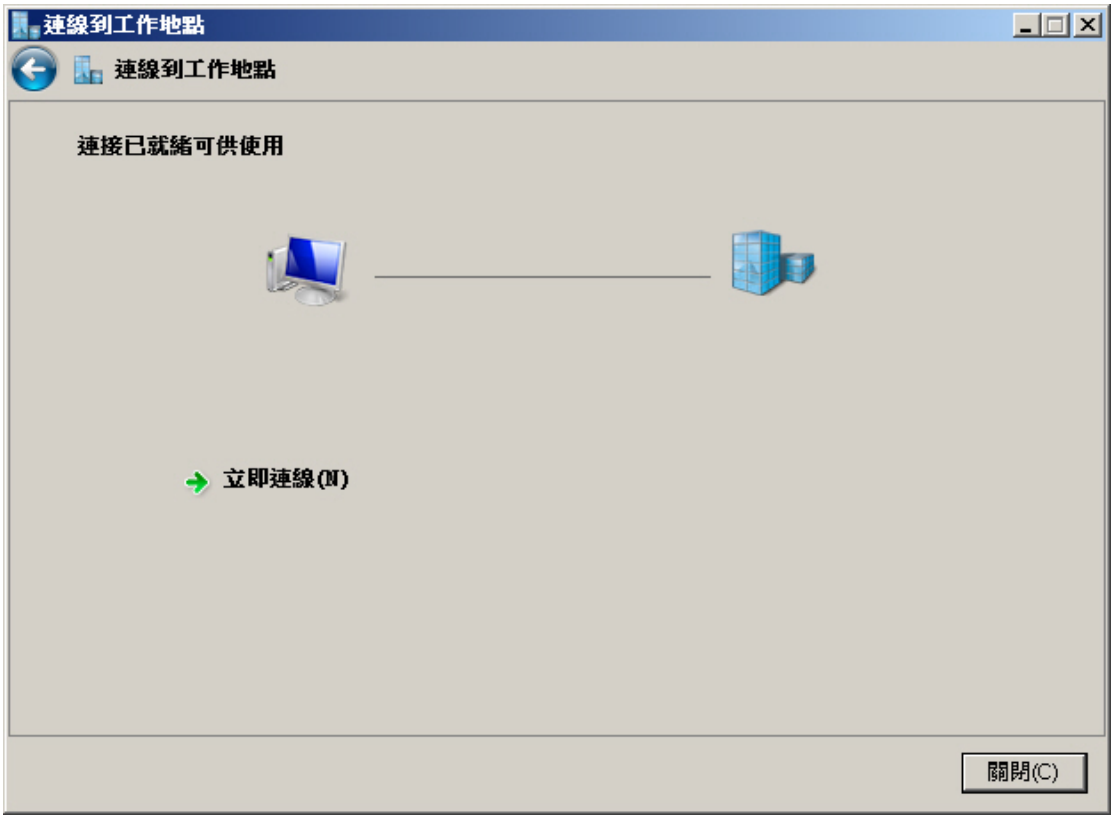


圖 11-333 完成連線設定

圖 11-334 開啟網路連線視窗

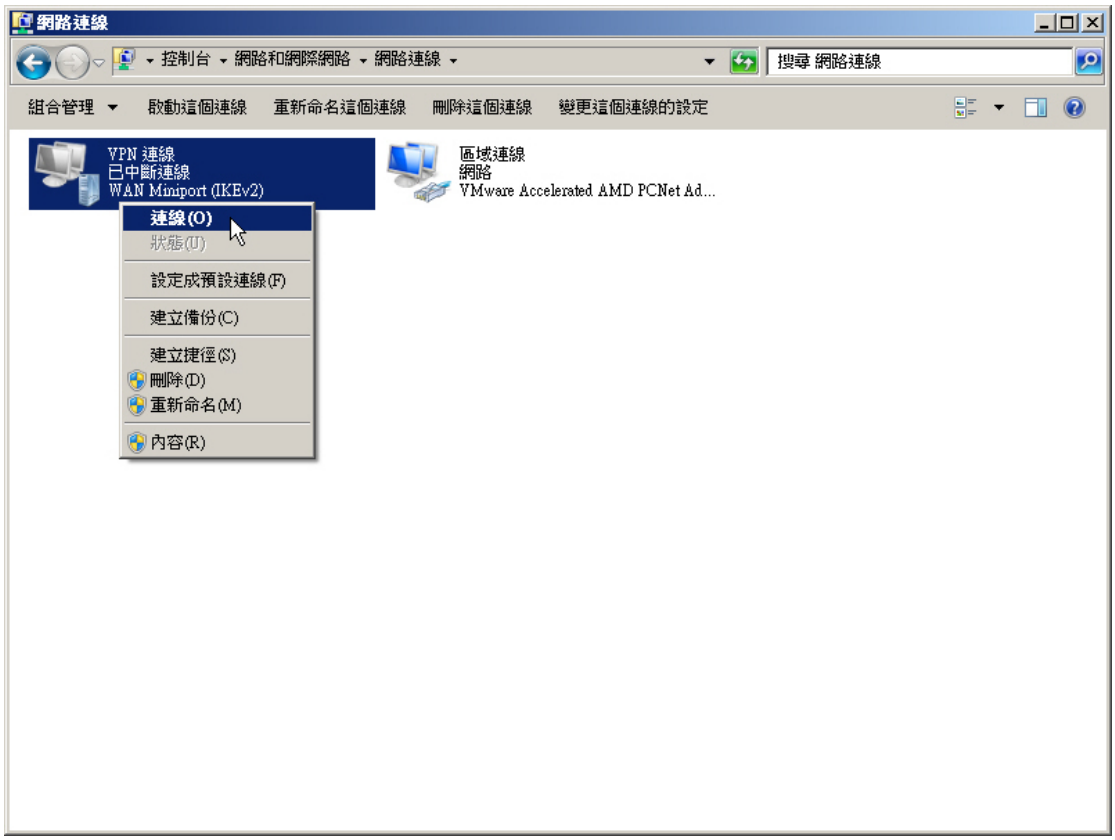


圖 11-335 開啟連線到 VPN 連線視窗

圖 11-336 VPN 連線設定

圖 11-337 建立 VPN 連線

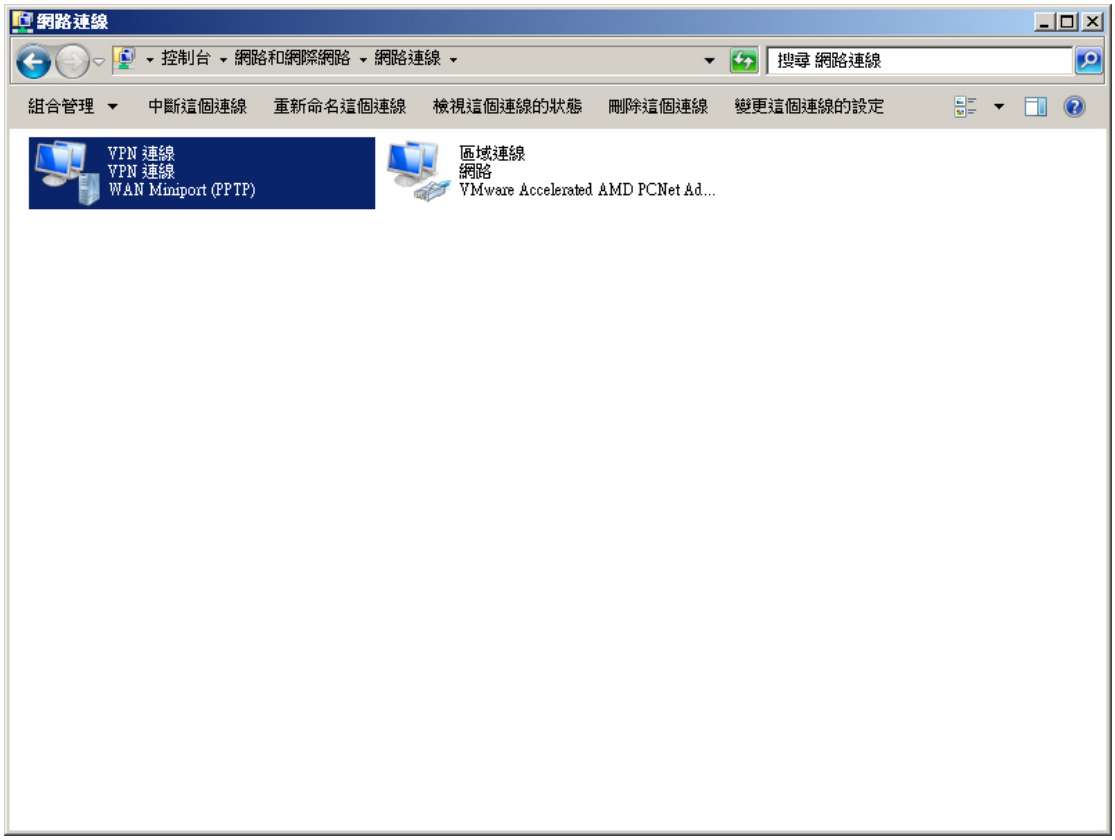


圖 11-338 完成 VPN 連線

步驟2. 完成 PPTP VPN 連線。（如圖 11-339）

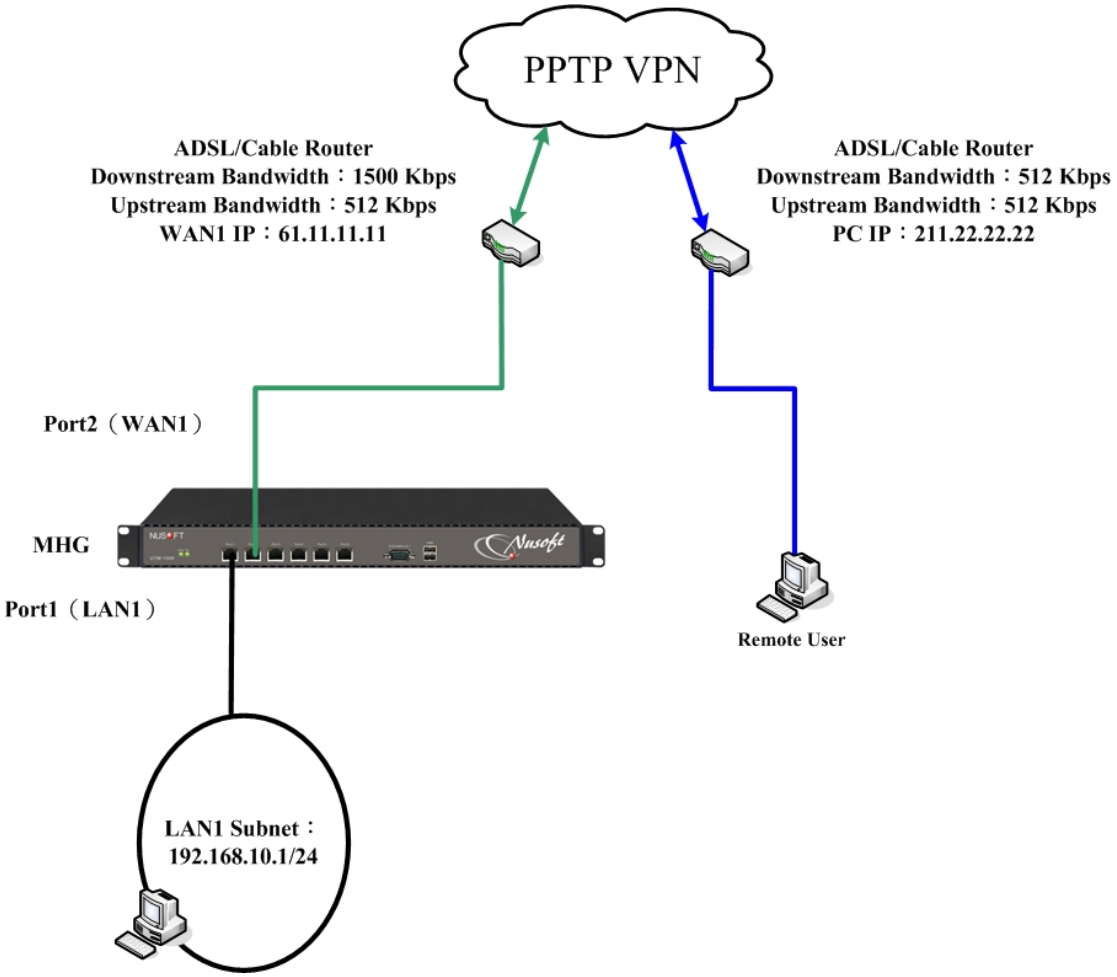


圖 11-339PPTP VPN 連線環境

網站管制

第12章　組態

用來控管使用者瀏覽網頁時存取的網站、檔案、MIME/Script，避免摸魚降低工作效率、在不知情的狀況下遭植入惡意程式（病毒）。

- 【網站白名單】: 系統管理員可透過完整網域名稱、關鍵字或萬用字元（＊），設定開放存取的特定網址。
- 【網站黑名單】: 系統管理員可透過完整網域名稱、關鍵字或萬用字元（＊），設定阻擋存取的特定網址。
- 【網站類別資料庫】: 系統管理員可針對網站分類，設定阻擋存取的規則。（須付費使用）
- 【檔案傳輸管制】: 管制直接透過 http 或 ftp 協定從網路下載、上傳特定副檔名之檔案。
- 【MIME/Script 管制】：管制網頁 Pop-up Window、ActiveX Control、Java Applet、Browser Cookie 的存取權限，和網頁傳送的資料型態。
- 【網站管制群組】：系統管理員可組合所設定的【網站白名單】、【網站黑名單】、【網站類別資料庫】、【檔案傳輸管制】或【MIME/Script 管制】項目，制定網站管制規則。

【設定】功能概述：

網站分類管制啟用狀態 說明如下：

- 如欲採用網站類別機制進行網站存取管控，必須在此匯入所購買的有效授權金鑰。
- 每筆金鑰皆為獨一無二，僅能適用於該設備，不同的設備、型號無法共用。如無金鑰或金鑰過期失效，請洽詢經銷商購買。

說明：

1. 若架設 MHG-2000【高可用性】環境，務必以 Port1 做為【高可用性連接埠】，讓依據運作中主機產品資訊申請連線【網站類別資料庫】的授權金鑰，可以有效同步至備機。

阻擋網站時顯示警告訊息 說明如下：

- 可在此設定 MHG-2000 阻擋網站時，於使用者瀏覽器所顯示的警訊。

網站管制日誌設定 說明如下：

- 可將網站管制記錄傳送至指定的遠端記錄主機。
  - 在【網站管制】>【組態】>【設定】頁面中，做下列設定：
    - 輸入所購買的網站類別資料庫授權金鑰儲存位址。
    - 勾選【開啟阻擋網站時顯示警告訊息】，輸入自訂的【警告訊息】。
    - 按下【確定】鈕，完成設定。（如圖 12-1）

圖 12-1 網站管制設定頁面

說明：

1. 【開啟 Syslog】前，要先於【系統管理】>【組態】>【系統設定】頁面的【Syslog 遠端記錄設定】欄位中，連線指定的外部記錄設備，以便將網站管制記錄傳送至該設備。

◆ 當內部使用者連線至阻擋的網站時，會顯示下列畫面：（如圖 12-2）

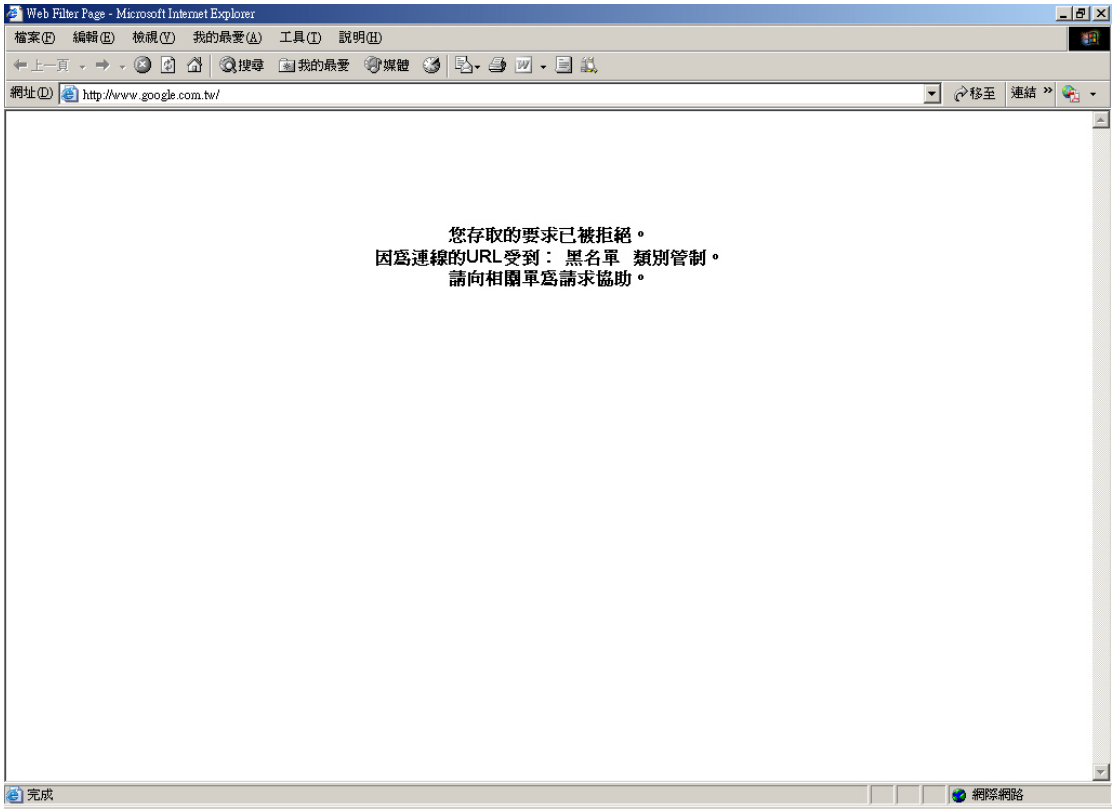


圖 12-2 網站阻擋警訊

【網站白名單】功能概述：

名稱 說明如下：

■ 網站白名單規則的辨識名稱。

URL 說明如下：

■ 設定允許存取的特定網址關鍵字。

■ 若將其設為*，則代表允許存取任何網址。

排除檔案傳輸管制 說明如下：

■ 可透過允許連結的網址存取所限制的檔案。

【網站黑名單】功能概述：

名稱 說明如下：

■ 網站黑名單規則的辨識名稱。

URL 說明如下：

- 設定阻擋存取的特定網址關鍵字。
- 若將其設為*，則代表阻擋存取任何網址。

【網站類別資料庫】功能概述：

名稱 說明如下：

- 網站類別規則的辨識名稱。

網站類別 說明如下：

- 可分為非法、情色、賭博與遊戲、社會與經濟、互動與服務、休閒嗜好、教育新知、其他等類別，於各大類別中包含了所屬的網站類型。
- 可組合特定的網站類型來設置管制規則。

說明：

1. MHG-2000 管制網站存取的規則比對順序：【網站白名單】→【網站黑名單】→【網站類別資料庫】。

【檔案傳輸管制】功能概述：

名稱 說明如下：

- 檔案傳輸管制規則的辨識名稱。

預設之副檔名 說明如下：

- 可阻擋使用者透過 HTTP 或 FTP 協定傳輸 MHG-2000 預設副檔名之檔案。

自訂之副檔名 說明如下：

- 可阻擋使用者透過 HTTP 或 FTP 協定傳輸自訂副檔名之檔案。

禁止傳遞所有檔案 說明如下：

- 可阻擋使用者透過 HTTP 或 FTP 協定傳輸任一預設和自訂副檔名之檔案。

禁止分段傳檔 說明如下：

- 可限制使用者將檔案分割，透過 HTTP 或 FTP 協定同時以多條連線傳輸。

【MIME/Script 管制】功能概述：

名稱 說明如下：

- MIME/Script 管制規則的辨識名稱。

阻擋的 Script 說明如下：

- Pop-up Window：可阻擋瀏覽網頁時自動彈跳出視窗。
- ActiveX Control：可阻擋執行網頁內嵌的 ActiveX 控制項。
- Java Applet：可阻擋執行網頁內嵌的 Java 程序。
- Browser Cookie：可阻擋網站儲存特定資訊於使用者電腦。

Mime 類型 說明如下：

- MIME（Multipurpose Internet Mail Extensions，多用途網際網路郵件擴展）是一個網際網路標準，它擴展了電子郵件標準，使其能夠支援二進位格式附件、非 ASCII 字元等多種格式的訊息。在 HTTP 協定中也使用了 MIME 的框架。
- MIME 規定了用於表示各樣資料類型的符號化方法。
- MIME 的內容類型（Content-Type）表頭（Header）是用於指定訊息類型，通常呈現的方式為 Type/Subtype。
  - Type 的種類有：
    - Text：用於標準化表示文字訊息，可以是多種字元集或格式的文字訊息。
    - Multipart：用於整合多個文件為一個訊息，這些文件可以是不同類型的資料。
    - Application：用於傳輸應用程式或二進位資料。
    - Message：用於封裝一個電子郵件訊息。
    - Image：用於傳輸靜態圖片資料。
    - Audio：用於傳輸音訊或聲音資料。
    - Video：用於傳輸動態影像資料，可以是與音訊編輯在一起的視訊資料。
  - Subtype 用於指定 Type 的細部種類，常見的有：
    - text/plain（純文字文件）。
    - text/html（HTML 文件）。
    - application/xhtml+xml（XHTML 檔案）。
    - image/gif（GIF 圖像）。
    - image/jpeg（JPEG 圖像）。
    - image/png（PNG 圖像）。

- video/mpeg（MPEG 影像）。
- application/octet-stream（任意的二進位資料）。
- application/pdf（PDF 檔案）。
- application/msword（Microsoft Word 文件）。

⚠ 注意：

1. 【網站白名單】、【網站黑名單】、【網站類別資料庫】、【檔案傳輸管制】和【MIME/Script 管制】規則皆要群組後，方能為【管制條例】所引用。

12.1 網站管制功能使用範例

編碼	適用範圍	範例環境	頁碼
12.1.1	**網站白名單** **網站黑名單** **網站管制群組**	使用白名單與黑名單來限制內部使用者存取特定網址	**422**
12.1.2	**網站類別資料庫** **檔案傳輸管制** **MIME/Script管制** **網站管制群組**	限制內部使用者連線特定類型的網站、以HTTP或FTP協定下載/上傳特定副檔名之檔案、存取網站之特定MIME資料/Script程式	**427**

12.1.1 使用白名單與黑名單來限制內部使用者存取特定網址

步驟1. 在【網站管制】>【組態】>【網站白名單】頁面中，做下列設定：

- 按下【新增】鈕。
- 輸入指定【名稱】。
- 【URL】輸入第一條允許連線的網址關鍵字。(例如：yahoo)
- 按下【確定】鈕。(如圖 12-3)
- 再次按下【新增】鈕。
- 輸入指定【名稱】。
- 【URL】輸入第二條允許連線的網址關鍵字。(例如：google)
- 按下【確定】鈕，完成設定。(如圖 12-4, 圖 12-5)

圖 12-3 設定第一條網站白名單規則

圖 12-4 設定第二條網站白名單規則

圖 12-5 完成網站白名單設定

說明：

1. 系統管理員可【匯出網站白名單至用戶端】來整理和保存相關設定資料，以利未來MHG-2000【網站白名單】錯亂時，可清除清單內容重新【從用戶端匯入網站白名單】。

步驟2. 在【網站管制】>【組態】>【網站黑名單】頁面中，做下列設定：（如圖 12-6）

- 輸入指定【名稱】。
- 【URL】輸入*（代表任一字元），用來阻擋連線任何網址。
- 按下【確定】鈕，完成設定。（如圖 12-7）

圖 12-6 設定網站黑名單

圖 12-7 完成網站黑名單設定

說明：

1. 系統管理員可【匯出網站黑名單至用戶端】來整理和保存相關設定資料，以利未來MHG-2000【網站黑名單】錯亂時，可清除清單內容重新【從用戶端匯入網站黑名單】。

步驟3. 在【網站管制】>【組態】>【網站管制群組】頁面中，做下列設定：（如圖 12-8）

- 輸入指定群組【名稱】。
- 將【可選取的網站白名單】新增至【已選取的網站白名單】。
- 將【可選取的網站黑名單】新增至【已選取的網站黑名單】。
- 按下【確定】鈕，完成設定。（如圖 12-9）

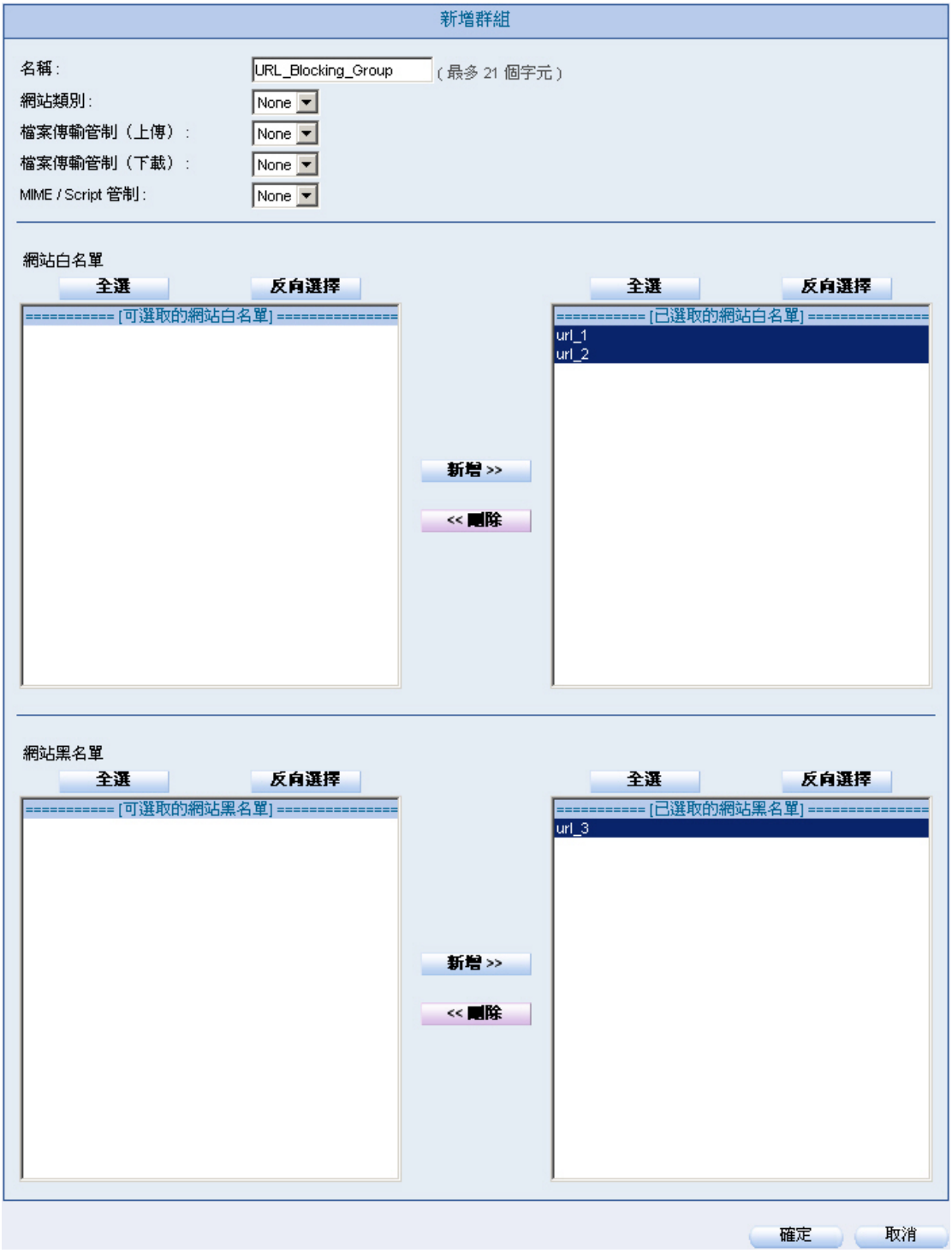


圖 12-8 設定網站管制群組

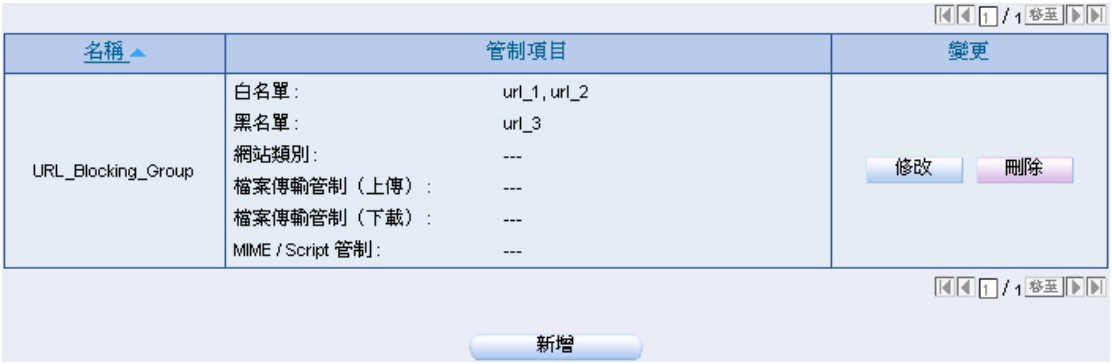


圖 12-9 完成網站管制群組設定

步驟4. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 12-10）

- 【網站管制】選擇所設定的網站管制群組規則。
- 按下【確定】鈕，完成設定。（如圖 12-11）
- 使用者僅能經由此管制條例連結含有 yahoo 和 google 關鍵字的網址。

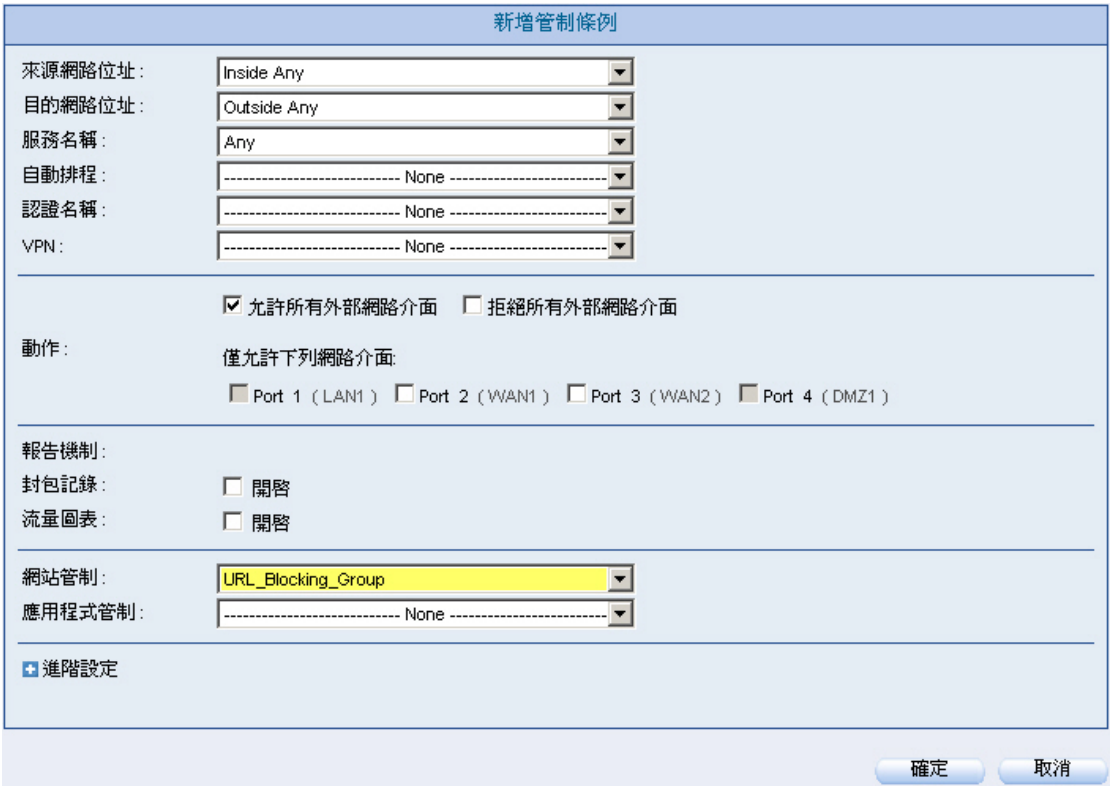


圖 12-10 管制條例套用網站管制規則

圖 12-11 完成管制條例設定

12.1.2 限制內部使用者連線特定類型的網站、以 HTTP 或 FTP 協定下載/上傳特定副檔名之檔案、存取網站之特定 MIME 資料/Script 程式

步驟1. 在【網站管制】>【組態】>【網站類別資料庫】頁面中，做下列設定：（如圖 12-12）

- 輸入指定【名稱】。
- 勾選【非法網站】、【情色網站】、【賭博與遊戲】等類別。
- 按下【確定】鈕，完成設定。（如圖 12-13）

圖 12-12 設定網站類別規則

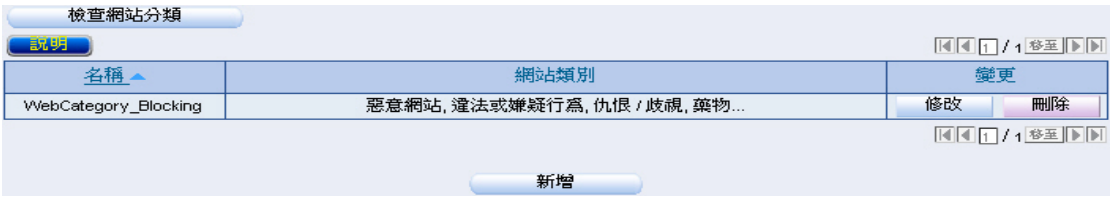


圖 12-13 完成網站類別規則設定

步驟2. 在【網站管制】>【組態】>【檔案傳輸管制】頁面中，做下列設定：（如圖 12-14）

- 輸入指定【名稱】。
- 勾選【禁止傳遞所有檔案】。
- 按下【確定】鈕，完成設定。（如圖 12-15）

圖 12-14 設定檔案傳輸管制

圖 12-15 完成檔案傳輸管制設定

說明：

1. 在【網站管制】>【組態】>【檔案傳輸管制】頁面中，於【副檔名清單】欄位按下【修改】鈕，做下列設定，使用者可自訂欲阻擋的檔案副檔名：
   - 按下【新增】鈕。（如圖 12-16）
   - 輸入自訂的【副檔名】。
   - 按下【確定】鈕，完成設定。（如圖 12-17，圖 12-18）

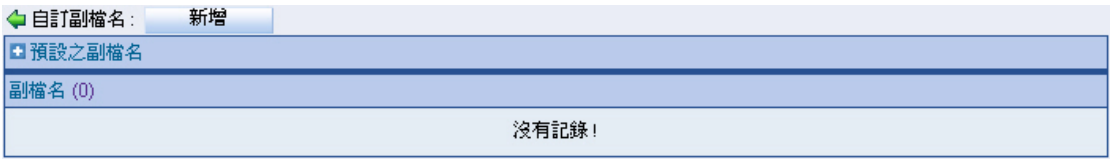


圖 12-16 副檔名設定頁面

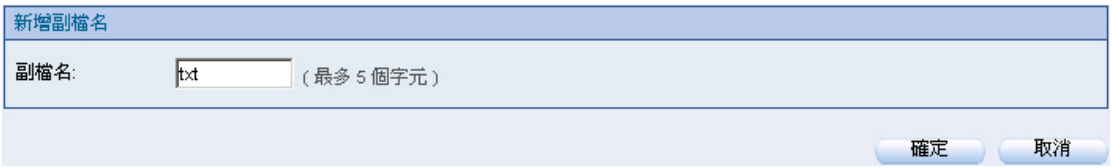


圖 12-17 新增副檔名

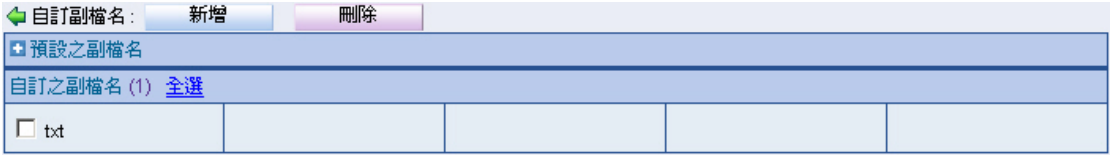


圖 12-18 完成副檔名新增

步驟3. 在【網站管制】>【組態】>【MIME/Script 管制】頁面中，做下列設定：（如圖 12-19）

- 輸入指定【名稱】。
- 勾選要【阻擋的 Script】Pop-up Window、ActiveX Control、Java Applet、Browser Cookie。
- 將【可選取的 Mime 類型】新增至【被選取的 Mime 類型】。
- 按下【確定】鈕，完成設定。（如圖 12-20）

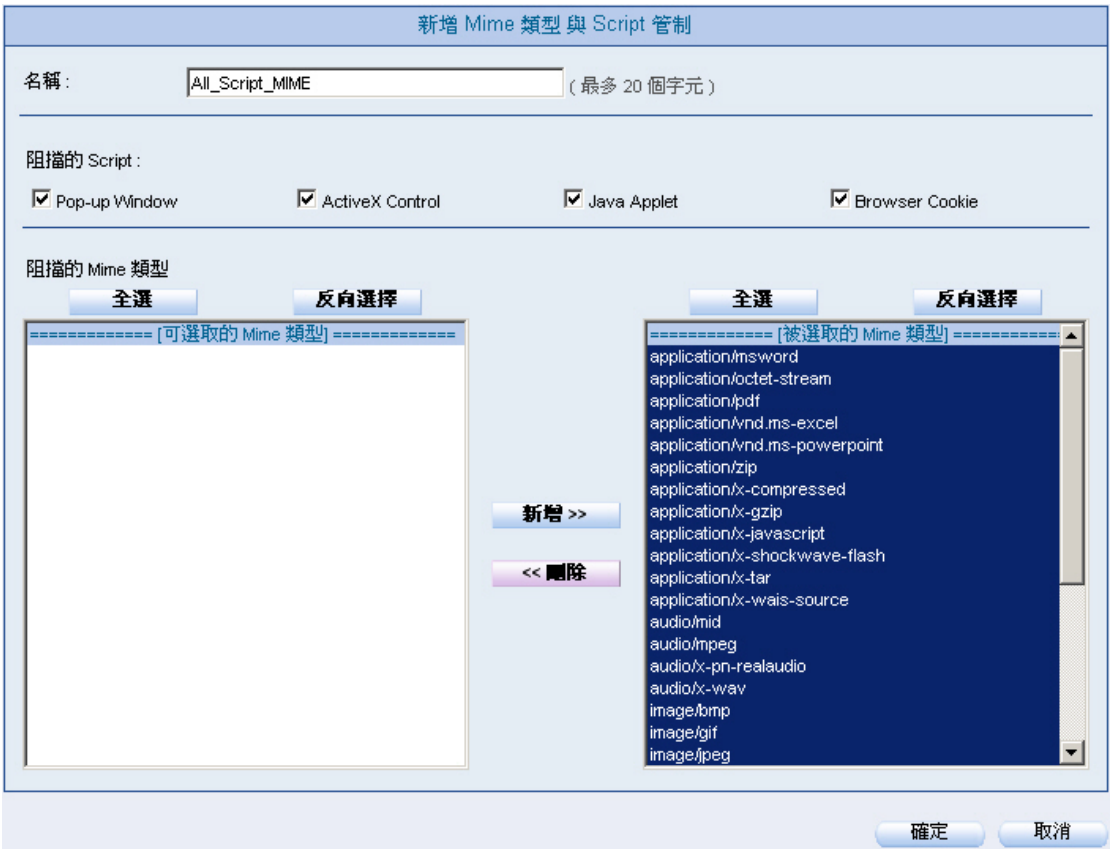


圖 12-19 設定 MIME/Script 管制

圖 12-20 完成 MIME/Script 管制設定

說明：

1. 在【網站管制】>【組態】>【MIME/Script 管制】頁面中，於【Mime 類型清單】欄位按下【修改】鈕，做下列設定，使用者可自訂欲阻擋的 Mime 類型：

- 按下【新增】鈕。（如圖 12-21）
- 輸入自訂的【Mime 類型】。
- 按下【確定】鈕，完成設定。（如圖 12-22, 圖 12-23）

圖 12-21Mime 類型設定頁面

圖 12-22 新增 Mime 類型

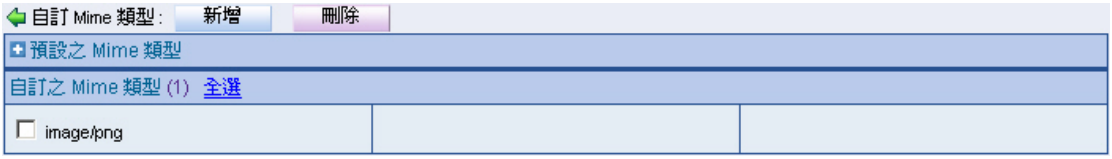


圖 12-23 完成 Mime 類型新增

步驟4. 在【網站管制】>【組態】>【網站管制群組】頁面中，做下列設定：（如圖 12-24）

- 輸入指定群組【名稱】。
- 選擇所設定的【網站類別】規則。
- 選擇所設定的【檔案傳輸管制（上傳）】、【檔案傳輸管制（下載）】規則。
- 選擇所設定的【MIME/Script 管制】規則。
- 按下【確定】鈕，完成設定。（如圖 12-25）

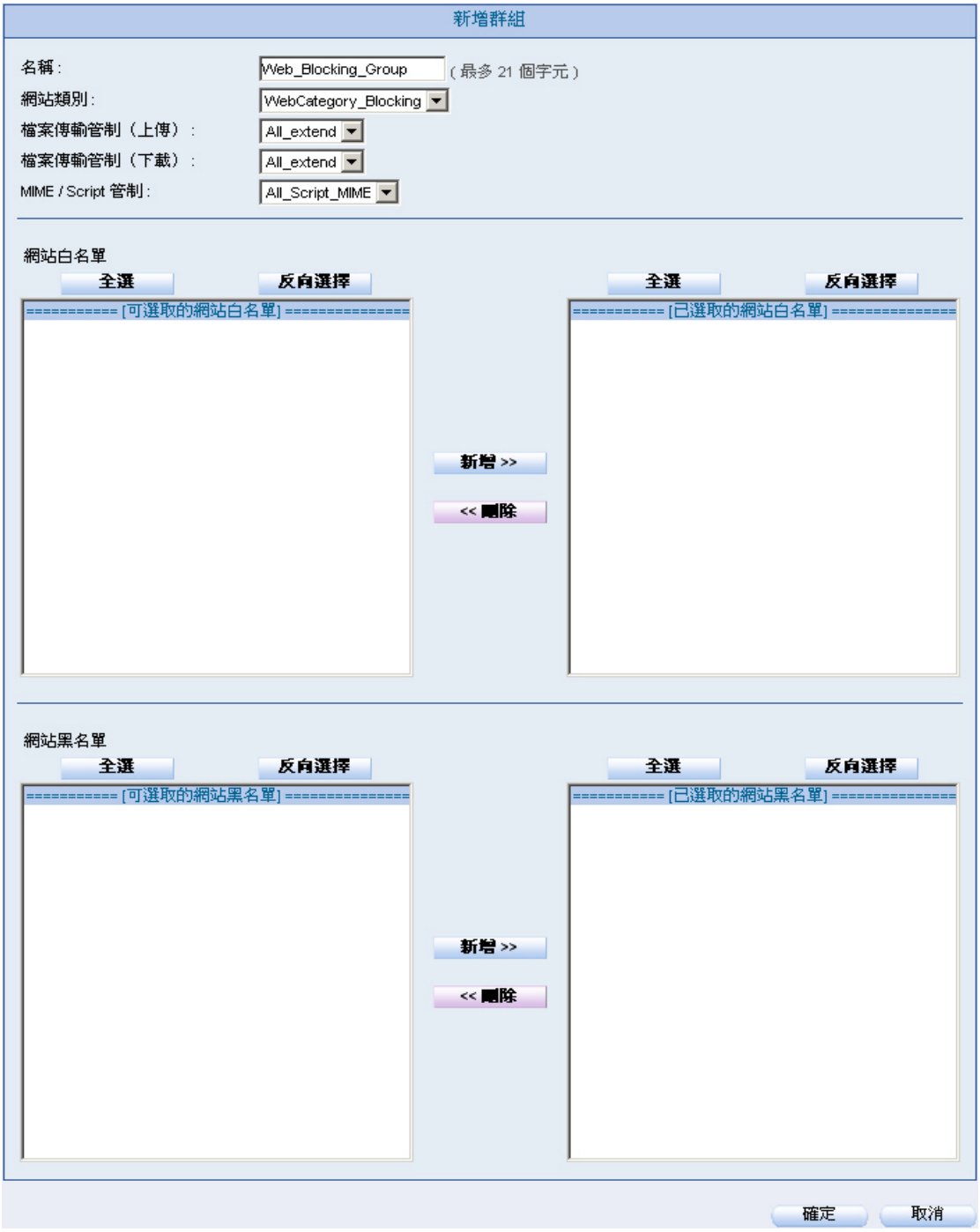


圖 12-24 設定網站管制群組

圖 12-25 完成網站管制群組設定

步驟5. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 12-26）

- 【網站管制】選擇所設定的網站管制群組規則。
- 按下【確定】鈕，完成設定。（如圖 12-27）

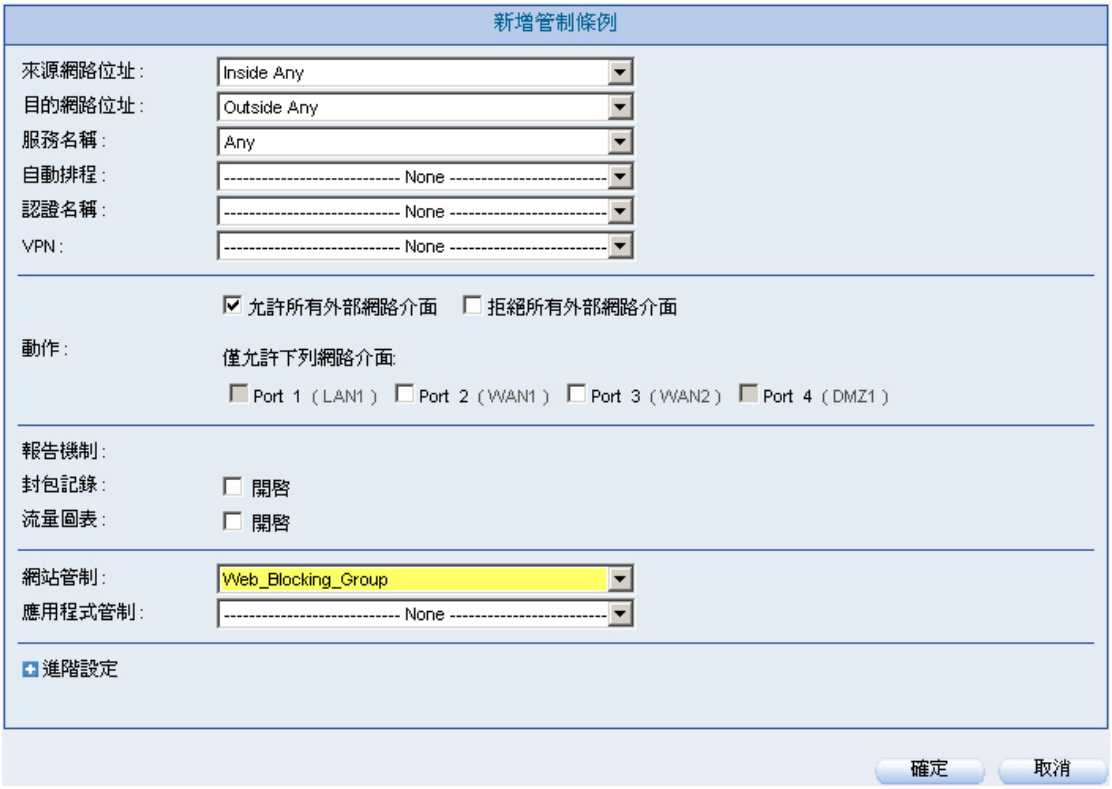


圖 12-26 管制條例套用網站管制規則

圖 12-27 完成管制條例設定

第13章　網站管制報告

MHG-2000 可將其網站管制記錄做成統計報表和日誌，以便瞭解整體存取外部網站的狀況。

【設定】功能概述：

定期報告 說明如下：

- 可依選擇的報表產生時間，定時寄送報告給收件者。
- 可指定報表的統計排行資料筆數。

歷史報告 說明如下：

- 可產生指定日期的報表並即時郵寄給收件者。
  - 在【系統管理】>【組態】>【系統設定】頁面中，啟動並進行【電子郵件警告 / 報告設定】，並在【網站管制】>【網站管制報告】>【設定】頁面中，做下列設定：
    - 在【定期報告】設定欄位中，【開啟定期報告功能】並勾選年報、月報、週報和日報。
    - 按下【確定】鈕。**（如圖 13-1）**
    - 當時間到達時，MHG-2000 會寄送統計報表給收件者。**（如圖 13-2, 圖 13-3, 圖 13-4, 圖 13-5, 圖 13-6, 圖 13-7, 圖 13-8, 圖 13-9）**
    - 在【歷史報告】設定欄位中，指定要郵寄的報告日期。**（如圖 13-10）**
    - 按下【郵寄報告】鈕。
    - 會即時寄送相關統計報表給收件者。**（如圖 13-11, 圖 13-12, 圖 13-13, 圖 13-14, 圖 13-15, 圖 13-16, 圖 13-17, 圖 13-18）**

說明：

1. 郵寄定期報告，其產生方式如下：

- 【年報】：會於每年的 1 月 1 日上午 00:00 產生。
- 【月報】：會於每月第一天的上午 00:00 產生。
- 【週報】：會於每週第一天的上午 00:00 產生。
- 【日報】：會於每天的上午 00:00 產生。

圖 13-1 郵寄定期報告設定頁面

圖 13-2 收到定期報告信件

Nusoft System Co.

Web Filter Day Report of : Website Category

Website Category Top 20 Chart

No.	Website Category	Blocked	Allowed	Total	Access Indicator
1	Unknown	0	3359	3359	3359
2	Whitelist	0	1634	1634	1634
3	Computers & Technology	0	1486	1486	1486
4	General	0	726	726	726
5	Information Security	0	548	548	548
6	Search Engines & Portals	0	520	520	520
7	News	0	193	193	193
8	Chat	0	141	141	141
9	Instant Messaging	0	141	141	141
10	Social Networking	0	94	94	94
11	Advertisements & Pop-Ups	0	78	78	78
12	Personal Sites	0	17	17	17
13	Entertainment	0	9	9	9
14	Business	0	8	8	8
15	Education	0	6	6	6
16	Forums & Newsgroups	0	3	3	3
17	Download Sites	0	2	2	2
18	Shopping	0	1	1	1
19	Gambling	0	1	1	1

Time: **2010/11/06 00:00 ~ 2010/11/06 23:59** Total: **8967** Average: **373.62 URLs/Hour**

Website Address Top 20 Chart

No.	Website Address	Blocked	Allowed	Total	Access Indicator
1	61.219.32.246	0	1768	1768	1768
2	210.60.226.253	0	1508	1508	1508
3	database.clamav.net	0	1008	1008	1008
4	webres1.nusoft.ctmail.com	0	624	624	624
5	talkgadget.google.com	0	406	406	406
6	tw.yimg.com	0	247	247	247
7	l.yimg.com	0	246	246	246
8	www.sophos.com	0	230	230	230
9	ad.yieldmanager.com	0	182	182	182
10	secure-yt.imrworldwide.com	0	180	180	180
11	tw.news.yahoo.com	0	159	159	159
12	ichart.finance.yahoo.com	0	147	147	147
13	tw.linkspot.search.yahoo.com	0	141	141	141
14	downloads.sophos.com	0	115	115	115
15	cmk.tw.yahoo.overture.com	0	111	111	111
16	tw.rd.yahoo.com	0	105	105	105
17	forecastfox.accuweather.com	0	87	87	87
18	sirocco.accuweather.com	0	87	87	87
19	tw.stock.yahoo.com	0	87	87	87
20	row.bc.yahoo.com	0	84	84	84

Time: **2010/11/06 00:00 ~ 2010/11/06 23:59** Total: **8967** Average: **373.62 URLs/Hour**

NetBIOS Name / IP Address Top 20 Chart

1

圖 13-3 網站管制定期報告內容第一頁

No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator
1	192.168.85.85	0	5830	5830	5830
2	172.19.20.100	0	841	841	841
3	172.19.200.164	0	589	589	589
4	172.19.100.51	0	443	443	443
5	172.19.250.254	0	381	381	381
6	172.19.0.1	0	357	357	357
7	172.19.10.20	0	196	196	196
8	172.19.50.15	0	158	158	158
9	172.19.10.10	0	63	63	63
10	172.19.0.128	0	38	38	38
11	172.19.20.12	0	27	27	27
12	172.19.1.108	0	18	18	18
13	172.19.100.54	0	11	11	11
14	172.19.1.106	0	8	8	8
15	172.19.100.32	0	6	6	6
16	172.19.10.2	0	1	1	1
Time: **2010/11/06 00:00 ~ 2010/11/06 23:59**				Total: **8967**	Average: **373.62 URLs/Hour**

2

圖 13-4 網站管制定期報告內容第二頁

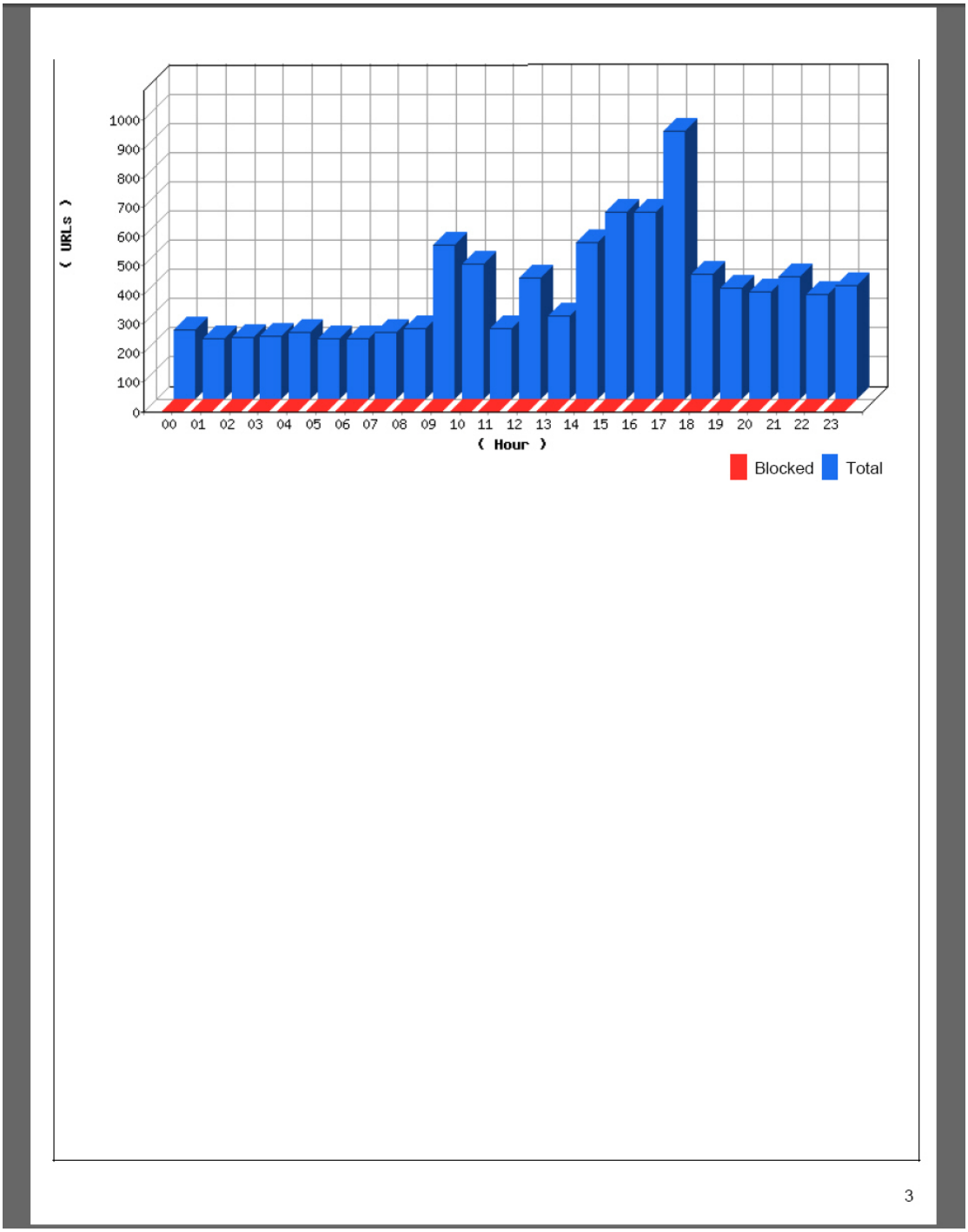
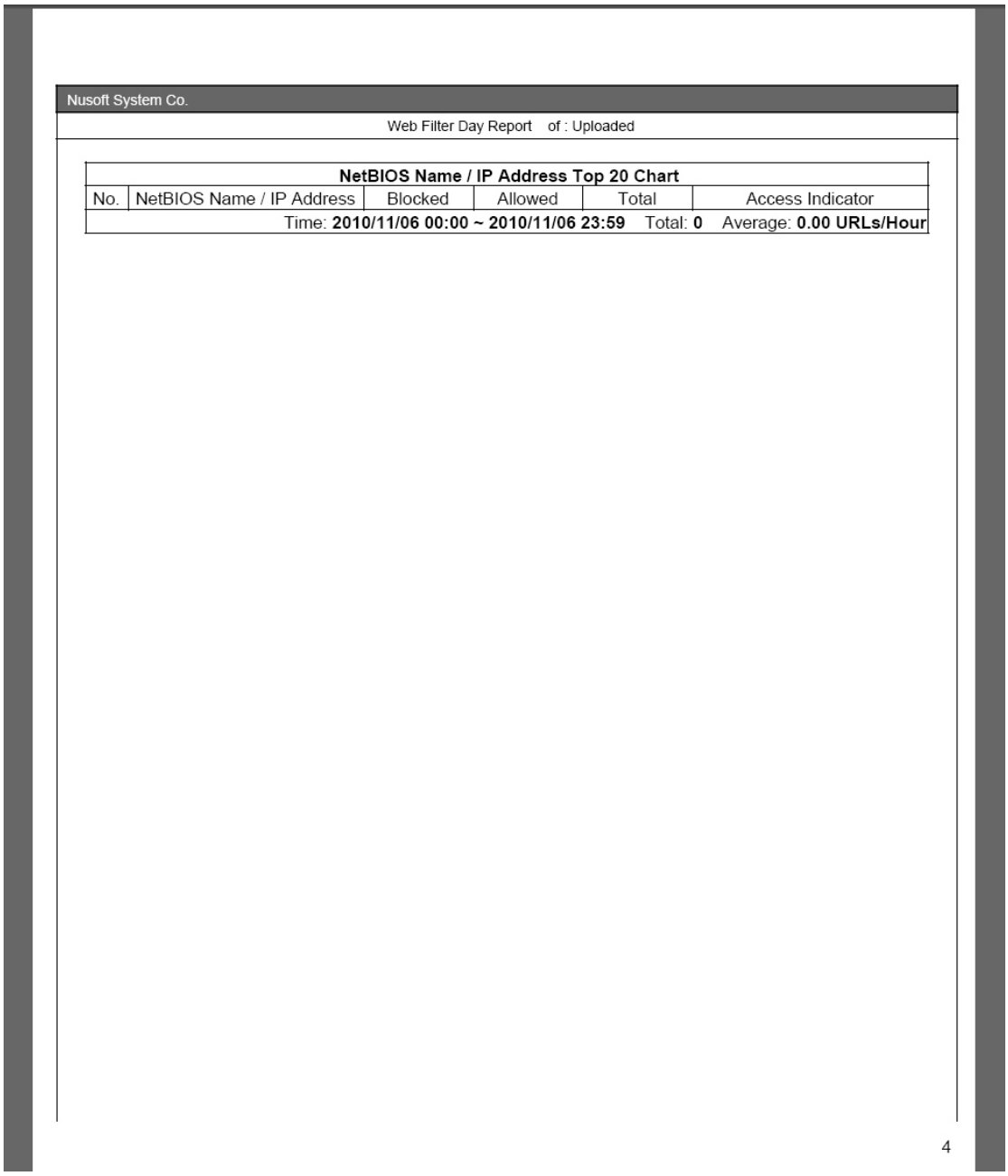


圖 13-5 網站管制定期報告內容第三頁



Nusoft System Co.

Web Filter Day Report of : Uploaded

NetBIOS Name / IP Address Top 20 Chart					
No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator
Time: **2010/11/06 00:00 ~ 2010/11/06 23:59** Total: **0** Average: **0.00 URLs/Hour**					

4

圖 13-6 網站管制定期報告內容第四頁

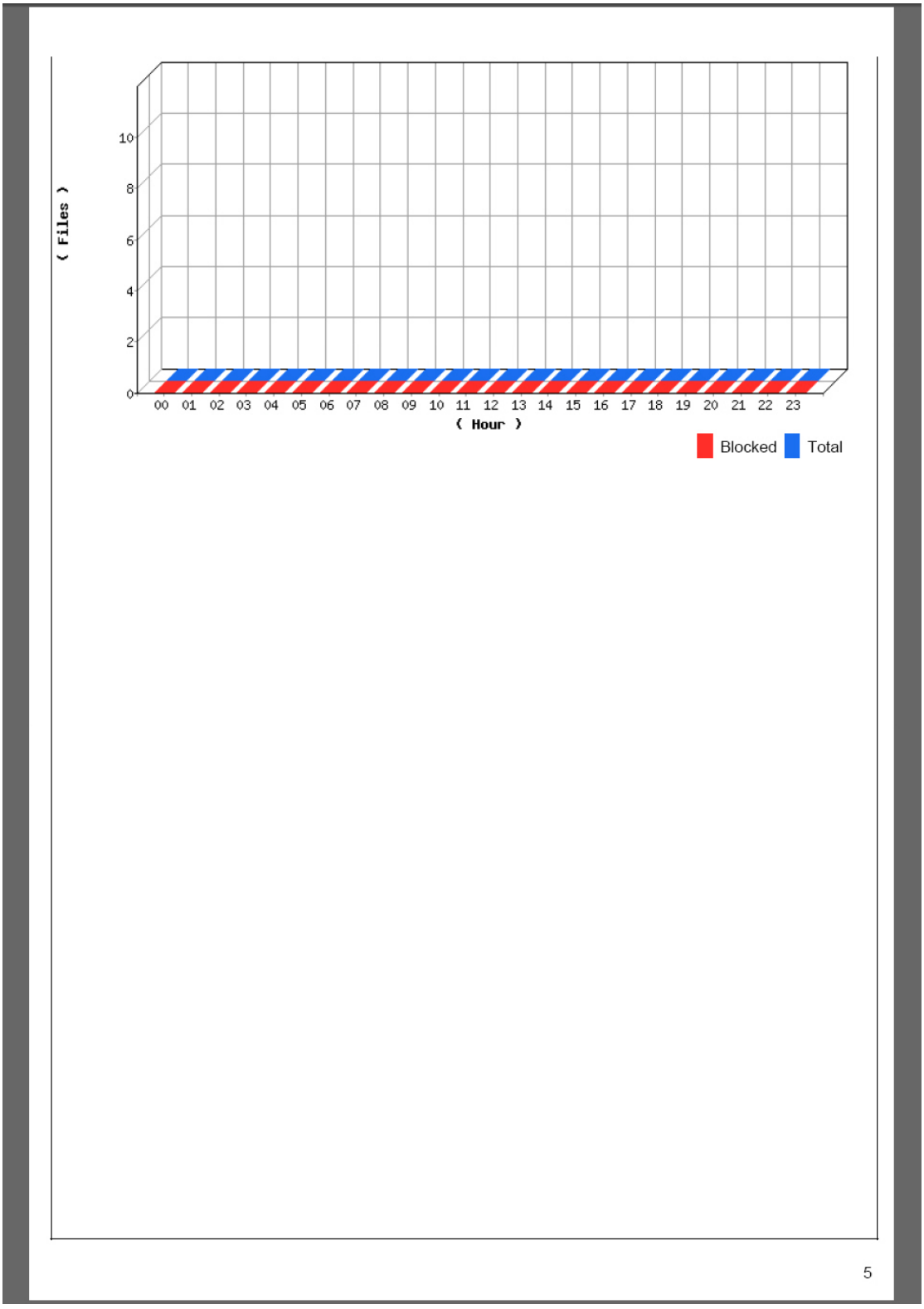
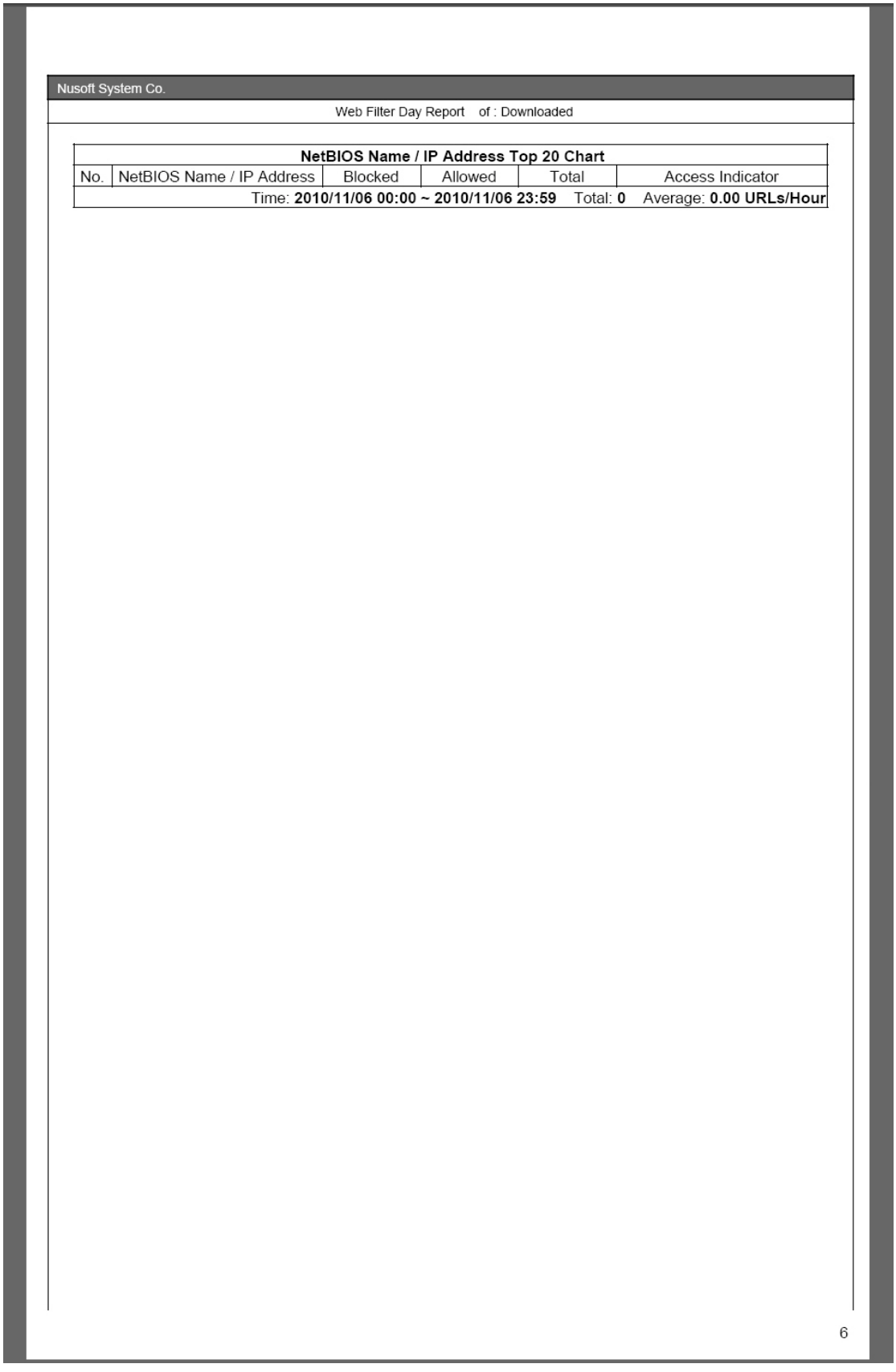


圖 13-7 網站管制定期報告內容第五頁



Nusoft System Co.

Web Filter Day Report of : Downloaded

NetBIOS Name / IP Address Top 20 Chart					
No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator
Time: **2010/11/06 00:00 ~ 2010/11/06 23:59** Total: **0** Average: **0.00 URLs/Hour**					

6

圖 13-8 網站管制定期報告內容第六頁

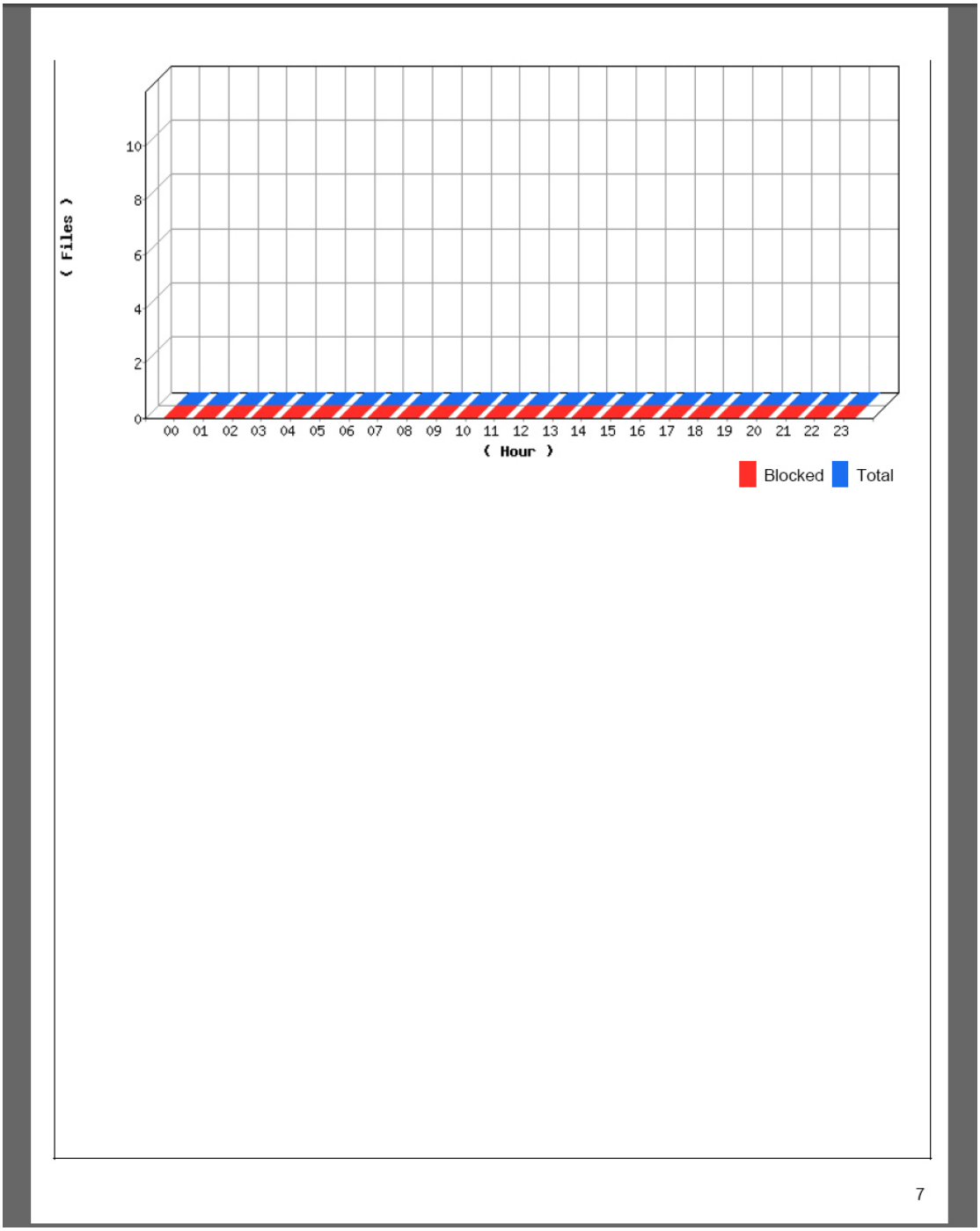


圖 13-9 網站管制定期報告內容第七頁

圖 13-10 郵寄歷史報告設定頁面

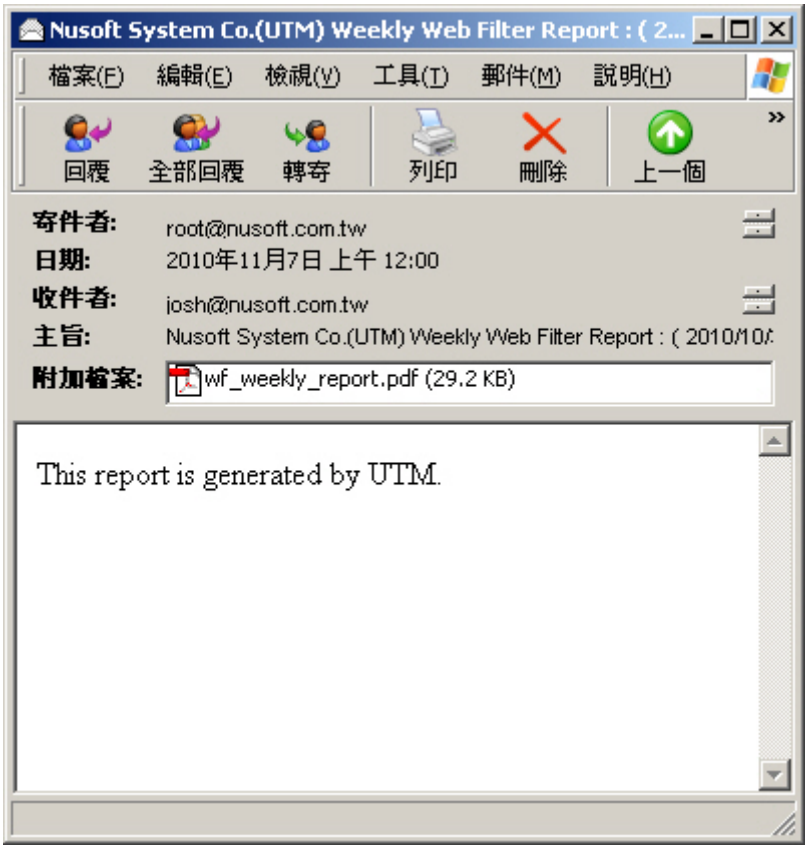


圖 13-11 收到歷史報告信件

Nusoft System Co.

Web Filter Weekly Report of : Website Category

Website Category Top 20 Chart

No.	Website Category	Blocked	Allowed	Total	Access Indicator
1	Whitelist	0	25952	25952	25952
2	Computers & Technology	0	24287	24287	24287
3	Unknown	0	23302	23302	23302
4	Search Engines & Portals	0	13328	13328	13328
5	General	0	8908	8908	8908
6	Information Security	0	8242	8242	8242
7	News	0	3990	3990	3990
8	Social Networking	0	3115	3115	3115
9	Advertisements & Pop-Ups	0	2689	2689	2689
10	Personal Sites	0	2676	2676	2676
11	Education	0	2323	2323	2323
12	Forums & Newsgroups	0	2211	2211	2211
13	Business	0	1513	1513	1513
14	Shopping	0	1479	1479	1479
15	Government	0	1142	1142	1142
16	Arts	0	963	963	963
17	Job Search	0	867	867	867
18	Transportation	0	747	747	747
19	Instant Messaging	0	734	734	734
20	Chat	0	734	734	734

Time: **2010/10/31(Sunday) ~ 2010/11/06(Saturday)** Total: **134251** Average: **19178.71 URLs/Day**

Website Address Top 20 Chart

No.	Website Address	Blocked	Allowed	Total	Access Indicator
1	61.219.32.246	0	8811	8811	8811
2	database.clamav.net	0	8009	8009	8009
3	210.60.226.253	0	7390	7390	7390
4	webres1.nusoft.ctmail.com	0	6366	6366	6366
5	l.yimg.com	0	4855	4855	4855
6	ad.yieldmanager.com	0	4068	4068	4068
7	tw.yimg.com	0	2688	2688	2688
8	secure-yt.imrworldwide.com	0	2134	2134	2134
9	safebrowsing-cache.google.com	0	1762	1762	1762
10	webpro10.url.trendmicro.com:80	0	1722	1722	1722
11	www.sophos.com	0	1505	1505	1505
12	safebrowsing.clients.google.com	0	1493	1493	1493
13	www.join-link.com.tw:8888	0	1458	1458	1458
14	tw.rd.yahoo.com	0	1438	1438	1438
15	www.google.com.tw	0	1418	1418	1418
16	tw.linkspot.search.yahoo.com	0	1413	1413	1413
17	ichart.finance.yahoo.com	0	1407	1407	1407
18	www.104.com.tw	0	1380	1380	1380
19	cmk.tw.yahoo.overture.com	0	1356	1356	1356
20	weather.noaa.gov	0	1291	1291	1291

Time: **2010/10/31(Sunday) ~ 2010/11/06(Saturday)** Total: **134250** Average: **19178.57 URLs/Day**

1

圖 13-12 網站管制歷史報告內容第一頁

NetBIOS Name / IP Address Top 20 Chart					
No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator
1	192.168.85.85	0	29177	29177	29177
2	172.19.100.32	0	8963	8963	8963
3	172.19.20.100	0	7408	7408	7408
4	172.19.100.111	0	7133	7133	7133
5	172.19.20.17	0	6110	6110	6110
6	172.19.100.106	0	5813	5813	5813
7	172.19.20.12	0	5381	5381	5381
8	172.19.100.44	0	4928	4928	4928
9	172.19.20.7	0	4796	4796	4796
10	172.19.0.1	0	4531	4531	4531
11	172.19.100.86	0	4321	4321	4321
12	172.19.200.164	0	4009	4009	4009
13	172.19.100.56	0	3516	3516	3516
14	172.19.20.15	0	3182	3182	3182
15	172.19.100.66	0	3003	3003	3003
16	172.19.100.51	0	2790	2790	2790
17	172.19.250.254	0	2646	2646	2646
18	172.19.100.46	0	2635	2635	2635
19	172.19.20.10	0	2321	2321	2321
20	172.19.50.19	0	2230	2230	2230
Time: **2010/10/31(Sunday) ~ 2010/11/06(Saturday)**				Total: **134251**	Average: **19178.71 URLs/Day**

2

圖 13-13 網站管制歷史報告內容第二頁

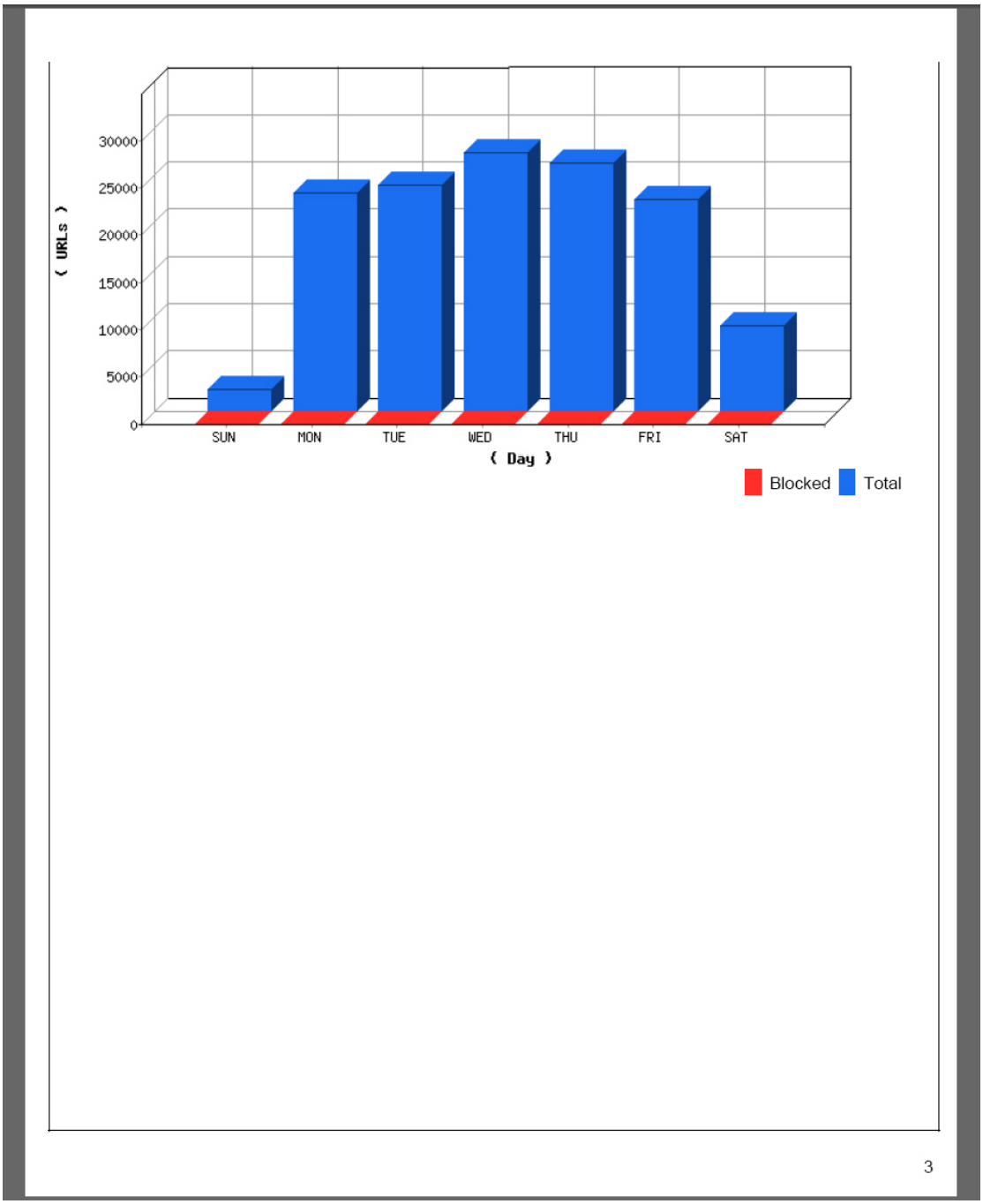
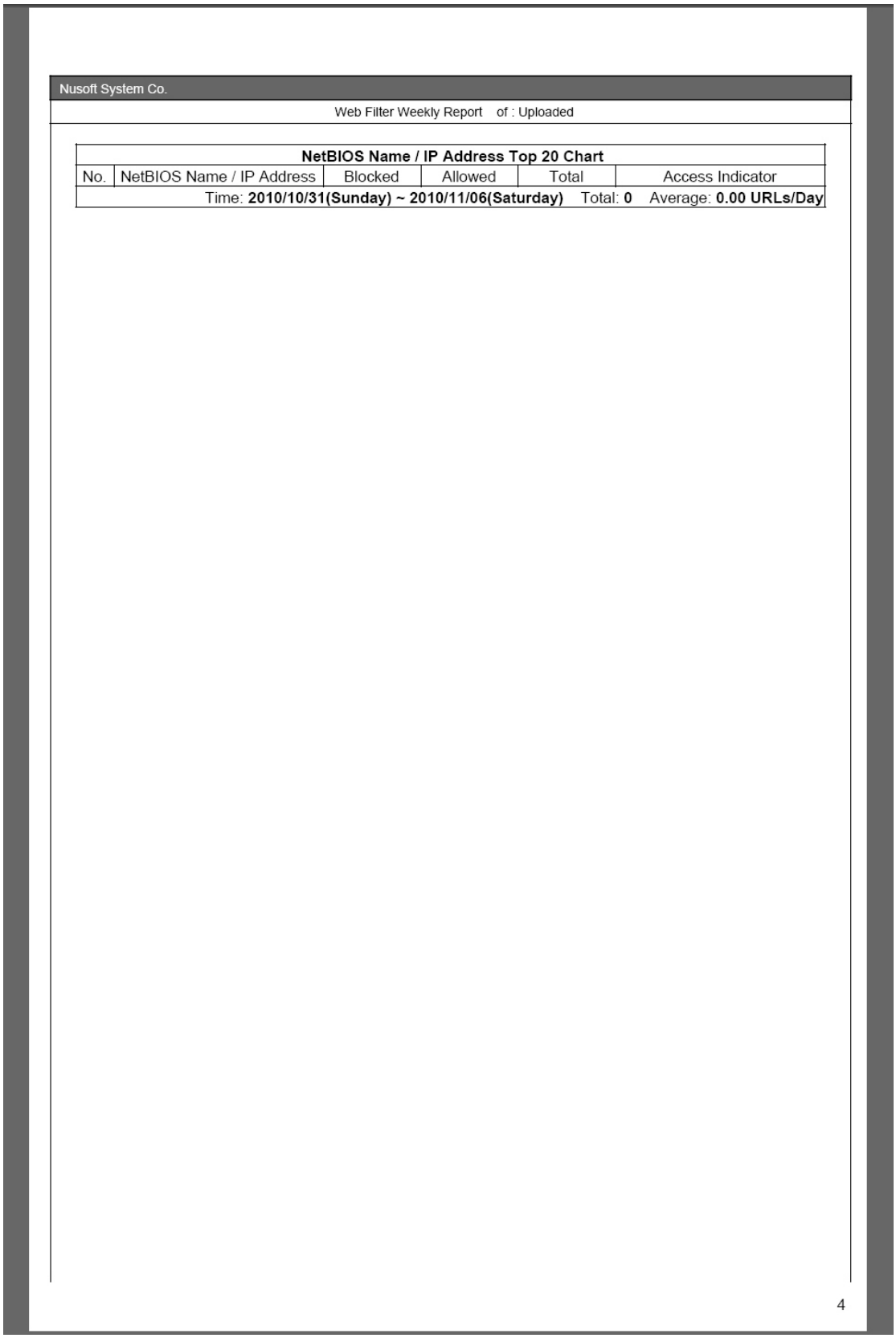


圖 13-14 網站管制歷史報告內容第三頁



Nusoft System Co.

Web Filter Weekly Report of : Uploaded

NetBIOS Name / IP Address Top 20 Chart					
No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator
Time: **2010/10/31(Sunday) ~ 2010/11/06(Saturday)** Total: **0** Average: **0.00 URLs/Day**					

4

圖 13-15 網站管制歷史報告內容第四頁

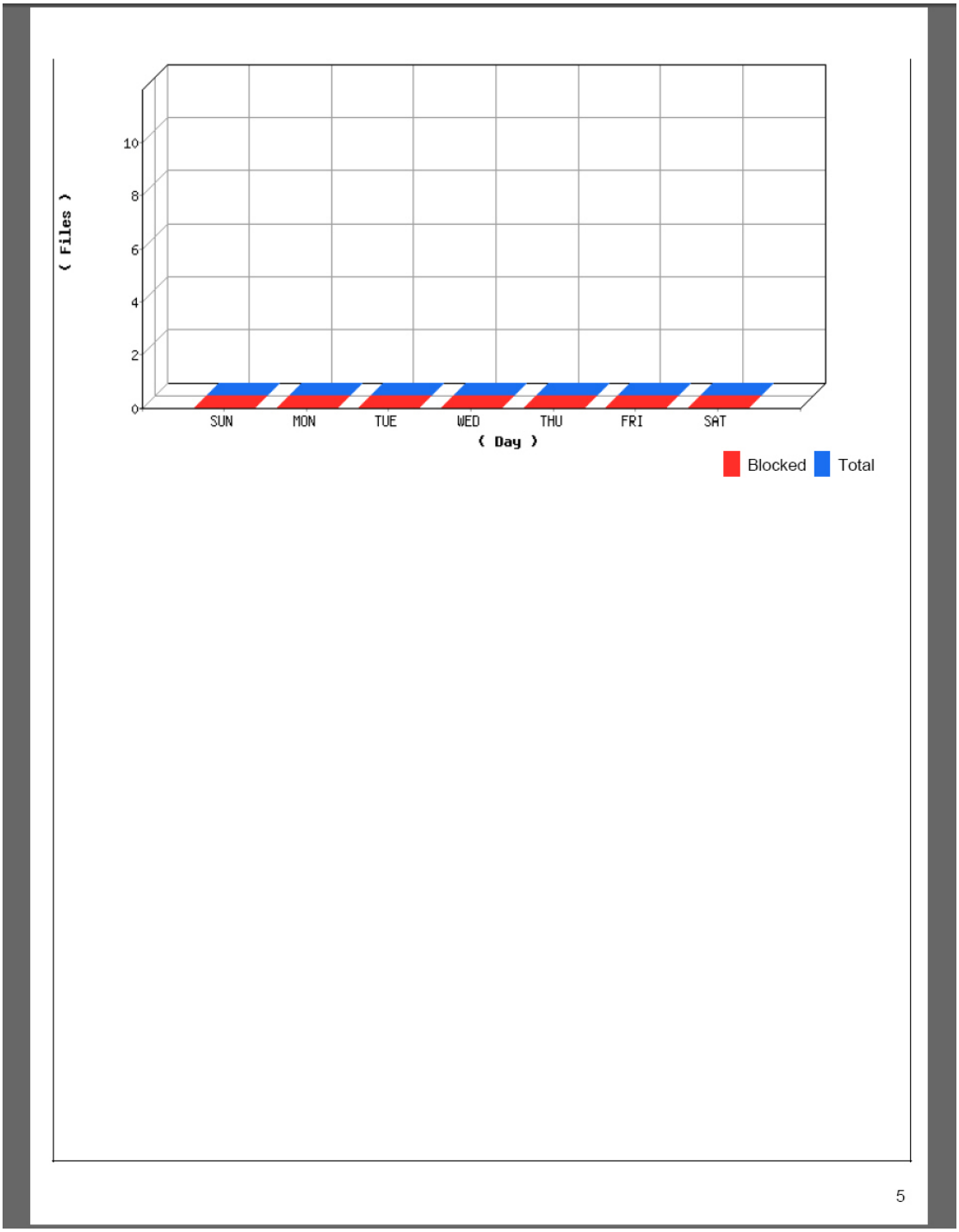


圖 13-16 網站管制歷史報告內容第五頁

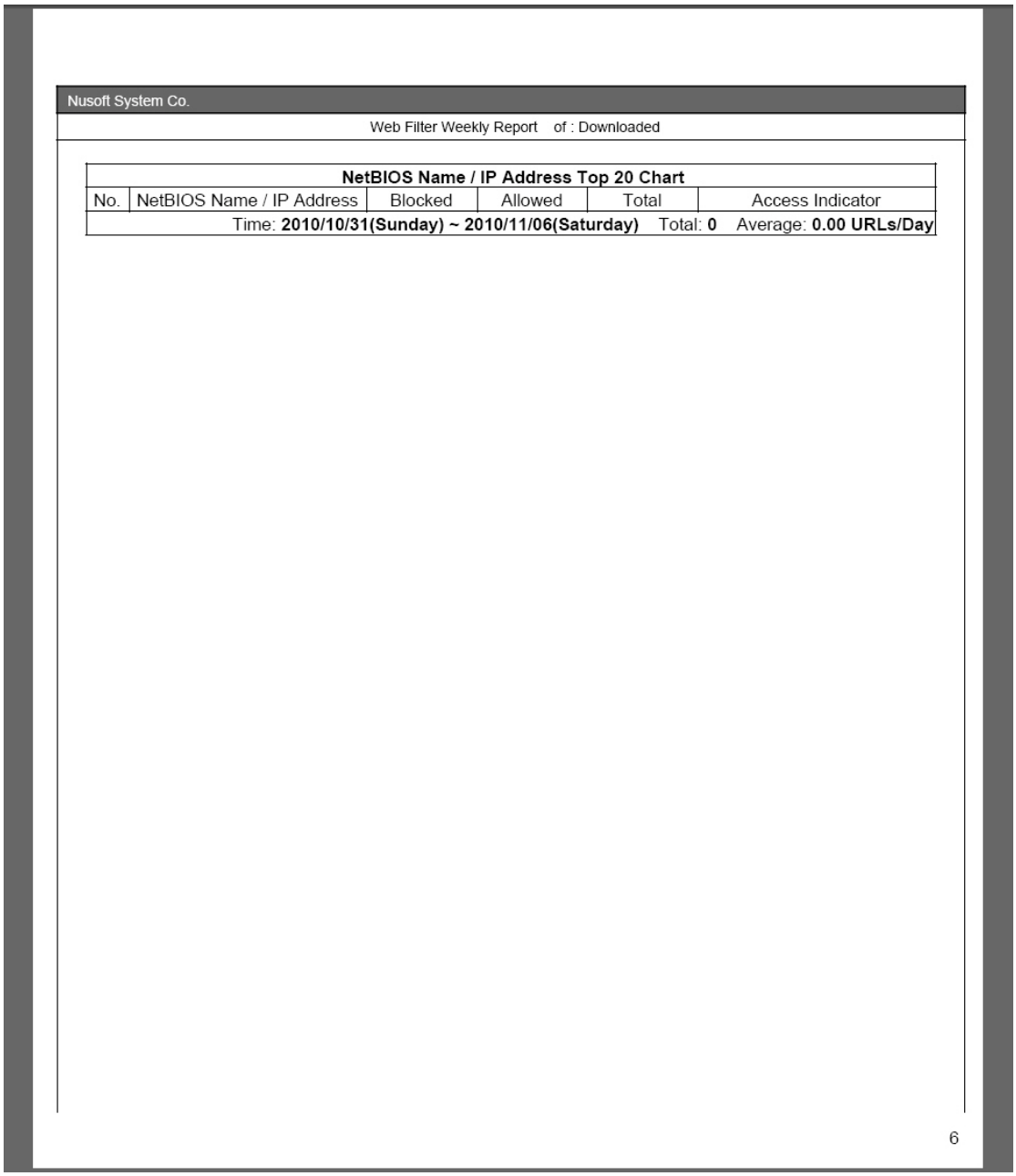


圖 13-17 網站管制歷史報告內容第六頁

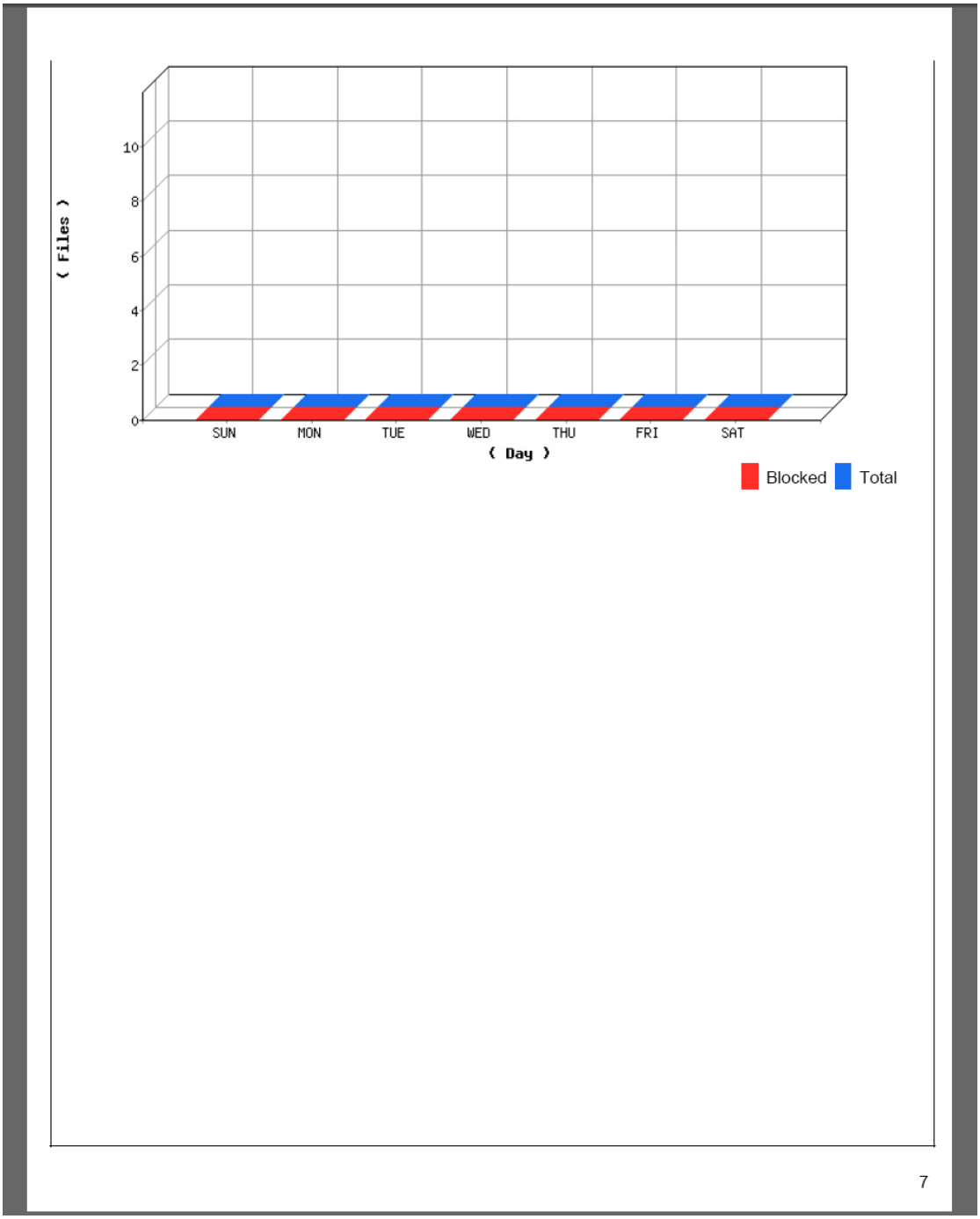


圖 13-18 網站管制歷史報告內容第七頁

【日誌】功能概述：

搜尋 說明如下：

- 網站類別：可依照日期、來源位址、網址、類別和處置方式等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- 檔案傳輸（上傳）：可依照日期、來源位址、網址、檔案名稱、管制規則和處置方式等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- 檔案傳輸（下載）：可依照日期、來源位址、網址、檔案名稱、管制規則和處置方式等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- MIME/Script：可依照日期、來源位址、網址、管制規則和處置方式等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【網站管制】>【網站管制報告】>【日誌】的【網站類別】>【搜尋】頁面中，做下列設定：
    - 開啟並設定搜尋指定時間區間內的記錄。
    - 選擇指定【類別】、【處置方式】。
    - 按下【搜尋】鈕。（如圖 13-19）
    - 按【下載】鈕，將目前搜尋到的記錄清單即時備份到本機電腦。（如圖 13-20）

時間	來源位址	網址	類別	處置方式
18:40:01	NAS	database.clamav.net	資訊安全	✔
18:40:01	NAS_128	database.clamav.net	資訊安全	✔
18:40:01	172.19.200.164	database.clamav.net	資訊安全	✔
18:40:01	NAS	database.clamav.net	資訊安全	✔
18:39:57	KONGMENG-CD32...	jbt.rfps.kh.edu.tw	教育	✔
18:39:57	KONGMENG-CD32...	www.gravatar.com	未分類	✔
18:39:56	KONGMENG-CD32...	jbt.rfps.kh.edu.tw	教育	✔
18:39:56	KONGMENG-CD32...	jbt.rfps.kh.edu.tw	教育	✔
18:39:56	KONGMENG-CD32...	jbt.rfps.kh.edu.tw	教育	✔
18:39:56	KONGMENG-CD32...	jbt.rfps.kh.edu.tw	教育	✔
18:39:55	KONGMENG-CD32...	jbt.rfps.kh.edu.tw	未分類	✔
18:39:51	V12	ap1.ks.vip.tw1.yahoo.com	教育	✔
18:39:50	V12	ad.yieldmanager.com	廣告 / 彈出式視窗	✔
18:39:50	V12	secure-yt.imrworldwide.com	商業	✔
18:39:50	V12	tw.pvc.news.yahoo.com	新聞與媒體	✔
18:39:50	V12	cmk.tw.yahoo.overture.com	廣告 / 彈出式視窗	✔
18:39:50	V12	tw.dcm.search.yahoo.com	搜尋引擎與入口網路	✔
18:39:49	V12	tw.linkspot.search.yahoo.com	搜尋引擎與入口網路	✔
18:39:47	V12	l.yimg.com	搜尋引擎與入口網路	✔
18:39:47	V12	tw.news.yahoo.com	新聞與媒體	✔

圖 13-19 搜尋特定記錄

說明：

1. 【網站管制】>【網站管制報告】>【日誌】的【網站類別】報表，可透過時間、來源位址、網址或類別做排序的動作。
2. 【網站管制】>【網站管制報告】>【日誌】的【檔案傳輸（上傳）】、【檔案傳輸（下載）】報表，可透過時間、來源位址、網址、檔案名稱或管制規則做排序的動作。
3. 【網站管制】>【網站管制報告】>【日誌】的【MIME/Script】報表，可透過時間、來源位址、網址或管制規則做排序的動作。

圖 13-20 下載搜尋到的記錄清單

13.1 統計

步驟1. 在【網站管制】>【網站管制報告】>【統計】頁面中，會顯示 MHG-2000 管制網站存取的統計報表。**（如圖 13-21）**

- 選擇指定【統計報表類型】。
- 點選【日】，可檢視以每日（Day）為單位的統計報表。
- 點選【週】，可檢視以週（Week）為單位的統計報表。
- 點選【月】，可檢視以月（Month）為單位的統計報表。
- 點選【年】，可檢視以年（Year）為單位的統計報表。

年 | 月 | 週 | 日　　日期：2011-03-25　　統計報表類型：網站類別

網站類別 排行榜　阻擋　允許　下載

名次	網站類別	阻擋	允許	全部	網站存取狀態
1	未分類	1	19347	19348	19348
2	資訊科技	0	146	146	146
3	搜尋引擎與入口網站	0	110	110	110
4	廣告 / 彈出式視窗	0	77	77	77
5	教育	0	46	46	46
6	資訊安全	0	36	36	36
7	商業	0	31	31	31
8	圖片分享	0	26	26	26
9	下載網站	0	23	23	23
10	串流媒體	0	23	23	23
11	購物	0	19	19	19
12	新聞與媒體	0	18	18	18
13	社交網站	0	18	18	18
14	個人網站	0	14	14	14
15	一般	0	9	9	9
16	非營利 / 非政府組織	0	7	7	7
17	娛樂	0	6	6	6
18	藝術	0	5	5	5
19	線上聊天	0	5	5	5
20	即時訊息傳送	0	5	5	5

時間: 2011/03/25 00:00 ~ 2011/03/25 18:49　總計: 19975　平均: 1051.32 瀏覽網站/時

網站位址 / 網域 排行榜　阻擋　允許　下載

名次	網站位址 / 網域	阻擋	允許	全部	檔案傳輸狀態
1	ad.yieldmanager.com	0	928	928	928
2	database.clamav.net	0	918	918	918
3	l.yimg.com	0	856	856	856
4	tw.yimg.com	0	697	697	697
5	dev.sencha.com	0	614	614	614
6	61.152.248.238:8080	0	485	485	485
7	www.bot.com.tw	0	444	444	444
8	secure-yt.imrworldwide.com	0	394	394	394
9	ichart.finance.yahoo.com	0	355	355	355
10	cmk.tw.yahoo.overture.com	0	289	289	289
11	tw.rd.yahoo.com	0	282	282	282
12	tw.yahoo.com	0	280	280	280
13	futai.com.tw	0	266	266	266
14	tw.linkspot.search.yahoo.com	0	256	256	256
15	tw.news.yahoo.com	0	243	243	243
16	61.219.32.242	0	226	226	226
17	www.google.com.tw	0	224	224	224
18	safebrowsing.clients.google.com	0	210	210	210
19	safebrowsing-cache.google.com	0	207	207	207
20	cmx.tw.yahoo.overture.com	0	192	192	192

時間: 2011/03/25 00:00 ~ 2011/03/25 18:49　總計: 19975　平均: 1051.32 瀏覽網站/時

電腦名稱 / IP位址 排行榜　阻擋　允許　下載

名次	電腦名稱 / IP位址	阻擋	允許	全部	檔案傳輸狀態
1	192.168.85.85	0	3563	3563	3563
2	NUSOFT-RD31	0	1960	1960	1960
3	V12	0	1405	1405	1405
4	NUSOFT-WIN	0	1336	1336	1336
5	RAYEARTH111	0	1258	1258	1258
6	NMXDSOOQRDJ	1	1021	1022	1022
7	172.19.20.17	0	910	910	910
8	172.19.100.8	0	872	872	872
9	P-4UQTBTY91ACAI	0	791	791	791
10	NOKIA-DESKTOP	0	766	766	766
11	172.19.100.56	0	712	712	712
12	172.19.100.32	0	517	517	517
13	172.19.100.76	0	513	513	513
14	KONGMENG-CD32DC	0	491	491	491
15	172.19.0.2	0	394	394	394
16	172.19.100.66	0	384	384	384
17	172.19.100.36	0	344	344	344
18	NUSOFT-261E54D2	0	248	248	248
19	172.19.50.123	0	226	226	226
20	JULIE	0	225	225	225

時間: 2011/03/25 00:00 ~ 2011/03/25 18:49　總計: 19975　平均: 1051.32 瀏覽網站/時

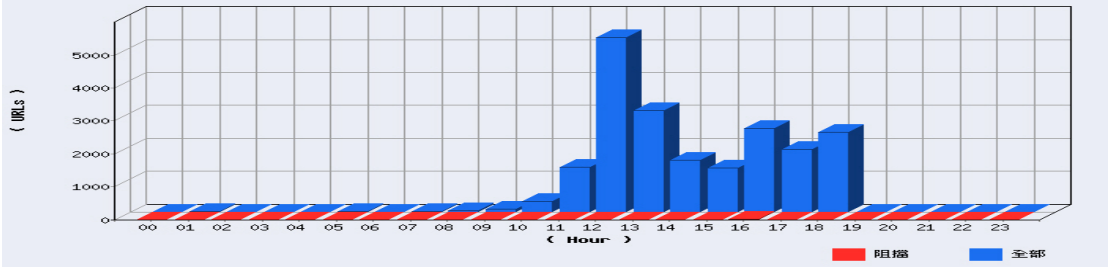


圖 13-21 網站管制統計報表

13.2 日誌

步驟1. 在【網站管制】>【網站管制報告】>【日誌】頁面中，會顯示目前 MHG-2000 的網站管制狀況。（如圖 13-22）

圖 13-22 網站管制日誌

SSL Web VPN

第14章　SSL Web VPN

由於網際網路的普遍應用，企業遠端安全登入的需求也與日俱增。對於使用者而言，最方便安全的解決方案莫過於 SSL Web VPN，用戶端只要使用標準的瀏覽器，就可直接透過 SSL 安全加密協定傳輸資料。

【VPN】專有名詞概述：

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，使用的加密金鑰爲 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，使用的加密金鑰爲 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。

【SSL Web VPN 精靈】功能概述：

SSL Web VPN 精靈 說明如下：

- 依照系統提示逐步完成建立 SSL Web VPN 連線的設定。
  - 在【SSL Web VPN】>【SSL Web VPN 精靈】頁面中，做下列設定：
    - 按【下一步】鈕，來開始設定。**（如圖 14-1）**
    - 輸入允許 SSL Web VPN 連線的內部子網路，按【下一步】鈕。**（如圖 14-2）**
    - 建立 SSL Web VPN 連線驗證帳號，按【下一步】鈕。**（如圖 14-3）**
    - 設定 SSL Web VPN 連線驗證帳號群組，按【下一步】鈕。**（如圖 14-4）**
    - 設定允許 SSL Web VPN 連線透過 VNC、HTTP、HTTPS 存取指定內網 PC 開啟的服務，或直接遠端喚醒指定內網 PC，按【下一步】鈕。**（如圖 14-5）**
    - 設定 SSL Web VPN 連線規則，按【下一步】鈕。**（如圖 14-6）**
    - 按下【完成】鈕。**（如圖 14-7, 圖 14-8）**
    - 此時會完成套用 SSL Web VPN 的相關【管制條例】設定，並於 SSL Web VPN 建起連線時，能正常透過此機制傳輸封包。**（如圖 14-9, 圖 14-10）**

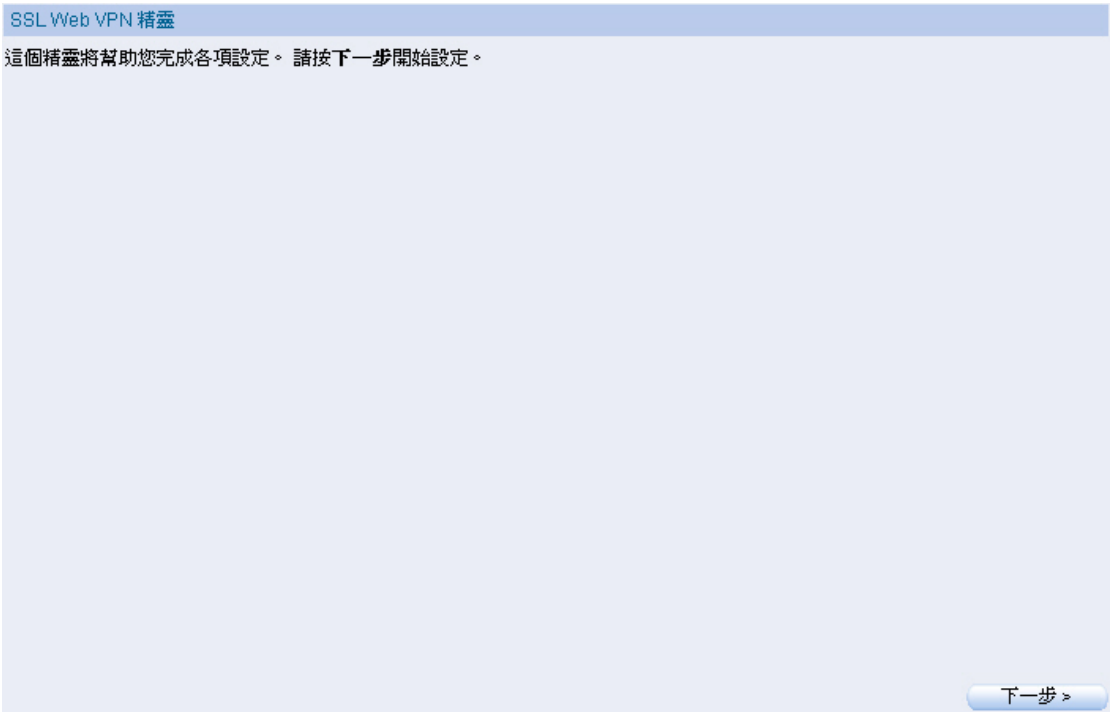


圖 14-1SSL Web VPN 精靈頁面

圖 14-2 設定允許連線的內部子網路

圖 14-3 建立連線驗證帳號

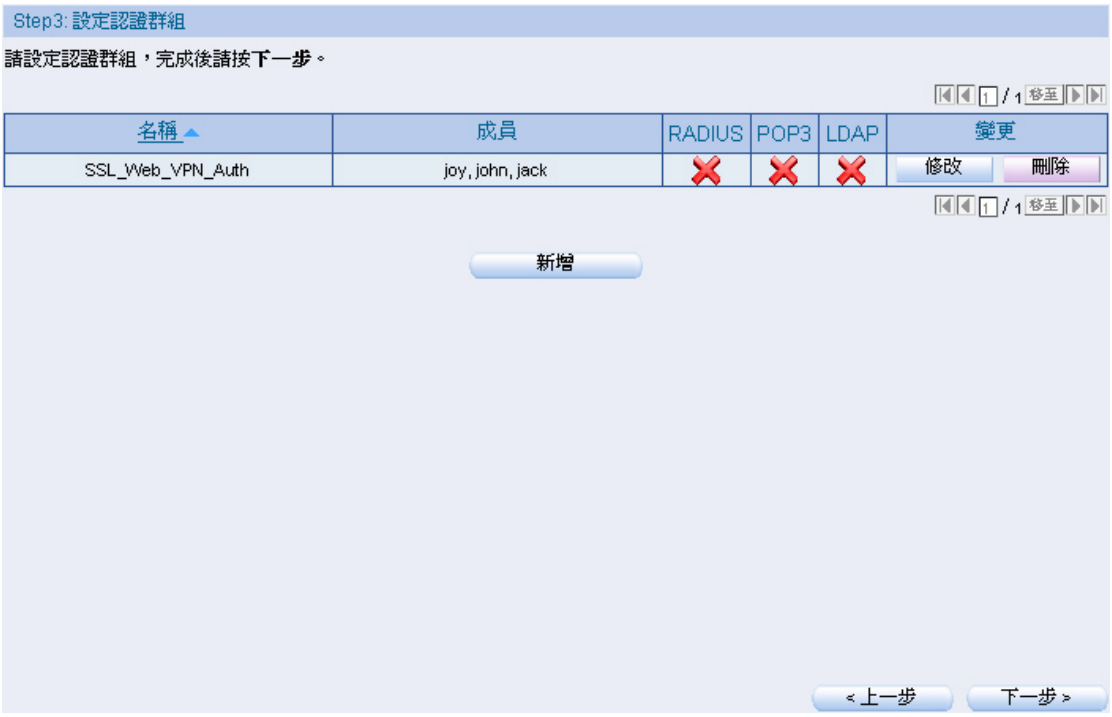


圖 14-4 設定連線驗證帳號群組

圖 14-5 設定 SSL 應用

圖 14-6 設定 SSL Web VPN 連線規則

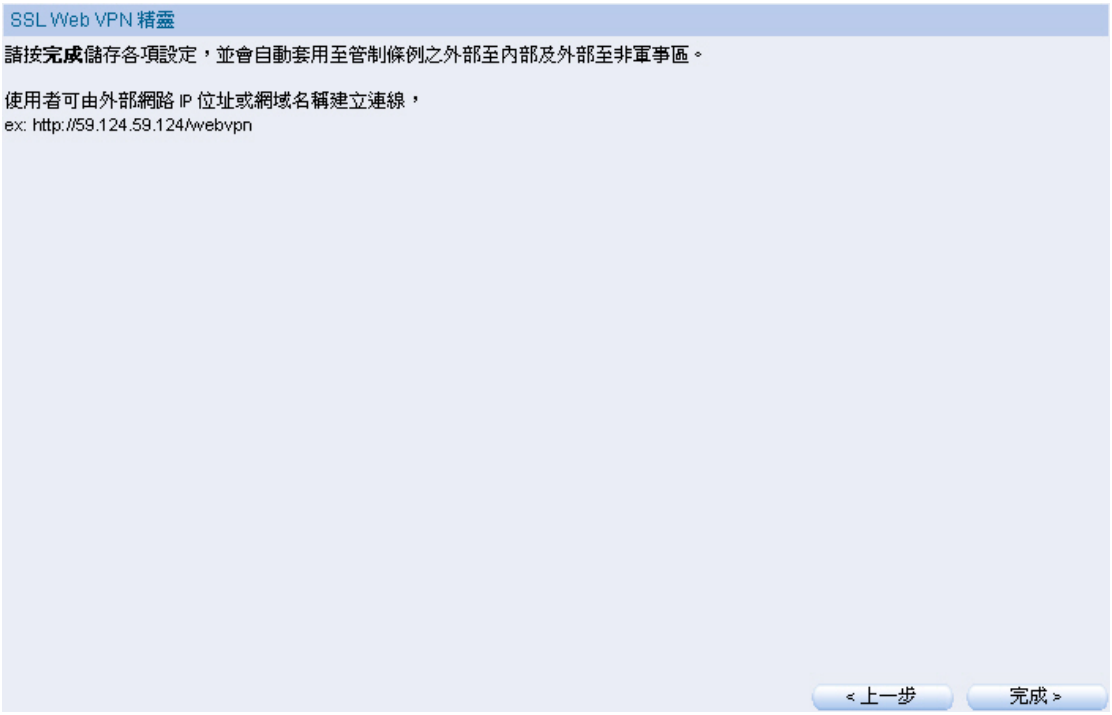


圖 14-7 注意事項

圖 14-8 完成 SSL Web VPN 連線設定

圖 14-9 完成 SSL Web VPN 外部至內部管制條例的設定

圖 14-10 完成 SSL Web VPN 外部至非軍事區管制條例的設定

【設定】功能概述：

SSL Web VPN 組態設定 說明如下：

- 可設定用戶端和 MHG-2000 建立 SSL Web VPN 連線時，採用的網際協定、IP 位址配發範圍、加密演算法、安全性憑證、通訊協定、埠號，是否要配發指定的 DNS（或 WINS）伺服器位址和連線狀態偵測。
- 設定用戶端可存取的伺服器端子網路。

說明：

1. SSL Web VPN IP 位址配發範圍不可等同或被包含於 MHG-2000 其他功能、介面已採用的網段。

名稱 說明如下：

- SSL Web VPN 連線認證規則的辨識名稱。

使用之認證帳戶或群組 說明如下：

- SSL Web VPN 連線驗證時比對的【管制條例選項】>【認證表】>【認證帳戶】、【認證群組】規則。

硬體認證 說明如下：

- 可讓曾和 MHG-2000 建立 SSL Web VPN 帳密認證連線，並列於【SSL Web VPN】>【硬體認證帳戶管理】頁面的設備，無需輸入帳密直接進行 SSL Web VPN 連線。

SSL 應用 說明如下：

- 可讓使用者在和 MHG-2000 建立 SSL Web VPN 連線時，透過特定的介面存取在【SSL Web VPN】>【SSL 應用】頁面中設定的指定應用項目。

【硬體認證帳戶管理】功能概述：

硬體認證帳戶清單 說明如下：

- 表列曾和 MHG-2000 建立 SSL Web VPN 帳密認證連線的設備資訊。

說明：

1. 若使用者曾輸入驗證帳號及密碼和 MHG-2000 建立 SSL Web VPN 連線，可由系統管理員將其連線時使用的硬體資訊，加入【SSL Web VPN】>【設定】頁面的【SSL Web VPN 認證方式設定】欄位中之【硬體認證】清單，往後使用者利用同台電腦和 MHG-2000 建立 SSL Web VPN 連線便不必再輸入帳號、密碼。

【SSL 應用】功能概述：

SSL 應用清單 說明如下：

- 設定可讓使用者透過和 MHG-2000 建立 SSL Web VPN 連線的介面，來直接存取的特定 VNC 連線、HTTP 連線、HTTPS 連線、遠端喚醒等應用項目。

【連線狀態】概述：

認證帳戶 說明如下：

- 顯示用戶端所使用的認證名稱。

電腦名稱 說明如下：

- 顯示用戶端電腦的主機名稱。

真實 IP 說明如下：

- 顯示用戶端所使用的真實 IP。

VPN IP 說明如下：

- 顯示 MHG-2000 配發給用戶端的 IP。

連線歷時 說明如下：

- 顯示用戶端與 MHG-2000 的持續連線時間。

變更 說明如下：

- 可中斷和 MHG-2000 建立的 SSL Web VPN 連線。（如圖 14-11）

認證帳戶	電腦名稱	真實 IP	VPN IP	連線歷時	變更
沒有記錄！					

圖 14-11SSL Web VPN 連線狀態表

14.1 SSL Web VPN 功能使用範例

14.1.1 外部用戶端和 MHG-2000 建立 SSL Web VPN 連線的方法

步驟1. 在【網路介面】>【介面位址】頁面中，開啟外部網路介面的 HTTPS 系統管理：（如圖 14-12）

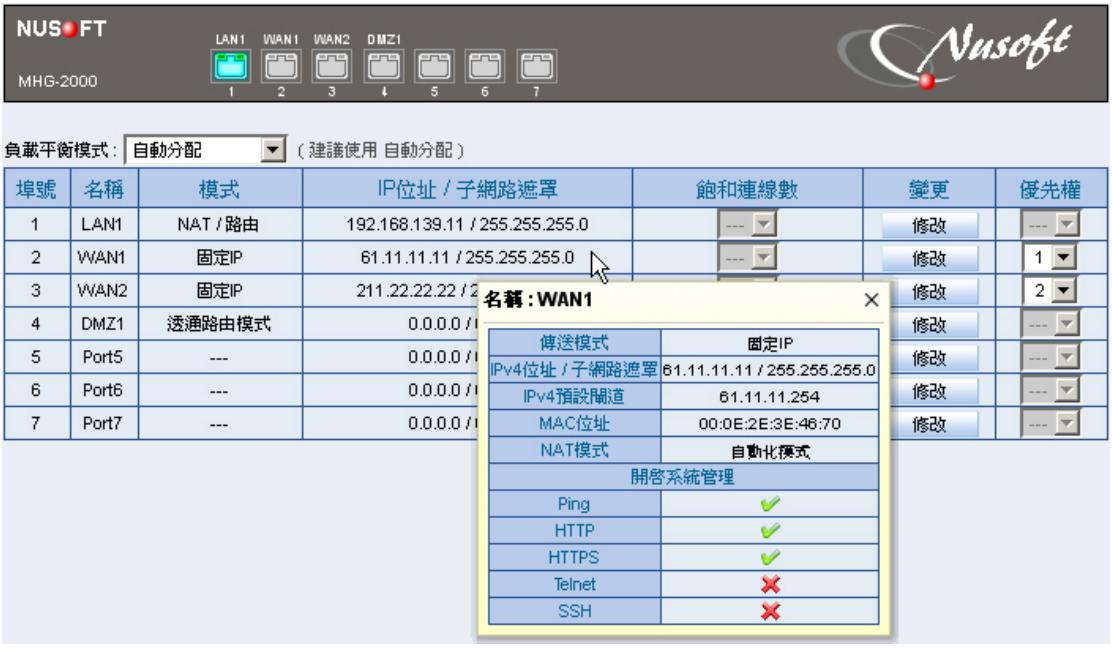


圖 14-12 外部網路介面設定

步驟2. 在【管制條例選項】>【認證表】>【認證帳戶】和【認證群組】頁面中，做下列設定：（如圖 14-13, 圖 14-14）

圖 14-13 認證帳戶設定

圖 14-14 認證群組設定

步驟3. 在【SSL Web VPN】>【設定】頁面中，做下列設定：

- 按下【修改】鈕。（如圖 14-15）
- 勾選【啟用 SSL Web VPN】。
- 選擇欲採用的【網際協定】。
- 輸入指定的【配給用戶端的 IP 位址範圍】。
- 選擇欲採用的【加密演算法】、【CA 憑證】、【本地授權憑證】、【遠端授權憑證】、【通訊協定】。
- 輸入欲採用的【連線埠號】。
- 設定允許用戶端存取的內部網段。
- 按下【確定】鈕。（如圖 14-16）
- 按下【新增】鈕。（如圖 14-17）
- 輸入所指定的 SSL Web VPN 連線認證規則【名稱】。
- 【使用之認證帳戶或群組】選擇所設定的認證帳戶、群組規則。
- 按下【確定】鈕，完成設定。（如圖 14-18）

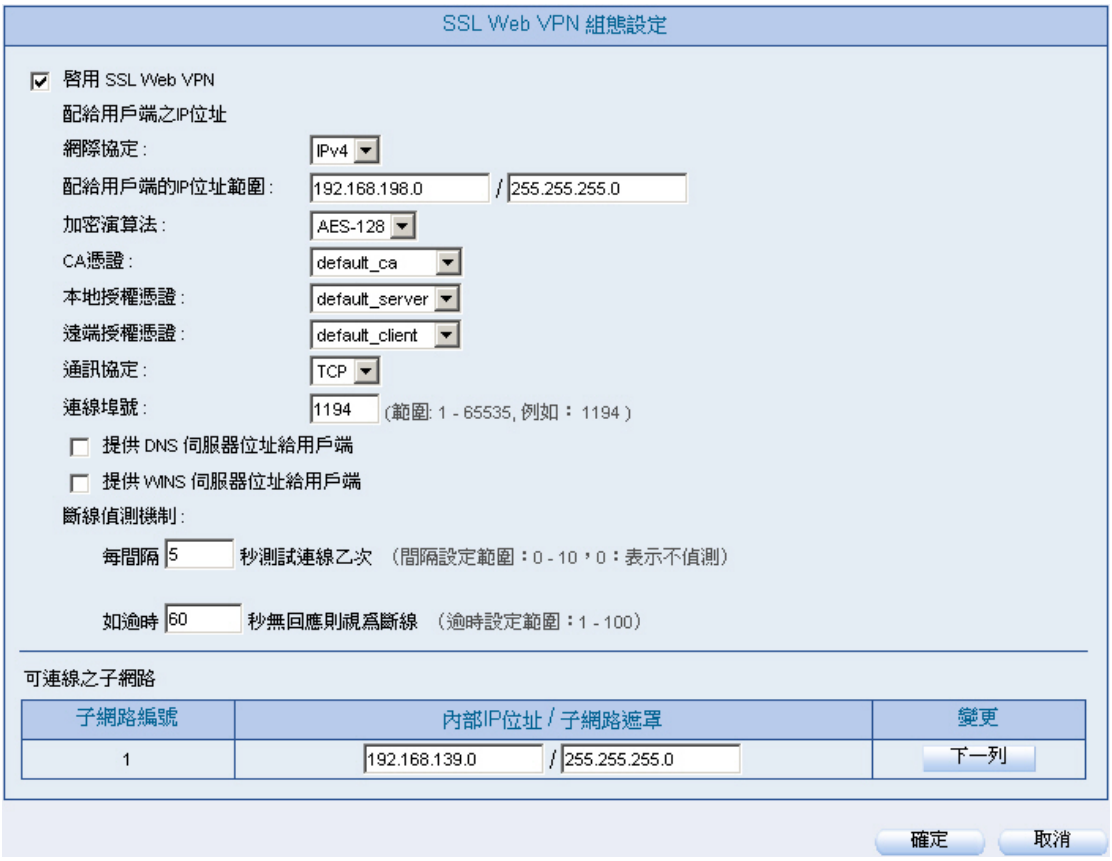


圖 14-15 啟動並設定 SSL Web VPN 用戶端組態

說明：

1. 可以指定的【進階功能】>【證書管理】>【本地 CA 憑證】、【遠端 CA 憑證】做為【CA 憑證】。

2. 可以將輸入 MHG-2000 的憑證申請書，經上述特定 Root CA 簽核後的【進階功能】>【證書管理】>【授權憑證】做為【本地授權憑證】、【遠端授權憑證】。

圖 14-16 完成 SSL Web VPN 組態設定

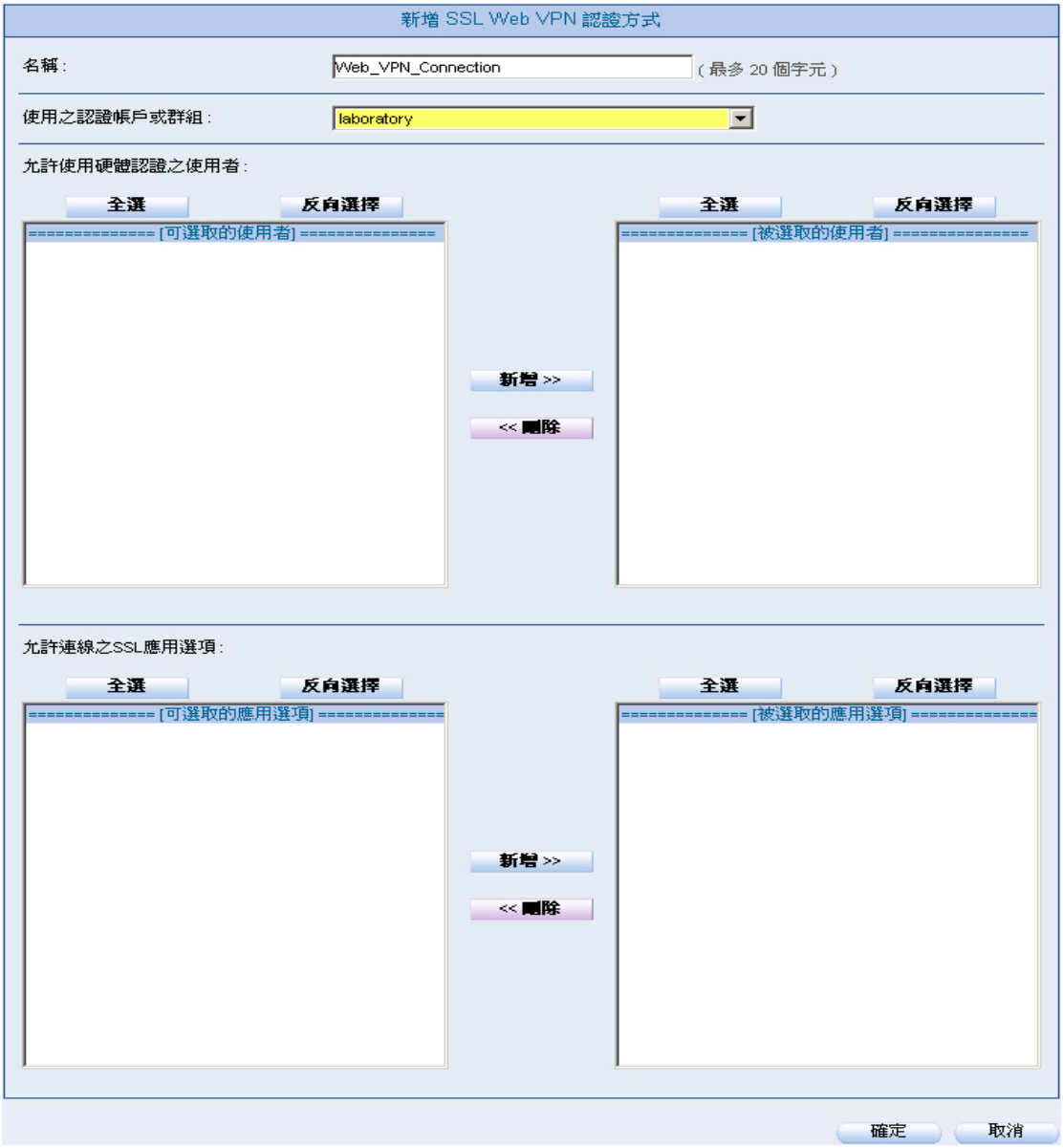


圖 14-17 設定 SSL Web VPN 認證

圖 14-18 完成 SSL Web VPN 認證設定

步驟4. 在【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 14-19）

- 【VPN】選擇所設定的 SSL Web VPN 規則。
- 按下【確定】鈕，完成設定。（如圖 14-20）

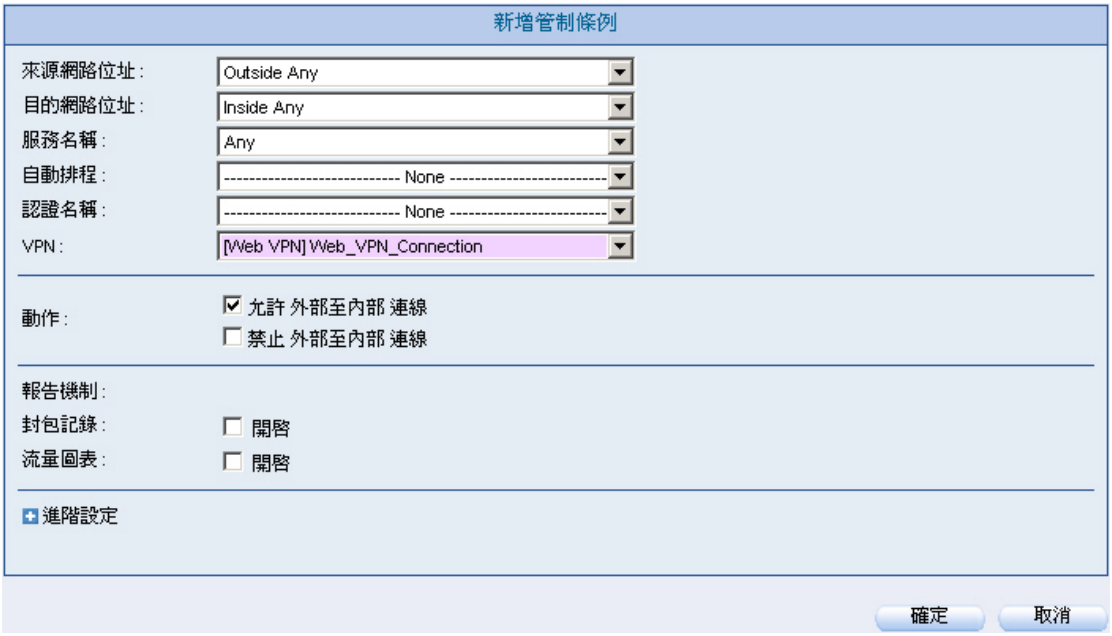


圖 14-19 設定 SSL Web VPN 外部至內部之管制條例

圖 14-20 完成管制條例設定

步驟5. 用戶端於瀏覽器中做下列設定：

- 【網址】輸入 http:// MHG-2000 介面位址/webvpn。
- 按下鍵盤的【Enter】鍵。**（如圖 14-21）**
- 於【安全性警訊】視窗中，按下【是】鈕。**（如圖 14-22）**
- 於【警告 - 安全】視窗中，按下【是】鈕。**（如圖 14-23）**
- 再次於【警告 – 安全】視窗中，按下【執行】鈕。**（如圖 14-24）**
- 於【SSL Web VPN 認證】視窗中，選擇【語言版本】、輸入【認證名稱】和【認證密碼】。**（如圖 14-25）**
- 按下【確定】鈕，建立連線。**（如圖 14-26, 圖 14-27, 圖 14-28）**

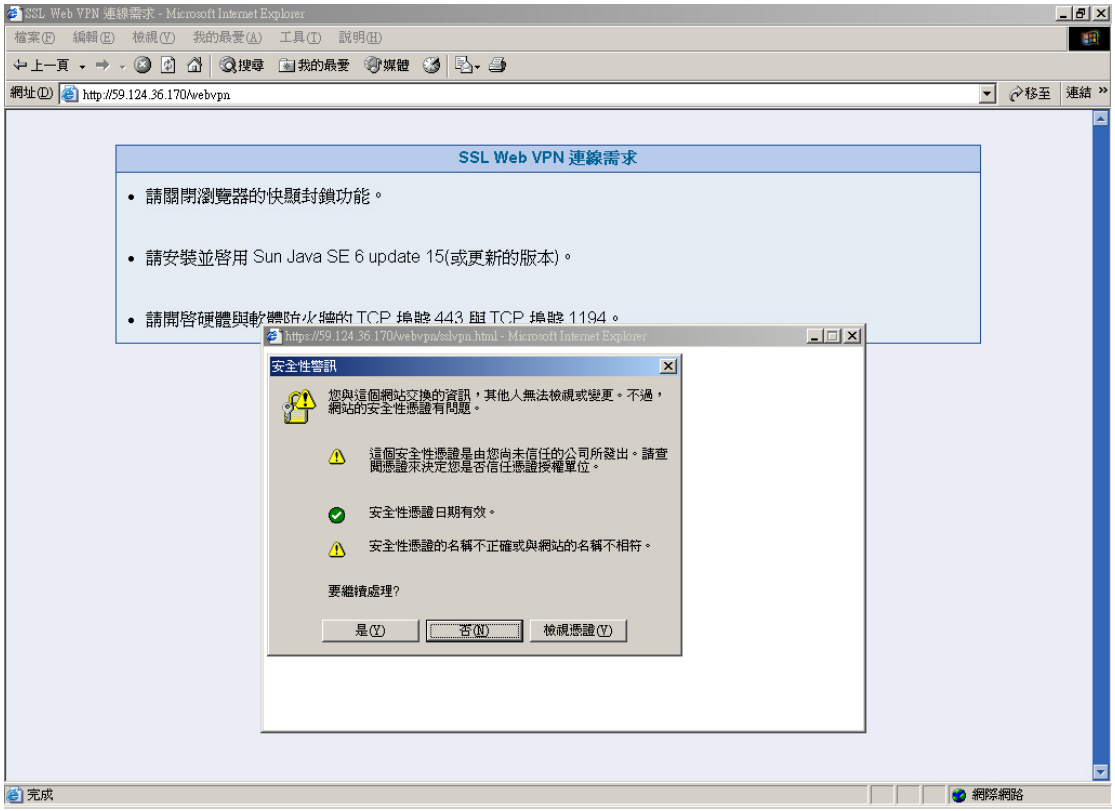


圖 14-21SSL Web VPN 連線頁面

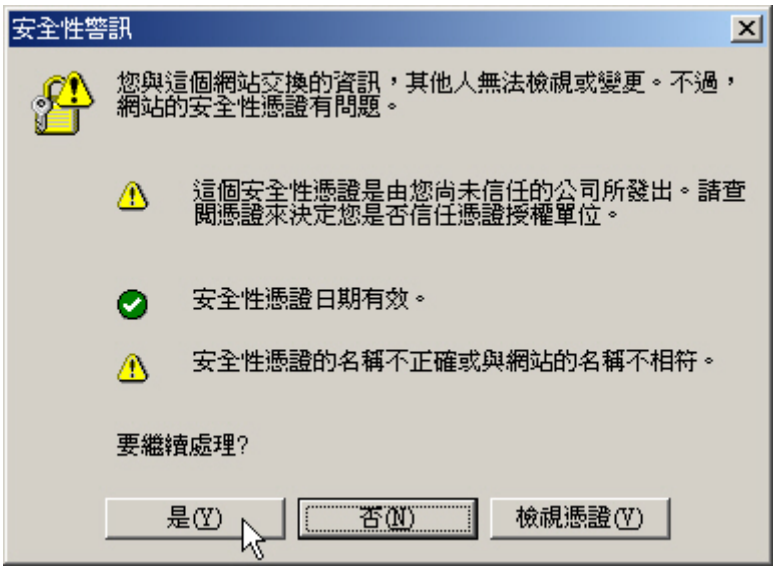


圖 14-22 安全性警訊視窗

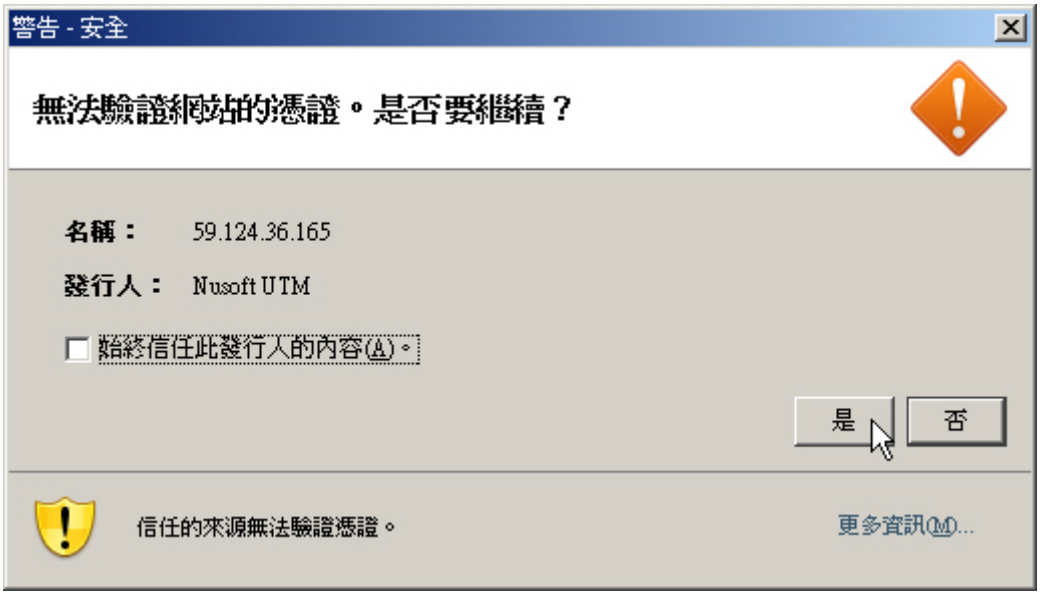


圖 14-23 警告 - 安全視窗

圖 14-24 警告 - 安全視窗

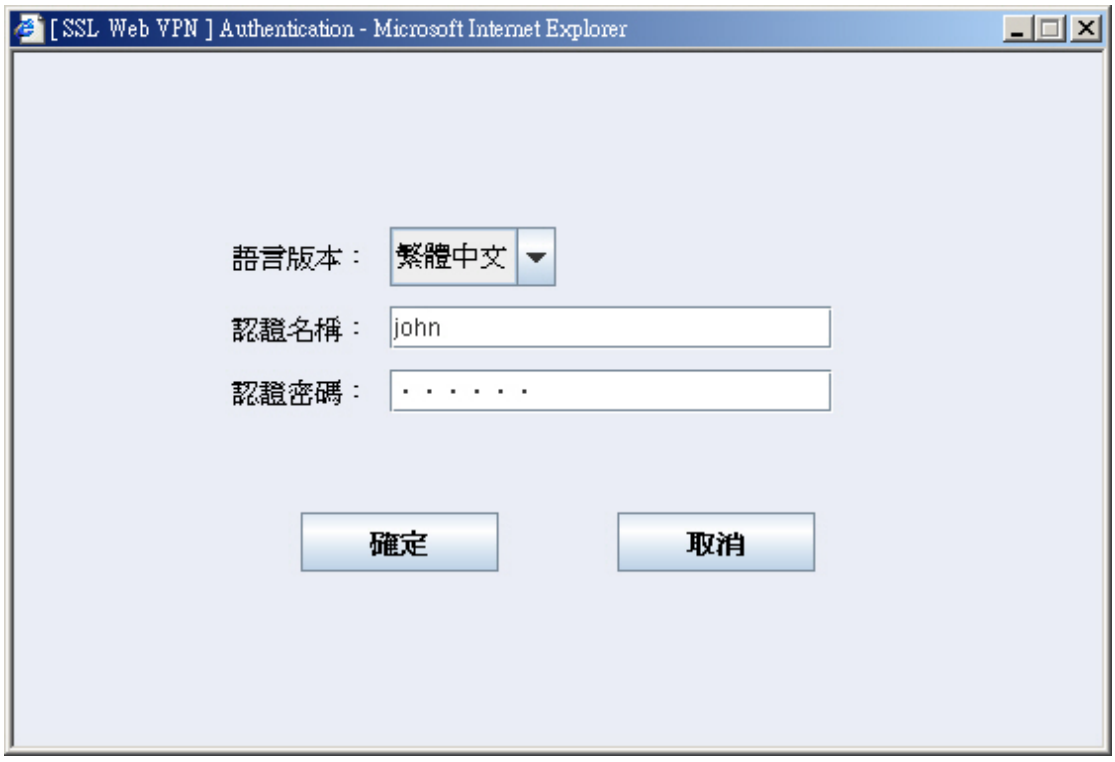


圖 14-25SSL Web VPN 帳密認證視窗

圖 14-26SSL Web VPN 連線視窗

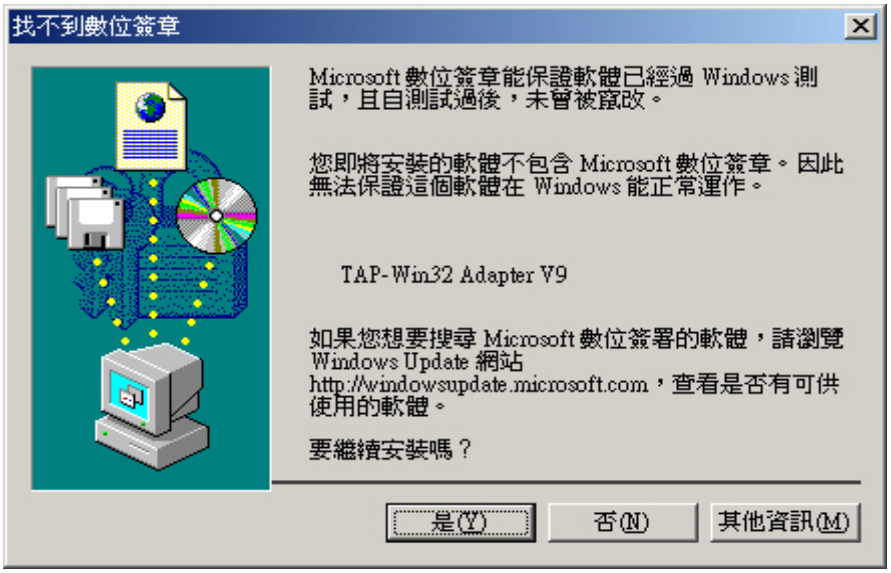


圖 14-27 初次連線安裝 SSL Web VPN 網卡

圖 14-28 完成 SSL Web VPN 連線

步驟6. 在【SSL Web VPN】>【連線狀態】頁面中，顯示如下連線訊息：（如圖 14-29）

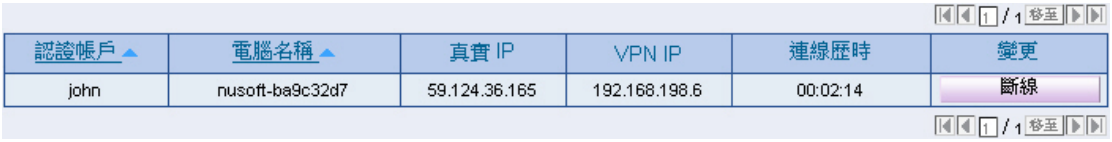


圖 14-29SSL Web VPN 帳密認證連線狀態

步驟7. 在【SSL Web VPN】>【硬體認證帳戶管理】頁面中，顯示曾和 MHG-2000 建立 SSL Web VPN 帳密認證連線的設備資訊。（如圖 14-30）

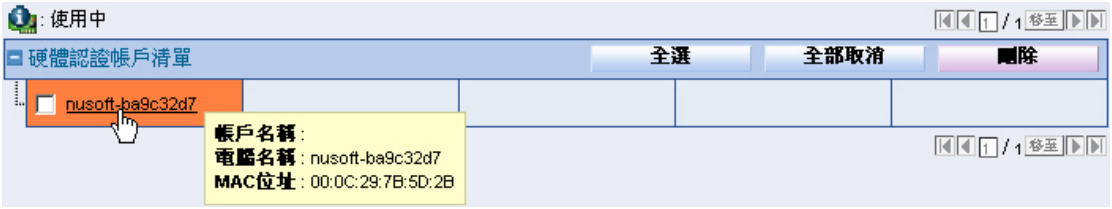


圖 14-30 曾和 MHG-2000 建立 SSL Web VPN 帳密認證連線的設備資訊

步驟8. 在【SSL Web VPN】>【設定】頁面的【SSL Web VPN 認證方式設定】欄位中，做下列設定：（如圖 14-31）

- 按下【修改】鈕。
- 於【允許使用硬體認證之使用者】列表中，將【可選取的使用者】新增至【被選取的使用者】清單中。
- 按下【確定】鈕，完成設定。（如圖 14-32）

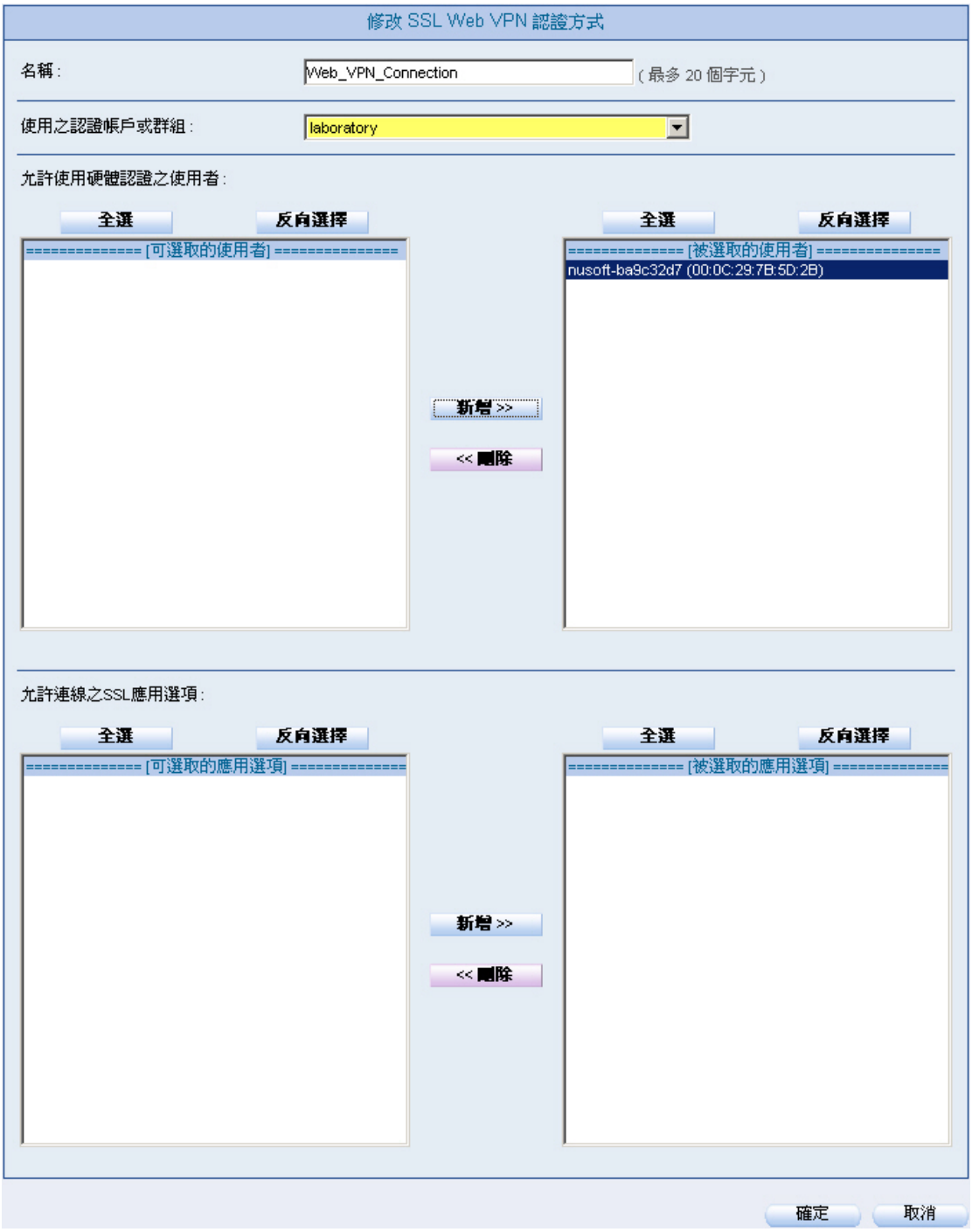


圖 14-31 設定 SSL Web VPN 硬體認證

圖 14-32 完成 SSL Web VPN 硬體認證設定

步驟9. 爾後當使用者透過同台電腦和 MHG-2000 建立 SSL Web VPN 連線時，將可以直接通過硬體認證機制，免去輸入帳號密碼的步驟。（如圖 14-33, 圖 14-34）

圖 14-33SSL Web VPN 硬體認證視窗

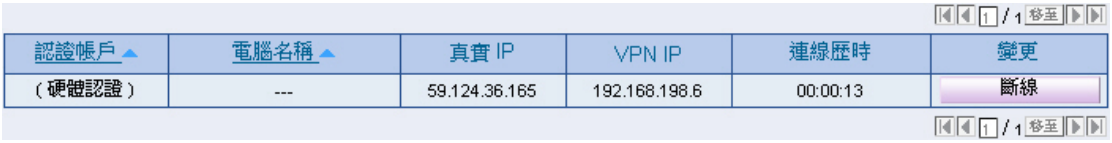


圖 14-34SSL Web VPN 硬體認證連線狀態

步驟10. 在【SSL Web VPN】>【SSL 應用】頁面中，做下列設定：（如圖 14-35）

- 按下【新增】鈕。
- 輸入指定的 SSL 應用規則【名稱】。
- 輸入指定的【辦公室電腦 IP 位址】，並設定和開啟其相關 VNC 連線、HTTP 連線、HTTPS 連線、遠端喚醒等應用項目。
- 按下【確定】鈕，完成設定。（如圖 14-36）

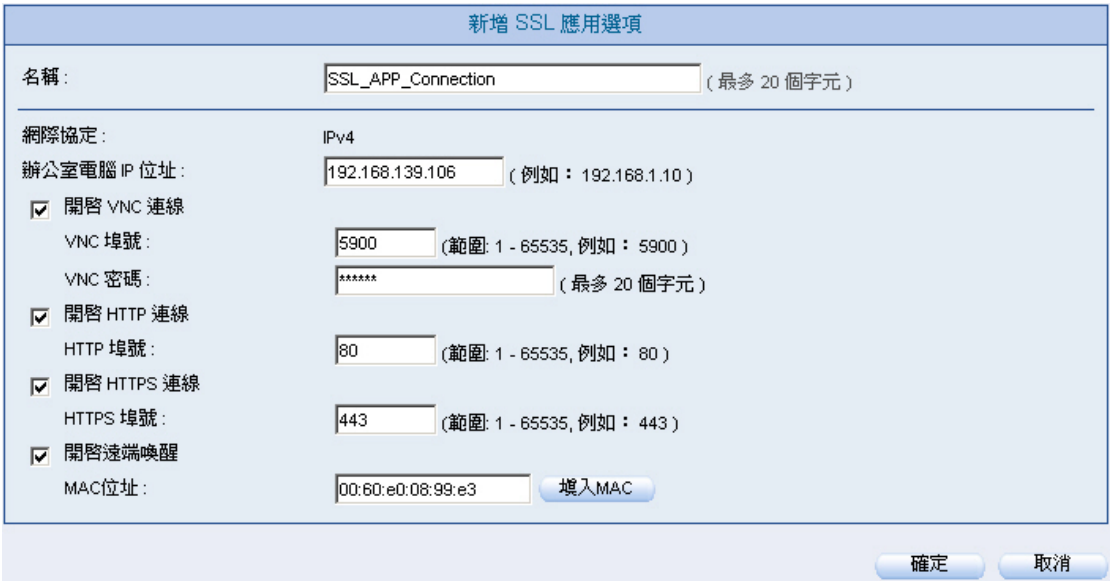


圖 14-35 設定 SSL 應用

圖 14-36 完成 SSL 應用設定

說明：

1. 若提供 SSL 應用的主機在有需要時才開機，可【開啟遠端喚醒】功能以達到此需求。

步驟11. 在【SSL Web VPN】>【設定】頁面的【SSL Web VPN 認證方式設定】欄位中，做下列設定：（如圖 14-37）

- 按下【修改】鈕。
- 於【允許連線之 SSL 應用選項】列表中，將【可選取的應用選項】新增至【被選取的應用選項】清單中。
- 按下【確定】鈕，完成設定。（如圖 14-38）

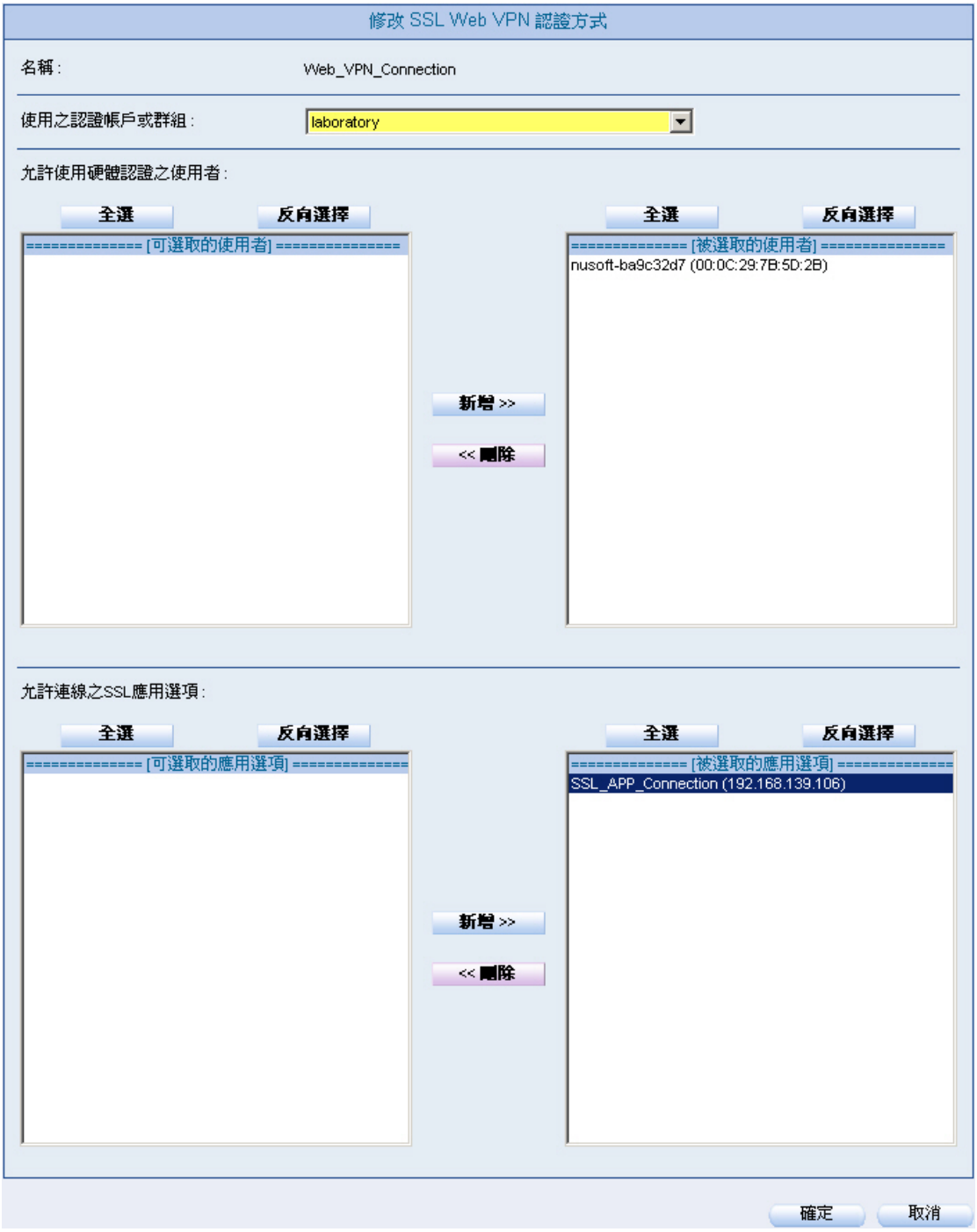


圖 14-37 設定 SSL Web VPN 應用選項

圖 14-38 完成 SSL Web VPN 應用選項設定

步驟12. 當使用者和 MHG-2000 建立 SSL Web VPN 連線時，可透過連線介面選擇指定的應用選項，直接存取特定主機提供的應用項目。（如圖 14-39, 圖 14-40）

圖 14-39 於 SSL Web VPN 連線介面選擇指定應用選項

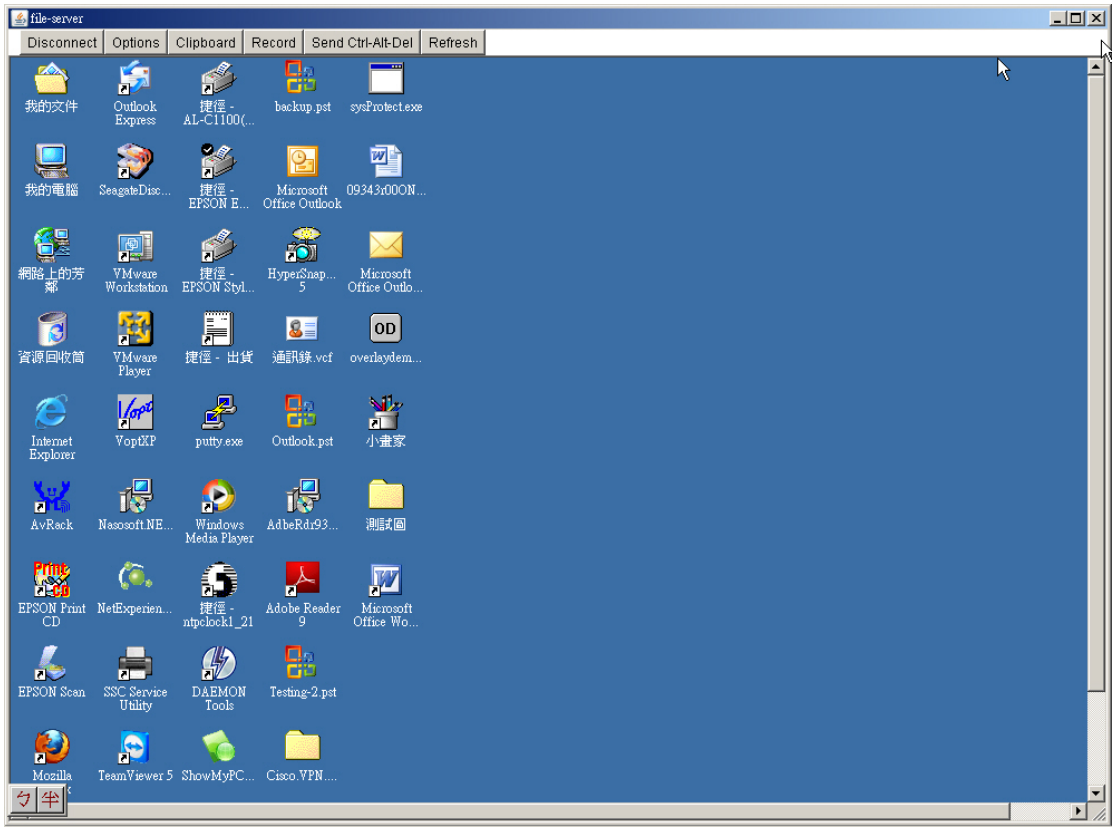


圖 14-40 存取特定主機提供的應用項目

說明：

1. 設定硬體認證並採用認證帳戶或群組：（系統會先進行硬體認證）
   - 若使用者 PC 硬體資訊被加入【SSL Web VPN】>【設定】頁面的連線認證規則清單，可直接完成 SSL Web VPN 連線。
   - 若使用者 PC 硬體資訊未被加入【SSL Web VPN】>【設定】頁面的連線認證規則清單，需輸入認證名稱和密碼做認證，決定是否可建立 SSL Web VPN 連線。
   - 當使用者 PC 和 MHG-2000 初次建立 SSL Web VPN 連線時，其硬體資訊不在【SSL Web VPN】>【硬體認證帳戶管理】名單中，需輸入驗證名稱和密碼做認證。（此時系統會自動將使用者 PC 的硬體資訊加入名單）
2. 僅設定硬體認證：
   - 若使用者 PC 硬體資訊被加入【SSL Web VPN】>【設定】頁面的連線認證規則清單，可直接完成 SSL Web VPN 連線。
   - 若使用者 PC 硬體資訊未被加入【SSL Web VPN】>【設定】頁面的連線認證規則清單，無法建立 SSL Web VPN 連線。
3. 僅採用認證帳戶或群組：
   - 會直接根據使用者輸入的驗證名稱和密碼做認證，決定是否可建立 SSL Web VPN 連線。
4. 當用戶端的 PC 未安裝 SUN JAVA Runtime Environment 軟體，於登入 SSL Web VPN 連線畫面時，會自動要求下載安裝此軟體。**（如圖 14-41，圖 14-42）**

圖 14-41 安裝 Java Runtime Environment Plug-in CA 確認視窗

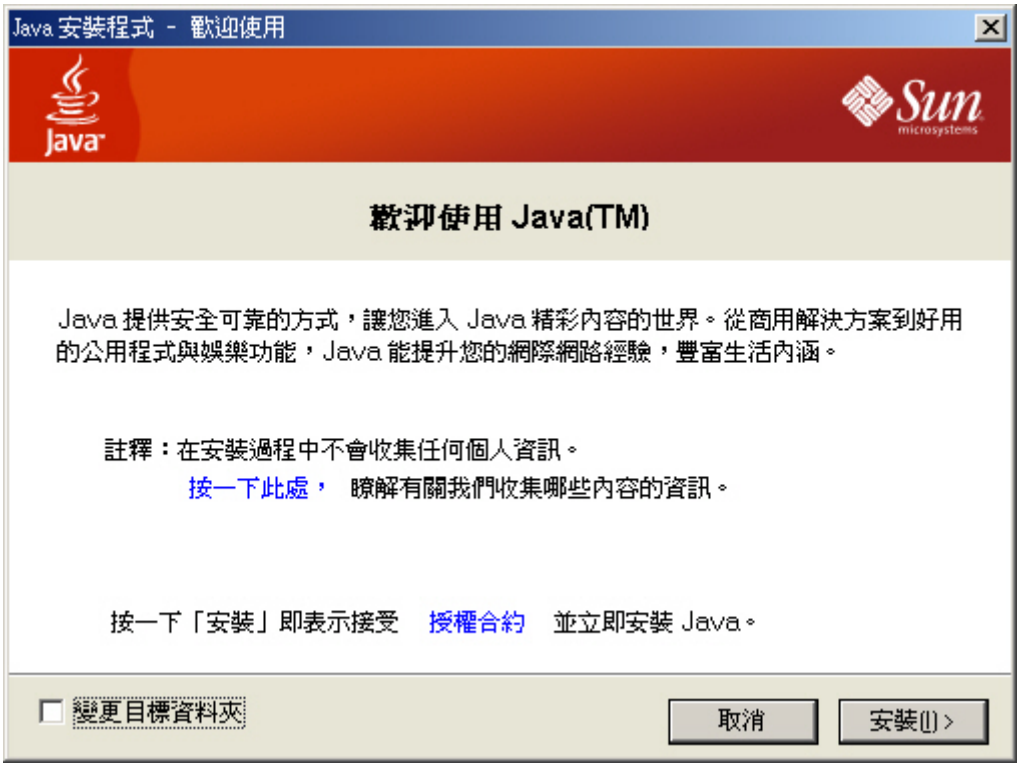


圖 14-42Java Runtime Environment Plug-in 安裝視窗

管制條例

第15章　管制條例

封包在通過 MHG-2000 前，需要比對是否符合管制條例（由第一條規則開始，依序往下比對）。當封包符合某條管制條例的規則時，就會按該管制條例來傳送，而不會再向下比對其他的管制條例。如封包無法符合任何管制條例時，該封包就會被攔截。

管制條例的參數包含有來源網路位址、目的網路位址、服務名稱、自動排程、認證名稱、VPN、動作、封包記錄、流量圖表、網站管制、應用程式管制、頻寬管理、每個來源 IP 最大頻寬限制、P2P 軟體最大頻寬限制、每個來源 IP 最大連線數限制、最大連線數限制、每個連線的傳輸量限制、每個來源 IP 的傳輸量限制、每天的傳輸量限制、傳送模式等。系統管理員可以由這些參數，管理、設定不同出入埠間的資料傳送以及服務項目，哪些網路物件、網路服務或應用程式的封包該予以攔截或放行。

MHG-2000 依據不同來源位址的資料封包，將管制條例設定功能區分為下列八項，以便系統主管理員，針對不同資料封包的來源 IP、來源埠、目的 IP、目的埠制訂管制規則。

- 【內部至外部】: 來源網路位址是內部網路區，目的網路位址是外部網路區。系統管理員在此功能中，訂定內部網路至外部網路間所有封包的管制、服務項目的管制規則。
- 【外部至內部】：來源網路位址是外部網路區，目的網路位址是內部網路區（如：IP 對應、連接埠對應）。系統管理員在此功能中，訂定外部網路至內部網路間所有封包的管制、服務項目的管制規則。
- 【外部至非軍事區】：來源網路位址是外部網路區，目的網路位址是非軍事區（如：IP 對應、連接埠對應）。系統管理員在此功能中，訂定外部網路至非軍事區間所有封包的管制、服務項目的管制規則。
- 【內部至非軍事區】：來源網路位址是內部網路區，目的網路位址是非軍事區。系統管理員在此功能中，訂定內部網路至非軍事區間所有封包的管制、服務項目的管制規則。
- 【非軍事區至外部】：來源網路位址是非軍事區，目的網路位址是外部網路區。系統管理員在此功能中，訂定非軍事區至外部網路間所有封包的管制、服務項目的管制規則。

- 【非軍事區至內部】：來源網路位址是非軍事區，目的網路位址是內部網路區。系統管理員在此功能中，訂定非軍事區至內部網路間所有封包的管制、服務項目的管制規則。
- 【內部至內部】：來源網路位址是內部網路區，目的網路位址是內部網路區。系統管理員在此功能中，訂定內部網路至內部網路間所有封包的管制、服務項目的管制規則。
- 【非軍事區至非軍事區】：來源網路位址是非軍事區，目的網路位址是非軍事區。系統管理員在此功能中，訂定非軍事區至非軍事區間所有封包的管制、服務項目的管制規則。

說明：

1. 所有經過 MHG-2000 處理的封包，必須要有管制條例許可才能通過。因此，MHG-2000 的內部網路、外部網路與非軍事區網路如要連線，則必須設定相符之管制條例。

2. MHG-2000 的 VPN 功能採用了 Trunk 的技術，並融合於管制條例之中，來控管 VPN 連線封包傳輸的權限。

【管制條例】功能概述：

來源網路位址（來源網路）& 目的網路位址（目的網路） 說明如下：

- 來源網路位址（來源網路）與 目的網路位址（目的網路）是以 MHG-2000 為觀察點。主動連線的一端為來源網路位址，被連線的一端為目的網路位址。
- 點擊管制條例列表中的【來源網路】、【目的網路】欄位，可即時修改所套用的【位址表】、【IP 對應】、【連接埠對應】、【連接埠對應群組】設定。

服務名稱 說明如下：

- 為該管制條例所管制的服務項目。可以選用系統預設，或是選用系統管理員所自訂的服務項目。
- 點擊管制條例列表中的【服務名稱】欄位，可即時修改所套用的【服務表】設定。

項目 說明如下：

- 顯示該管制條例之各項監控功能是否已啟動，若該項功能已啟動則會出現該功能的代表圖示。（圖示說明如下方表格）

圖 示	名 稱	說　　明
	自動排程	已啟動排程表所制訂時間範圍內自動執行功
	認證名稱	認證功能已運作。
	封包記錄	封包記錄功能已運作。
	流量圖表	流量圖表功能已運作。
	網站管制	網站管制功能已開啟。
	應用程式管制	已啟用應用程式管制功能。
	頻寬管理	頻寬管理功能已開啟。
	傳送模式	已設定透過指定埠傳輸的封包，要轉換成特定 IP 或以使用者電腦 IP 位址連上網路。

自動排程 說明如下：

- 設定該條管制條例的運作時間。
- 點擊管制條例列表中的，可即時修改所套用的【排程表】設定。

認證名稱 說明如下：

- 使用者必須通過認證，才可經由該管制條例連線。
- 點擊管制條例列表中的，可即時修改所套用的【認證表】設定。

VPN 說明如下：

- 將 SSL Web VPN、套用至 VPN Trunk 的 IPSec 和 PPTP VPN 連線傳輸封包，經由該管制條例控管。

動作 說明如下：

- 指定資料封包經由 MHG-2000，允許傳送的路徑（WAN1、WAN2、...）或禁止傳送。（圖示說明如下方表格）

圖 示	名 稱	說　　明
	允許所有外部網路介面	允許符合該管制條例的封包從 WAN1、WAN2、...進出。
	允許 WAN1	允許符合該管制條例的封包從 WAN1 進出。
	允許 WAN2	允許符合該管制條例的封包從 WAN2 進出。
	允許虛擬外部網路	允許符合該管制條例的封包從指定虛擬外部網路進出。
	允許 VPN	允許符合該管制條例的 VPN 連線封包進出。
	拒絕所有外部網路介面	拒絕符合該管制條例的封包進出。
	暫停	暫停該管制條例的運作。

封包記錄 說明如下：

- 記錄通過該條管制條例所有封包使用的協定、埠號、來源位址、目的位址、…。
- 點擊管制條例列表中的 ，可即時查閱相關封包記錄。

流量圖表 說明如下：

- 將通過該條管制條例的網路流量繪製成圖表。
- 點擊管制條例列表中的 ，可即時查閱相關流量圖表。

網站管制 說明如下：

- 可管制透過網頁（HTTP）和 FTP 存取的網路資源、連線的特定網站。
- 點擊管制條例列表中的 ，可即時修改所套用的【網站管制】設定。

應用程式管制 說明如下：

- 可管制即時通訊、點對點軟體、影音軟體、網頁郵件、線上遊戲、通道軟體和遠端控制軟體的連線。
- 點擊管制條例列表中的 ，可即時修改所套用的【應用程式管制】設定。

頻寬管理 說明如下：

- 設定該條管制條例的最大頻寬與保證頻寬(頻寬由符合該管制條例之使用者共享)。
- 點擊管制條例列表中的 ，可即時修改所套用的【頻寬表】設定。

每個來源 IP 最大頻寬限制 說明如下：

- 限定每個 IP 透過管制條例存取網路資源時，可用的頻寬。

說明：

1. 當【每個來源 IP 最大頻寬限制】使用量的總和，達到【頻寬管理】所賦予的資源量時，將無法提供頻寬給新的連線，做傳輸的動作。
2. 當管制條例僅進行【每個來源 IP 最大頻寬限制】時，可使每位使用者，擁有相等的頻寬，穩定的存取網路資源。

P2P 軟體最大頻寬限制 說明如下：

- 限定以【管制條例選項】>【應用程式管制】的點對軟體透過管制條例存取網路資源時，可用的頻寬。

最大頻寬限制 說明如下：

- 設定該條管制條例的最大頻寬（頻寬由符合該管制條例之使用者共享）。

每個來源 IP 每秒連線數限制 說明如下：

- 指定每個 IP 透過管制條例存取網路資源每秒可產生的連線數。如連線數超過設定值，則超過的連線無法建立成功。

每個來源 IP 最大連線數限制 說明如下：

- 指定每個 IP 透過管制條例存取網路資源的同時連線數。如連線數超過設定值，則超過的連線無法建立成功。

最大連線數限制 說明如下：

- 指定管制條例允許的同時連線數。如連線數超過設定值，則超過的連線無法建立成功。

說明：

1. 當【每個來源 IP 最大連線數限制】的設定值，大於【最大連線數限制】的設定值時，所有通過該管制條例的連線數，皆會受限於【最大連線數限制】。

每個連線的傳輸量限制 說明如下：

- 該管制條例中，每個連線可使用的最高流量（KBytes）

每個來源 IP 的傳輸量限制 說明如下：

- 該管制條例中，每個 IP 每天可使用的最高總流量（MBytes）

每天的傳輸量限制 說明如下：

- 該管制條例中，每天可使用的最高總流量（MBytes）。

傳送模式 說明如下：

- 封包於外部網路、內部網路、非軍事區間，有下列傳輸模式：
  - 自動：來源位址直接轉換為 MHG-2000 的預設網路介面位址，進行傳輸的動作。
  - 路由：依原本來源（目的）位址透過 MHG-2000 網路介面進行傳輸的動作。
  - NAT：來源位址轉換為隸屬於 MHG-2000 網路介面相同網段的其他指定位址，進行傳輸的動作。

說明：

1. 在【網路介面】>【介面位址】頁面中，外部網路【介面類型】的【NAT 模式】，旨在設定所有對外封包的統一位址轉換；【管制條例】的 NAT【傳送模式】則可再根據特定的來源網段進行個別指定的轉址。

暫停 說明如下：

- 用於停止該管制條例的作用。

排序 說明如下：

- 由於每一個封包在通過 MHG-2000 時，是由前至後逐條檢查是否符合管制條例。由此可變更管制條例之編號，以更動管制條例的優先順序。

15.1 管制條例功能使用範例

編碼	適用範圍	範例環境	頁碼
15.1.1	內部至外部	建立可監控內部使用者上網之管制條例(以封包記錄和流量圖表為例)	**497**
15.1.2	內部至外部	禁止使用者存取特定之網路資訊(以特定外部網路IP和網站、應用程式管制為例)	**501**
15.1.3	內部至外部	於特定時間內，限定只有通過認證之使用者，可存取網路資源	**507**
15.1.4	外部至內部	外部使用者透過遠端遙控軟體操控內部網路之電腦(以pcAnywhere為例)	**509**
15.1.5	外部至 DMZ	在非軍事區為NAT的模式下，架設一FTP Server，並限制外部使用者下載的頻寬、每日下載量和最多同步下載連線數	**511**
15.1.6	外部至 DMZ DMZ 至外部 內部至 DMZ	非軍事區為透通路由模式，架設一郵件伺服器，允許內部和外部網路使用者透過其收發	**513**

環境設定

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接（可用的 IP 範圍：61.11.11.10 ~ 61.11.11.14），連上網際網路。

Port3 設為 WAN2（211.22.22.22）和 ATU-R 對接（可用的 IP 範圍：211.22.22.18 ~ 211.22.22.30），連上網際網路。

Port4 設為 DMZ1 連接對外服務的電腦。

15.1.1 建立可監控內部使用者上網之管制條例（以封包記錄和流量圖表為例）

步驟1. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 15-1）

- 勾選【封包記錄】。
- 勾選【流量圖表】。
- 按下【確定】鈕，完成設定。（如圖 15-2）

圖 15-1 管制條例啟用封包記錄、流量圖表

圖 15-2 完成管制條例設定

步驟2. 按下 即可監控經由該管制條例之封包(【封包記錄過濾】視窗)。(如圖 15-3)

- 【封包記錄】過濾視窗可經由左上角之下拉式選單來變更更新頻率。
- 點選【封包記錄】過濾視窗中所示之 IP，可過濾出該 IP 的封包記錄。
- 若需觀察所有通過 MHG-2000 管制條例監控之封包，則可於【監控報告】>【監控記錄】>【封包記錄】頁面中，獲取相關訊息。(如圖 15-4)

圖 15-3 封包記錄過濾視窗

更新
1 / 1758 移至
時間 來源位置 目的位置 通訊協定 埠號 流量 處置方式
13:23:27 192.168.85.83 66.134.75.238 UDP 40269→53(WAN=2) 62.0 B
13:23:27 192.168.85.83 24.30.199.7 UDP 40269→53(WAN=2) 62.0 B
13:23:27 192.168.85.83 202.96.199.133 UDP 40269→53(WAN=2) 62.0 B
13:23:27 192.168.85.83 202.136.254.1 UDP 40269→53(WAN=2) 62.0 B
13:23:27 192.168.85.83 202.106.127.1 UDP 40269→53(WAN=2) 62.0 B
13:23:27 192.168.85.83 168.95.192.1 UDP 40269→53(WAN=2) 62.0 B
13:23:27 192.168.85.83 168.95.1.1 UDP 40269→53(WAN=2) 124.0 B
13:23:27 172.19.70.202 95.220.117.182 UDP 38073→32083(WAN=1) 60.0 B
13:23:26 192.168.85.83 66.134.75.238 UDP 34732→53(WAN=2) 62.0 B
13:23:26 192.168.85.83 24.30.199.7 UDP 34732→53(WAN=2) 62.0 B
13:23:26 192.168.85.83 202.96.199.133 UDP 34732→53(WAN=2) 62.0 B
13:23:26 192.168.85.83 202.136.254.1 UDP 34732→53(WAN=2) 62.0 B
13:23:26 192.168.85.83 202.106.127.1 UDP 34732→53(WAN=2) 62.0 B
13:23:26 192.168.85.83 168.95.192.1 UDP 34732→53(WAN=2) 62.0 B
13:23:26 192.168.85.83 168.95.1.1 UDP 34732→53(WAN=2) 124.0 B
13:23:25 192.168.85.83 66.134.75.238 UDP 33275→53(WAN=2) 62.0 B
13:23:25 192.168.85.83 24.30.199.7 UDP 33275→53(WAN=2) 62.0 B
13:23:25 192.168.85.83 202.96.199.133 UDP 33275→53(WAN=2) 62.0 B
13:23:25 192.168.85.83 202.136.254.1 UDP 33275→53(WAN=2) 62.0 B
13:23:25 192.168.85.83 202.106.127.1 UDP 33275→53(WAN=2) 62.0 B
1 / 1758 移至
清除

圖 15-4 封包記錄頁面

步驟3. 在【監控報告】>【流量圖表】>【管制條例】頁面中，會顯示通過管制條例存取網路資源之流量。（如圖 15-5）

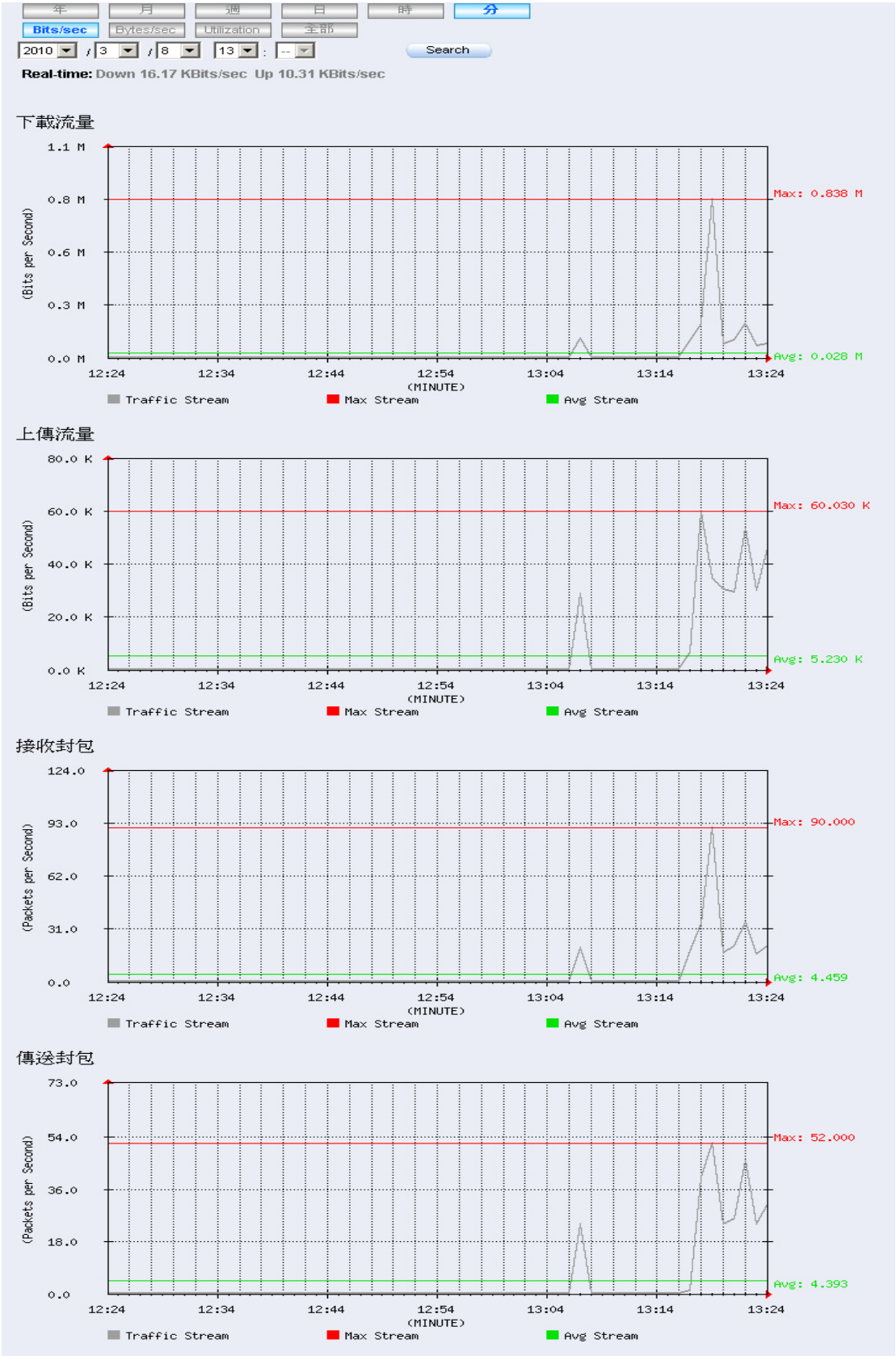


圖 15-5 流量統計頁面

15.1.2 禁止使用者存取特定之網路資訊（以特定外部網路 IP 和網站、應用程式管制為例）

步驟1. 在【網站管制】>【組態】>【網站白名單】、【網站黑名單】、【檔案傳輸管制】、【MIME/Script 管制】與【網站管制群組】頁面中，做下列設定：（如圖 15-6, 圖 15-7, 圖 15-8, 圖 15-9, 圖 15-10）

圖 15-6 網站白名單設定

圖 15-7 網站黑名單設定

圖 15-8 檔案傳輸管制設定

圖 15-9MIME/Script 管制設定

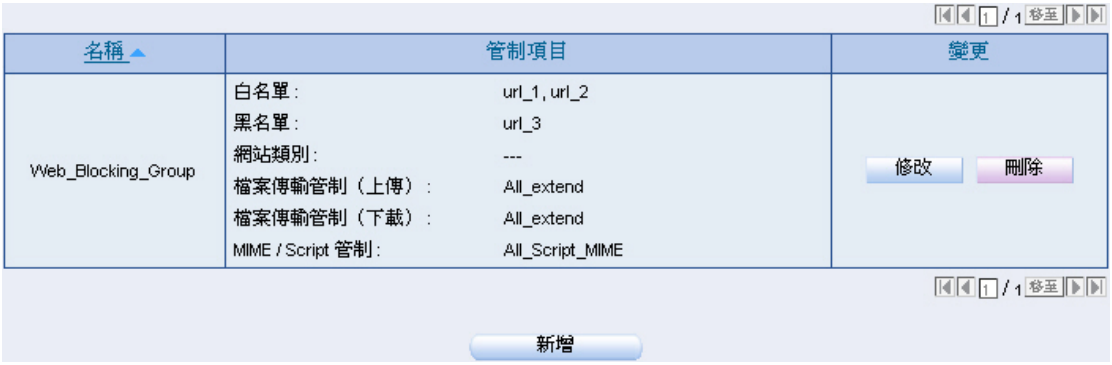


圖 15-10 網站管制群組設定

步驟2. 在【管制條例選項】>【應用程式管制】>【設定】頁面中，做下列設定：

（如圖 15-11, 圖 15-12）

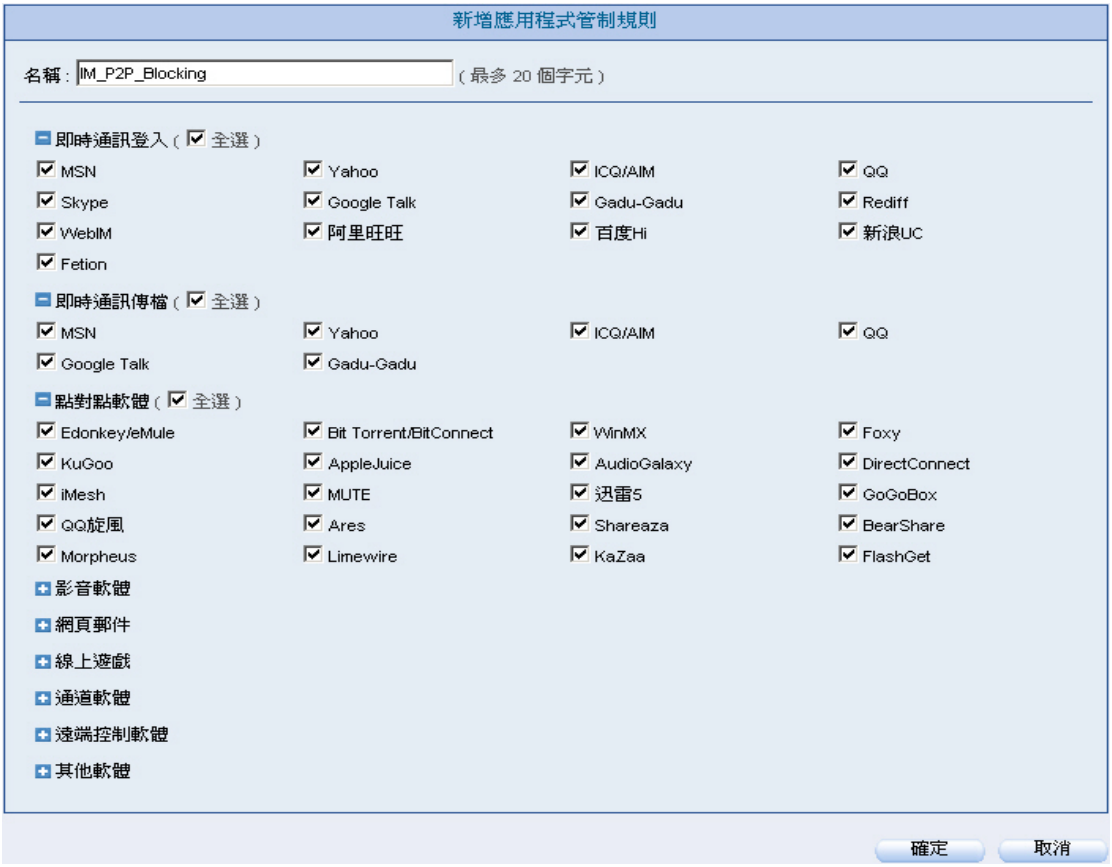


圖 15-11 設定應用程式管制

圖 15-12 完成應用程式管制設定

說明：

1. 網站管制可以阻擋使用者瀏覽特定網頁、使用特定網路功能（Java、Cookie...，例如：證券交易網站、...）、透過 HTTP 和 FTP 協定傳輸特定副檔名之檔案。
2. 應用程式管制可以阻擋使用者使用特定的即時通訊軟體、點對點軟體、影音軟體、網頁郵件、線上遊戲、通道軟體、遠端控制軟體。

步驟3. 在【管制條例選項】>【位址表】>【外部網路】、【外部網路群組】頁面中，做下列設定：（如圖 15-13, 圖 15-14）

圖 15-13 外部網路位址設定

圖 15-14 外部網路位址群組設定

步驟4. 在【管制條例】>【內部至外部】頁面中，做下列設定：

- 按下【新增】鈕。
- 【目的網路位址】選擇所設定的外部網路位址群組規則。(以 IP 做阻擋的動作)
- 【動作】勾選拒絕所有外部網路介面。
- 按下【確定】鈕。(如圖 15-15)
- 再次按下【新增】鈕。
- 【網站管制】選擇所設定的網站管制群組規則。
- 【應用程式管制】選擇所設定的應用程式管制規則。
- 按下【確定】鈕，完成設定。(如圖 15-16, 圖 15-17)

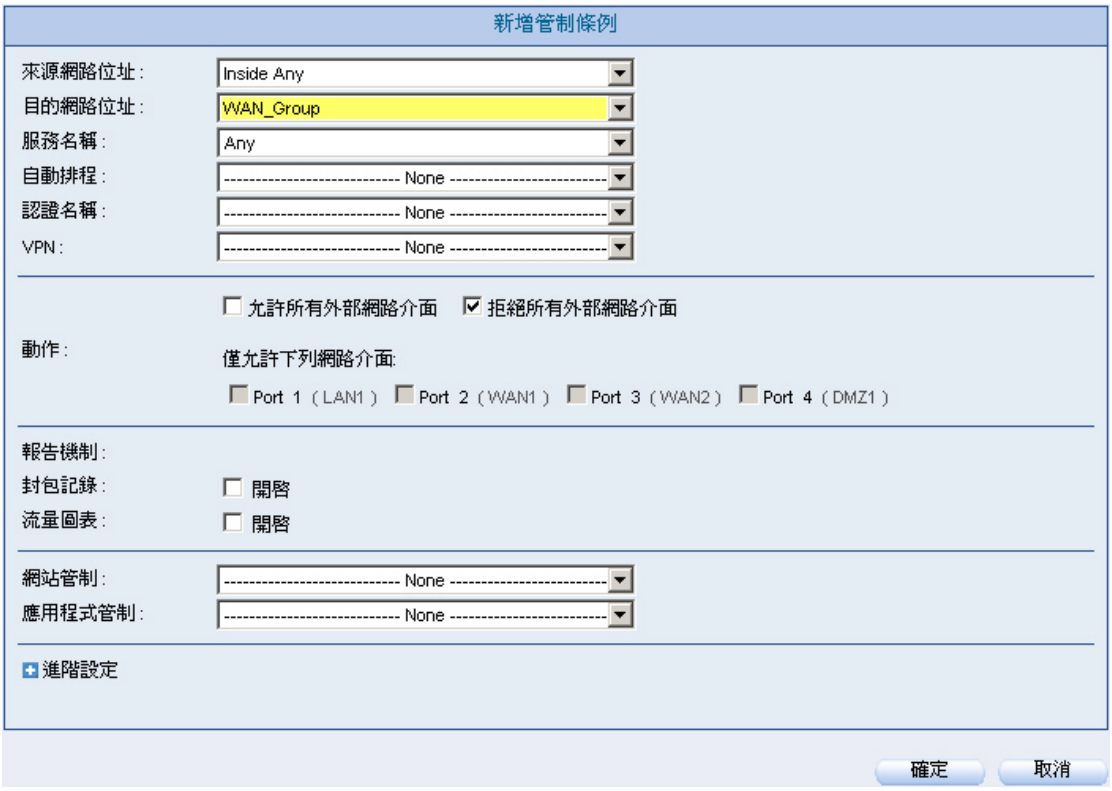


圖 15-15 設定阻擋連線指定外部網路位址之管制條例

圖 15-16 管制條例套用網站、應用程式管制規則

圖 15-17 完成管制條例設定

說明：

1. 管制條例的拒絕動作可阻擋符合該管制條例的封包進出，系統管理員可將該管制條例置於第一位階，來阻止使用者與特定 IP 連線。

15.1.3 於特定時間內，限定只有通過認證之使用者，可存取網路資源

步驟1. 在【管制條例選項】>【排程表】>【設定】頁面中，做下列設定：（如圖 15-18）

圖 15-18 排程表設定

步驟2. 在【管制條例選項】>【認證表】>【認證帳戶】、【認證群組】頁面中，做下列設定：（如圖 15-19）

圖 15-19 認證群組設定

步驟3. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 15-20）

- 【自動排程】選擇所設定的排程表規則。
- 【認證名稱】選擇所設定的認證群組規則。
- 按下【確定】鈕，完成設定。（如圖 15-21）

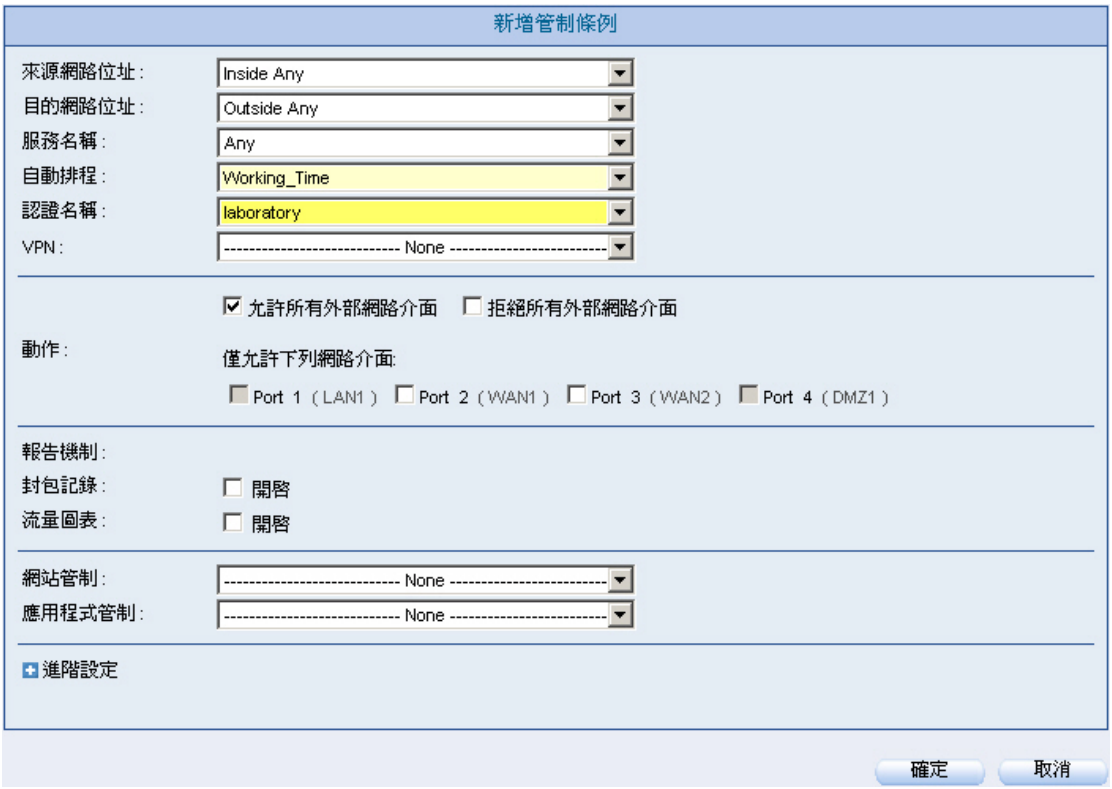


圖 15-20 管制條例套用排程表、認證群組規則

圖 15-21 完成管制條例設定

15.1.4 外部使用者透過遠端遙控軟體操控內部網路之電腦（以 pcAnywhere 為例）

步驟1. 架設一部接受遠端控管之電腦，其 IP 位址為 192.168.1.2。

步驟2. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 15-22）

圖 15-22 虛擬伺服器設定

步驟3. 在【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 15-23）

- 【目的網路位址】選擇所設定的虛擬伺服器規則。
- 【服務名稱】選擇 PC-Anywhere(5617-5632)。
- 按下【確定】鈕，完成設定。（如圖 15-24）

圖 15-23 設定外部使用者遙控內部電腦之管制條例

圖 15-24 完成管制條例設定

15.1.5 在非軍事區為 NAT 的模式下，架設一 FTP Server，並限制外部使用者下載的頻寬、每日下載量和最多同步下載連線數

步驟1. 在【非軍事區】架設一 FTP 伺服器，其 I P 位址為 192.168.3.2。(非軍事區的界面位址設為 192.168.3.1，為 192.168.3.x/24 網段)

步驟2. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：(如圖 15-25)

圖 15-25 虛擬伺服器設定

說明：

1. 當使用【管制條例】>【外部至內部】或【外部至非軍事區】功能時，建議千萬不要選擇服務為 ANY。這樣容易使位於 MHG-2000 下的電腦遭受到駭客之入侵。

步驟3. 在【管制條例選項】>【頻寬表】>【設定】頁面中，做下列設定：(如圖 15-26)

圖 15-26 頻寬表設定

步驟4. 在【管制條例】>【外部至非軍事區】頁面中，做下列設定：（如圖 15-27）

- 【目的網路位址】選擇所設定的虛擬伺服器規則。
- 【服務名稱】選擇 FTP(20-21)。
- 【頻寬管理】選擇所設定的頻寬表規則。
- 【最大連線數限制】輸入 100。
- 【每天的傳輸量限制】輸入 100000 MBytes。
- 按下【確定】鈕，完成設定。（如圖 15-28）

圖 15-27 設定限制外部使用者存取內部伺服器服務之管制條例

圖 15-28 完成管制條例設定

15.1.6 非軍事區為透通路由模式，架設一郵件伺服器，允許內部和外部網路使用者透過其收發電子郵件

步驟1. 在【非軍事區】架設一郵件伺服器，其網卡 IP 設定為 61.11.11.12、DNS 設定指向於外部 DNS 伺服器。

步驟2. 在【管制條例選項】>【位址表】>【非軍事區網路】頁面中，做下列設定：（如圖 15-29）

圖 15-29 非軍事區網路位址表設定

步驟3. 在【管制條例選項】>【服務表】>【服務群組】頁面中，做下列設定：（如圖 15-30）

圖 15-30 服務群組設定

步驟4. 在【管制條例】>【外部至非軍事區】頁面中，做下列設定：（如圖 15-31）

- 【目的網路位址】選擇所設定的非軍事區網路位址表規則。
- 【服務名稱】選擇所設定的服務群組規則。
- 按下【確定】鈕，完成設定。（如圖 15-32）

圖 15-31 設定外部至非軍事區存取電子郵件服務之管制條例

圖 15-32 完成管制條例設定

步驟5. 在【管制條例】>【內部至非軍事區】頁面中，做下列設定：（如圖 15-33）

- 【目的網路位址】選擇所設定的非軍事區網路位址表規則。
- 【服務名稱】選擇所設定的服務群組規則。
- 按下【確定】鈕，完成設定。（如圖 15-34）

圖 15-33 設定內部至非軍事區存取電子郵件服務之管制條例

圖 15-34 完成管制條例設定

步驟6. 在【管制條例】>【非軍事區至外部】頁面中，做下列設定：（如圖 15-35）

- 【來源網路位址】選擇所設定的非軍事區網路位址表規則。
- 【服務名稱】選擇所設定的服務群組規則。
- 按下【確定】鈕，完成設定。（如圖 15-36）

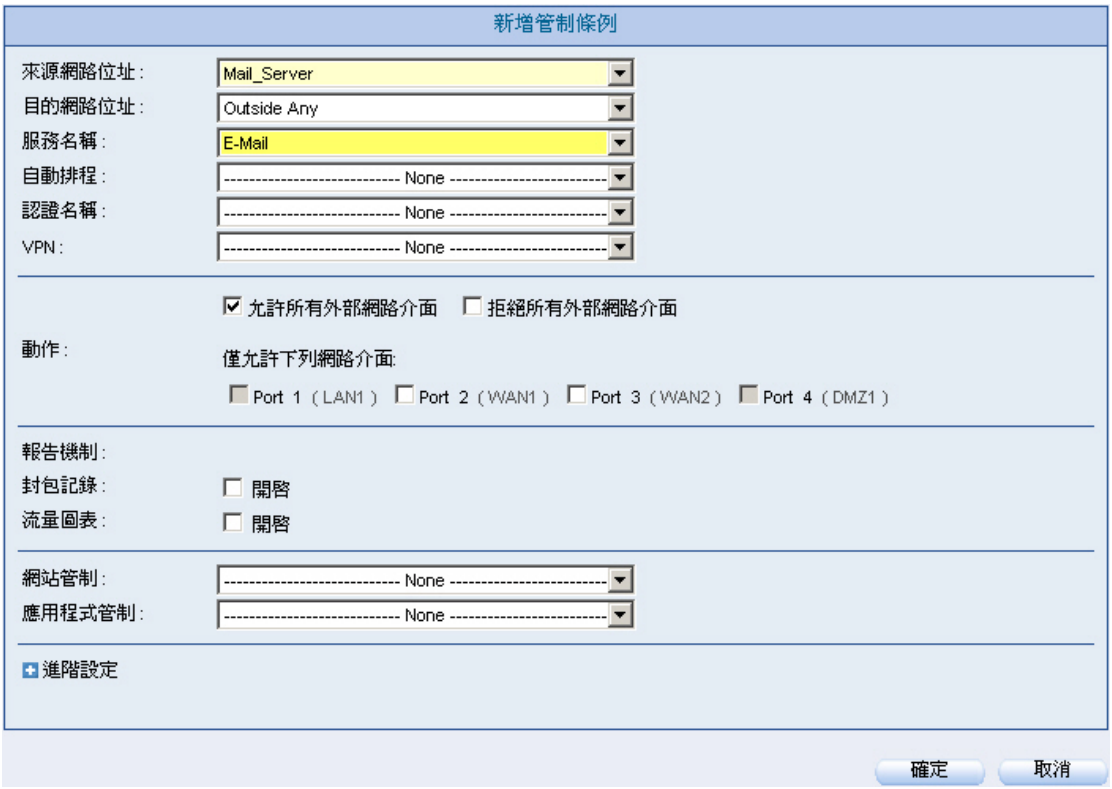


圖 15-35 設定非軍事區至外部存取電子郵件服務之管制條例

圖 15-36 完成管制條例設定

異常流量 IP

第16章　異常流量 IP

當 MHG-2000 收到內部機器所發出的大量不正常封包時，會阻擋此類封包的傳送，以避免企業網路癱瘓，整體作業停擺，並喪失許多商機。

16.1 異常流量 IP 功能使用範例

16.1.1 MHG-2000 警示與防止內部中毒電腦發出大量 DDoS 攻擊封包

步驟1. 在【系統管理】>【組態】>【系統設定】頁面中，啟動並進行【電子郵件警告 / 報告設定】。

步驟2. 在【系統管理】>【組態】>【SNMP】頁面的【SNMP Trap 設定】欄位中，做下列設定：（如圖 16-1）

圖 16-1SNMP Trap 設定

步驟3. 在【異常流量 IP】>【設定】頁面中，做下列設定：**（如圖 16-2）**

- 設定【每個 IP 的異常流量連線臨界值】（預設為每秒 100 個連線數）。
- 勾選【開啟異常流量 IP 阻擋功能】並設定其【阻擋時間】（預設為 60 秒）。
- 勾選【開啟電子郵件警訊通知】。
- 勾選【開啟 SNMP Trap 警訊通知】。
- 勾選【開啟 NetBIOS 警訊通知】並輸入指定的【管理員 IP 位址】。
- 按下【確定】鈕，完成設定。

圖 16-2 異常流量 IP 設定頁面

說明：

1. 可新增【不偵測 IP】，這些特定 IP 將不受此功能控管。
2. 可將特定的警訊內容，透過瀏覽器傳送給發出異常封包的 PC。

步驟4. 若是 MHG-2000 偵測到內部電腦有發出大量 DDoS 攻擊封包的現象時，會立即將警告訊息顯示在【異常流量 IP】>【異常流量報告】頁面中，或立即以NetBIOS 發出警訊給中毒和管理員的電腦。**（如圖 16-3, 圖 16-4, 圖 16-5）**

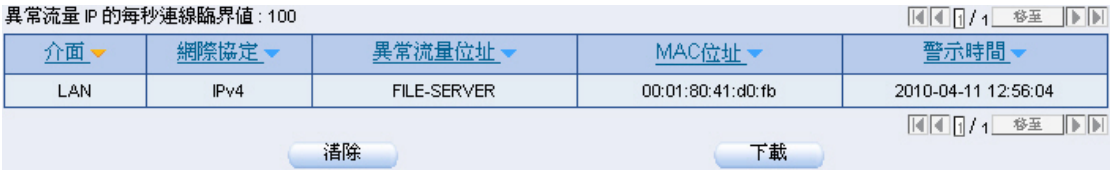


圖 16-3 異常流量 IP 列表

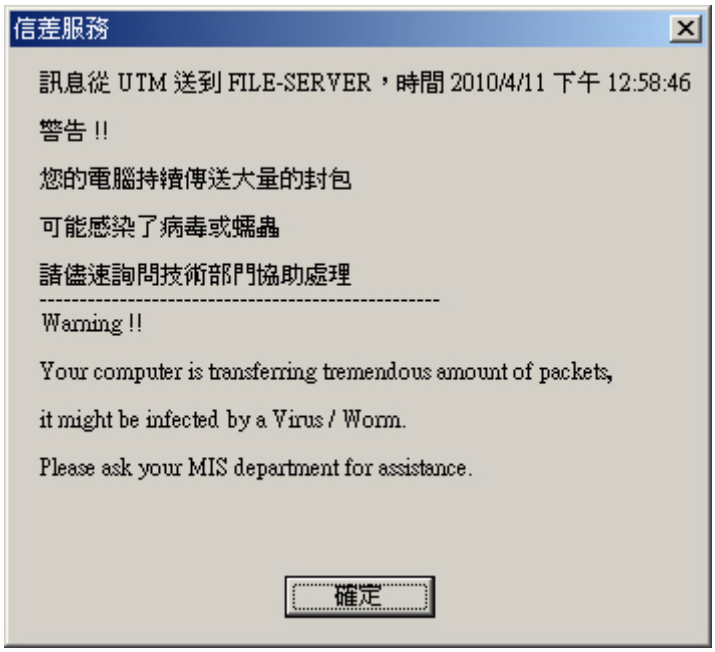


圖 16-4 發送至中毒電腦之 NetBIOS 警訊通知

圖 16-5 發送給管理員之 NetBIOS 警訊通知

步驟5. MHG-2000 會自動發出電子郵件警訊給指定的收件者。（如圖 16-6）

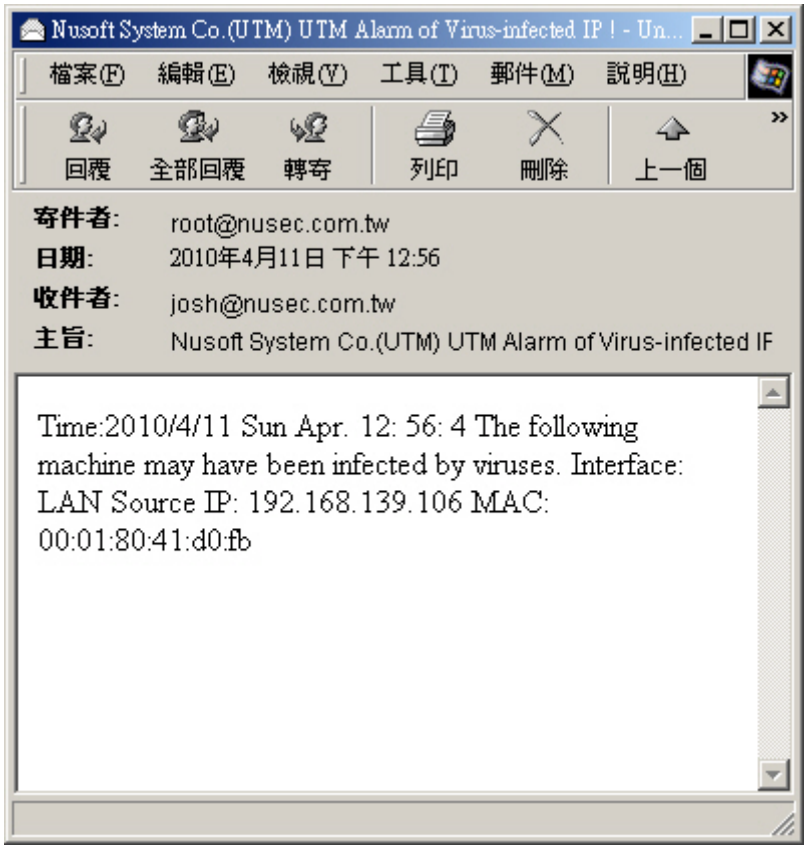


圖 16-6 電子郵件警訊通知

步驟6. MHG-2000 會將警告訊息即時顯示於管理端電腦所安裝之 SNMP Trap 用戶端軟體上。（如圖 16-7）

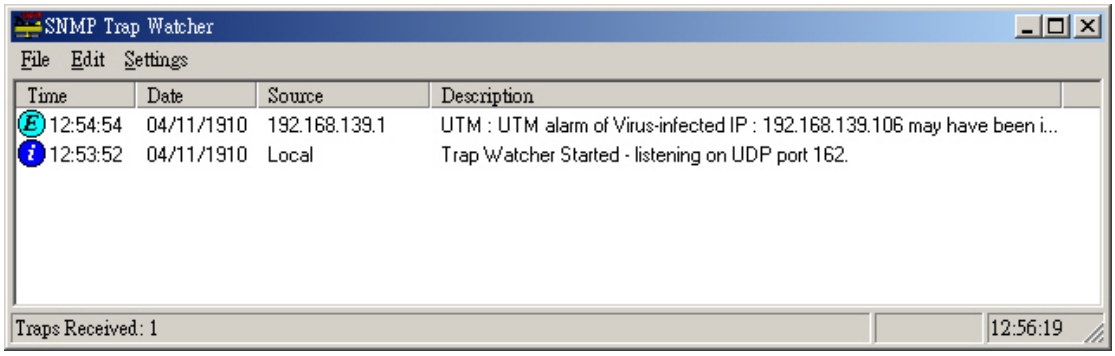


圖 16-7SNMP Trap 用戶端軟體所接收到的警訊

步驟7. 當內部使用者的電腦中毒後，第一次透過瀏覽器上網時，MHG-2000 會於其瀏覽器上顯示警告之畫面，告知其電腦已中毒。(使用者若是不能排除本身中毒之情況，往後皆會受到 MHG-2000 限制，導致上網變慢，且不會再有警告訊息顯示於瀏覽器)(如圖 16-8)

圖 16-8 顯示於中毒電腦瀏覽器之警告訊息

進階功能

第17章　InBound 負載平衡

可將外部使用者對內部伺服器尋求服務的連線，依權值比重分配給各連外線路，減少彼此的負載流量；當有線路發生斷線情形時，外部使用者仍可經由其他正常線路連接至內部伺服器，避免錯失商機。

【設定】功能概述：

網域名稱（Domain Name） 說明如下：

- 對於使用電腦的人來說，IP 的位址不適合記憶與管理，因此有 Domain 的出現，例如：ccu.edu.tw、nusoft.com.tw，這樣的表示方式較適合人來使用，以較有意義的文字來代替 IP，這一串文字即為網域名稱。
- 我們熟悉的網址為二個部分組成：主機名稱跟網域名稱。如一般用戶要瀏覽 yahoo 網頁，他會在瀏覽器的網址列輸入 www.yahoo.com（主機名稱即 www，網域名稱即 yahoo.com），實際上 yahoo 網站的 IP 位址為 66.218.71.84，至於如何建立 www.yahoo.com 這個網址與 IP 的對應，中間就需要有 DNS Server 來做轉換了。

啟動 DNS 設定（Enable DNS Zone） 說明如下：

- 指啟動 InBound 負載平衡所採用的 DNS 機制。**（如圖 17-1）**

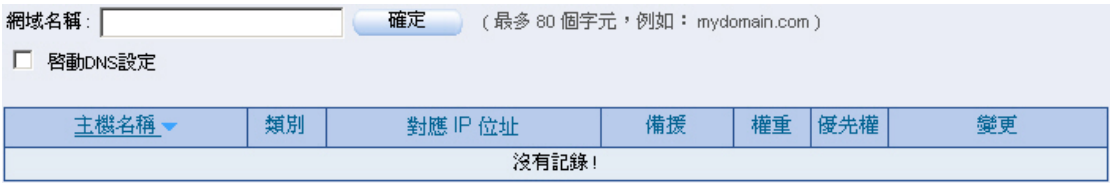


圖 17-1InBound 負載平衡規則表

選擇使用類別（Select type） 說明如下：

- 網路位址（A）：用來設定主機名稱對應的 IP 位址。
  - 建立主機名稱和IP位址的對應關係如下：**（如表17-1）**

名稱	類別	位址
host1.nu.net.tw	A	61.11.11.12
host2.nu.net.tw	A	61.11.11.13
host2.nu.net.tw	A	211.22.22.23

表17-1主機名稱和IP位址的對應關係

  - 其中A表示網路位址，而每筆記錄將一個主機名稱對應到一個IP位址。host2主機擁有兩個IP位址，因此DNS資料檔中有兩筆IP位址記錄。DNS查詢可為一個主機名稱傳回一筆以上的記錄，並利用address-sorting或round-robin的方式排列DNS查詢結果的順序。

- 別名（CNAME）：用來設定主機別名對應的真實名稱。
  - 建立主機別名和真實名稱的對應關係如下：（如表 17-2）

名稱	類別	位址
host23.nu.net.tw	A	61.11.11.14
host5.nu.net.tw	CNAME	host23.nu.net.tw

表17-2主機別名和真實名稱的對應關係

  - 在DNS資料檔中可有多筆主機別名對應同一真實名稱的記錄。CNAME可以對應一個網路位址（A）之主機名稱，但不建議對應另一個別名（CNAME）。所以host5.nu.net.tw這個主機別名是對應到host23.nu.net.tw這個真實名稱，在DOS下Ping host5.nu.net.tw會Ping到61.11.11.14這個IP。
- 郵件伺服器（MX）：用來設定郵件伺服器名稱對應的主機名稱。
  - 建立郵件伺服器名稱和主機名稱的對應關係如下：（如表 17-3）

名稱	類別	位址
host25.nu.net.tw	A	211.22.22.24
mail.nu.net.tw	MX	host25.nu.net.tw

表 17-3 郵件伺服器名稱和主機名稱的對應關係

  - MX即Mail Exchange，這是一種專用於E-mail的DNS記錄資料。如果要更換郵件伺服器，只需修改DNS記錄中對應的郵件交換主機。如在DOS輸入nslookup -type=MX mail.nu.net.tw（nslookup為DNS查詢指令，-type後所接的是DNS記錄的類別，mail.nu.net.tw則為欲查詢的DNS名稱），則會顯示出mail.nu.net.tw所對應到的郵件交換器（host25.nu.net.tw），並顯示出host25.nu.net.tw的IP（211.22.22.24）。
  - 假設test客服中心要發一封E-mail給mary@mail.nu.net.tw這個收件者。客服人員透過test.com.tw當作外送伺服器（SMTP Server）發送信件，test.com.tw這台主機透過DNS查詢判斷mail.nu.net.tw要如何遞送。查詢mail.nu.net.tw的MX Record如下：（如表17-4）

名稱	類別	位址
host3.nu.net.tw	A	61.11.11.10
mail.nu.net.tw	MX	host3.nu.net.tw

表 17-4 mail.nu.net.tw 的 MX Record

  - 因此伺服器會往目的地主機 host3.nu.net.tw 去遞送（透過SMTP Protocol）E-mail。
- Sender Policy FrameWork（SPF）：為防堵垃圾郵件、釣魚郵件，驗明寄件者身份之機制。

- ◆ DNS 的 MX 記錄對應網域中合法的郵件伺服器；而 SPF 則可讓網域管理者，對外公布合法的郵件伺服器 IP 位址。當郵件伺服器收到信件時，可依寄件者的郵件地址查詢 DNS SPF 記錄，檢查寄件者的郵件伺服器 IP 是否列於 SPF 記錄的 IP 清單中。

■ IPv6 網路位址（AAAA）：等同 IPv4 網路位址（A）類別，用來表示主機名稱和 IPv6 位址的對應關係。

- ◆ 它是對 IPv4 協定 A 類別的擴展，由於 IP 位址由 32 位元擴展至 128 位元，擴大了 4 倍，所以記錄資料由 A 擴大至 AAAA。（如表 17-5）

名稱	類別	位址
host33.nu.net.tw	AAAA	FEC0::2AA:FF:FE3F:2A1C

表 17-5 主機名稱和 IPv6 位址的對應關係

■ Text strings（TXT）：用來保存網域名稱的附加（說明）文字訊息，可包含任意文字，也能用於定義機器可讀文字。

- ◆ 絕大多數用來設定 SPF 記錄，亦可用來證明網域所有權。最典型的 SPF 格式 TXT 記錄為 v=spf1 a mx -all，表示只有這個網域名稱的 A 和 MX 記錄對應之 IP 位址，允許使用這個網域名稱來發送郵件。（如表 17-6）

名稱	類別	說明
nu.net.tw	TXT	v=spf1 a mx -all

表 17-6 網域名稱對應的 TXT 記錄

反解域名（Reverse） 說明如下：

■ 可以使用 IP 位址來反查網域名稱，DNS 的對應機制可分為兩種：正解和反解；平常我們輸入網址，DNS 就會幫我們連至相對應的 IP 位址，這就是正解的功能，當然相反就是反解。

■ IPv4 反解採用 PTR（Pointer）記錄資料，若 host1.nu.net.tw 對應的 IP 位址為 61.11.11.12，反向輸入此 IP 並加上.in-addr.arpa，即為對應的反查區域（Zone）位址 12.11.11.61.in-addr.arpa。

■ IPv6 反解亦採用 PTR（Pointer）記錄資料，若 host33.nu.net.tw 對應的 IP 位址為 FEC0::2AA:FF:FE3F:2A1C（完整形式為 FEC0:0000:0000:0000:02AA:00FF:FE3F:2A1C），反向輸入並以點分各十六進位數字然後加上.IP6.INT.，即為對應的反查區域（Zone）位址 C.1.A.2.F.3.E.F.F.F.0.0.A.A.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.C.E.F.IP6.INT.。

- 以【表 17-1】為例，在 DOS 下使用 nslookup 指令測試正向、反向的解析是否正常時會出現下列情況：

C:\>**nslookup** host1.nu.net.tw ---------->正查
Server: dns.hinet.net
Address: 168.95.1.1

Name：host1.nu.net.tw
Address：61.11.11.12

C:\>**nslookup** 61.11.11.12 ---------->反查
Server: dns.hinet.net
Address: 168.95.1.1

Name：host1.nu.net.tw
Address：61.11.11.12

所以 61.11.11.12 對應到 host1.nu.net.tw

平衡模式（Balance Mode） 說明如下：

- 循環分配（Round-Robin）：依照權重及優先權來分配外部使用者連線內部伺服器的流量至不同的對外線路。
- 備援（Backup）：可將內部伺服器擇一對外線路來提供外部使用者常態連線，並指定另一線路在原線路異常時接續服務的工作。

進階說明：

所謂的 DNS 指向，是公告大家該網域是由哪台 DNS 伺服器來管理，所有關於該網域名稱的網路資料都記錄在該 DNS 主機，例如：網站對應的實體位址或郵件伺服器對應的實際位址。所以，該 DNS 伺服器要確實連上網際網路且記錄要正確才行。

依照國際慣例，DNS 系統指向必須指定二部 DNS 伺服器。其原因在於為確保網路運作順暢，當一部 DNS 無法正常作用時，另一部 DNS 能夠即時備援，讓你的網域名稱能夠順利使用。除了保障你的網域名稱正常使用，也保障所有網路人口查詢網域名稱的順暢。

假設我們需要建立應用於以下情況的名稱伺服器：

- 自備專線或固定制 ADSL 線路與網際網路連接。
- 註冊一個網域名稱 nu.net.tw。
- 主要名稱伺服器設為 dns1.nu.net.tw。
- 次要名稱伺服器設為 dns2.nu.net.tw。
- 要解析的伺服器有：
  - Web 伺服器 www.nu.net.tw。
  - E-Mail 伺服器 mail.nu.net.tw。

向 ISP 申請二條固接 IP 的 ADSL 線路（或專線）：

- 假設申請到的 IP 位址為：
  - 61.11.11.10 ~ 61.11.11.14。
  - 211.22.22.18 ~ 211.22.22.30。

到網域註冊網站申請（註冊）DNS 設定：

- 主要名稱伺服器：
  - Host Name：dns1.nu.net.tw。
  - IP Address：61.11.11.11。
- 次要名稱伺服器：
  - Host Name：dns2.nu.net.tw。
  - IP Address：211.22.22.22。

說明：

1. 向網域註冊網站申請的 DNS 網域名稱必須對應到固接 IP。

在 InBound 負載平衡功能設定下列資料：（如表 17-7）

名稱	類別	位址	反查	權重	優先權
nu.net.tw	A	61.11.11.11	O	1	1
nu.net.tw	A	211.22.22.22	O	1	2

表 17-7 主要和次要 DNS 的名稱和 IP 對應記錄

當主要 DNS 無法正常作用時，次要 DNS 能夠即時取代，讓你的網域名稱能夠順利使用，這就是備援。

由【表 17-7】可以知道，在 DOS 下使用 nslookup 指令測試正向、反向的解析是否正常時會出現下列情況：

C:\>nslookup nu.net.tw
Server: dns.hinet.net
Address: 168.95.1.1

Name: nu.net.tw
Addresses: 61.11.11.11, 211.22.22.22 ---------->檢驗是否指向正確 IP(正查)

C:\>nslookup 61.11.11.11
Server: dns.hinet.net
Address: 168.95.1.1

Name: nu.net.tw ---------->檢驗是否對應正確 Domain Name(反查)
Address: 61.11.11.11

在 InBound 負載平衡功能設定下列資料：（如表 17-8）

名稱	類別	位址	權重	優先權
web.nu.net.tw	A	61.11.11.11	1	1
web.nu.net.tw	A	211.22.22.22	2	2
www.nu.net.tw	CNAME	web.nu.net.tw	--	--

表 17-8www.nu.net.tw 的 CNAME（別名）記錄

由【表 17-8】可以知道，在 DOS 下使用 nslookup 指令測試正向的解析是否正常時會出現下列情況：

C:\>nslookup

Default Server：dns.hinet.net

Address：168.95.1.1

> server 61.11.11.11 ---------->切換至自己架設的 DNS server

Default Server：web.nu.net.tw

Address：61.11.11.11

> www.nu.net.tw ---------->檢驗 www 所指向的正式名稱(正查)

Server：web.nu.net.tw

Address：61.11.11.11

Name：web.nu.net.tw ---------->www.nu.net.tw 對應到的正式名稱

Addresses：61.11.11.11, 211.22.22.22 ---------->web.nu.net.tw 的對應 IP

Aliases：www.nu.net.tw ----------> web.nu.net.tw 的主機別名

所以說 web.nu.net.tw 是 DNS 用來對應主機名稱和其 IP 地址的 Address 記錄，而 www.nu.net.tw 則是提供和上述主機名稱對應的別名，具有查詢導向的能力，以得到相同的查詢結果。

由【表 17-8】設定可知
當使用者連線 www.nu.net.tw 時，會依下列順序連到伺服器
第一位使用者透過 61.11.11.11 連到伺服器
第二位使用者透過 211.22.22.22 連到伺服器
第三位使用者透過 211.22.22.22 連到伺服器
(循環權重已分配完畢)
第四位使用者透過 61.11.11.11 連到伺服器
(重新循環分配權重)
第五位使用者透過 211.22.22.22 連到伺服器
第六位使用者透過 211.22.22.22 連到伺服器

當第三位使用者連線 www.nu.net.tw，已超過 61.11.11.11 設定的權重 1，InBound 負載平衡會分配第三位使用者透過權重設定為 2 的 211.22.22.22 來進行連線，當依序完成所有的權重分配時，系統會依權重及優先權再次循環分配上述的位址提供使用者來連到伺服器，做到負載平衡的機制。

在【表 17-9】中 MX 設定的優先權（Priority）數字越小擁有較高的優先權，假使一位寄件者 A 要發一封信件給 mary@mail.nu.net.tw 這個收件者 B。
寄件者 A 透過 hinet.net.tw 當作外送伺服器（SMTP Server）發送信件，hinet.net.tw 這台主機透過 DNS 查詢判斷 mail.nu.net.tw 要如何遞送。查詢 mail.nu.net.tw 的 MX 記錄可得知有兩筆資料分別如下：**（如表 17-9）**

名稱	類別	位址	反查	權重	優先權
mail.nu.net.tw	MX	smtp1.nu.net.tw	X	--	1
mail.nu.net.tw	MX	smtp2.nu.net.tw	X	--	2

表 17-9mail.nu.net.tw 的 MX 記錄

因此伺服器會先嘗試往 MX 優先權設定為 1 的主機 smtp1.nu.net.tw 去遞送（透過 SMTP Protocol）E-mail；倘若失敗，才會往 MX 優先權設定為 2 的主機 smtp2.nu.net.tw 去遞送 E-mail。

17.1 InBound 負載平衡功能使用範例

編碼	範例環境	頁碼
17.1.1	於InBound負載平衡設定Web伺服器採用A（網路位址）記錄的備援機制	**537**
17.1.2	於InBound負載平衡設定Web伺服器採用A（網路位址）記錄的循環分配機制	**543**
17.1.3	於InBound負載平衡設定Web伺服器採用CNAME（別名）記錄的循環分配機制	**550**
17.1.4	於InBound負載平衡設定MAIL伺服器採用MX（郵件伺服器）記錄的循環分配機制	**558**

環境設定

DNS 的網域名稱必須對應到固接 IP。

申請兩條有固接 IP 的 ADSL 線路。

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1（61.11.11.11）所連線路的固接 IP 為 61.11.11.10 ~ 61.11.11.14。

Port3 設為 WAN2（211.22.22.22）所連線路的固接 IP 為 211.22.22.18 ~ 211.22.22.30。

註冊一個網域名稱 nusec.com.tw。

主要名稱伺服器的 IP 為 61.11.11.11，主機名為 dns1.nusec.com.tw。

次要名稱伺服器的 IP 為 211.22.22.22，主機名為 dns2.nusec.com.tw。

17.1.1 於 InBound 負載平衡設定 Web 伺服器採用 A（網路位址）

記錄的備援機制

步驟1. 在【進階功能】>【InBound 負載平衡】>【設定】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 17-2）
- 輸入申請的 DNS【網域名稱】。
- 勾選【啟動 DNS 設定】。
- 按下【新增】鈕。（如圖 17-3）
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 www。
- 【對應 IP 位址】選擇 WAN1 並輸入 61.11.11.11。
- 【平衡模式】選擇循環分配。
- 按下【確定】鈕。
- 再次按下【新增】鈕。（如圖 17-4）
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 www。
- 【對應 IP 位址】選擇 WAN2 並輸入 211.22.22.22。
- 【平衡模式】選擇備援 WAN1。
- 按下【確定】鈕，完成設定。（如圖 17-5）

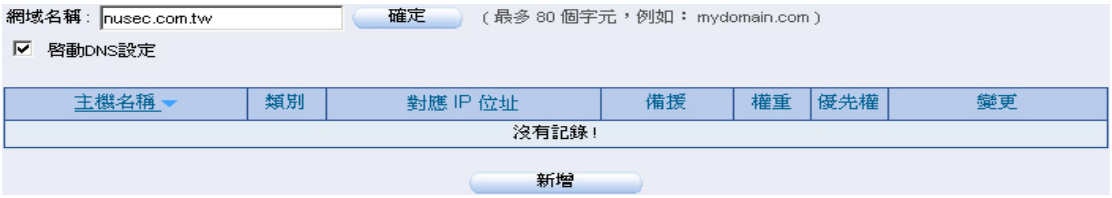


圖 17-2InBound 負載平衡網域名稱設定

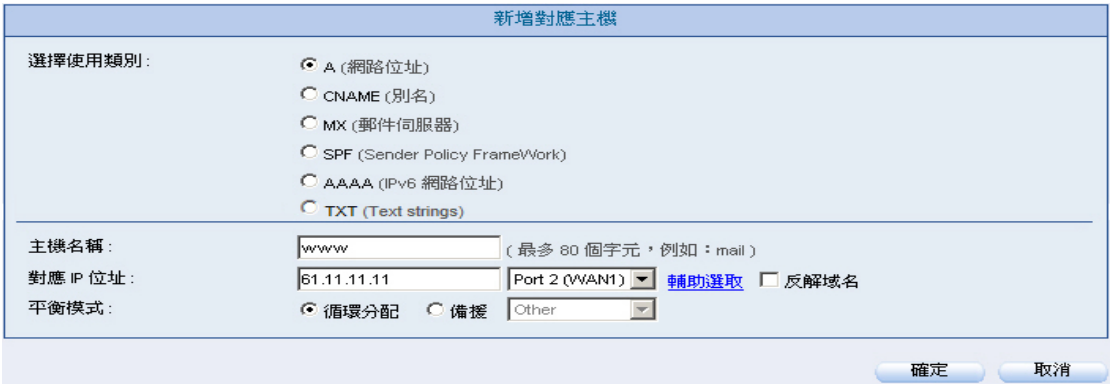


圖 17-3 設定第一條 InBound 負載平衡規則

圖 17-4 設定第二條 InBound 負載平衡規則

圖 17-5 完成 InBound 負載平衡規則設定

說明：

1. 【主機名稱】若輸入@，代表所設定的【網域名稱】，以此例來說就是 nusec.com.tw.。
2. 點（.）號代表一個完整主機名稱（FQDN），以此例來說【主機名稱】輸入 www，代表其完整名稱為 www.nusec.com.tw.；若輸入 www.nusec.com.tw，由於尾端並未加上點號，則網域名稱會主動加入該主機名稱，所以其完整名稱會變成 www.nusec.com.tw.nusec.com.tw.。
3. 在啟用【反解域名】機制前，請務必確認申請的線路具有一個 C Class（或 B Class、A Class）的 IP 使用權；若是不符合此基本要素，則需逕向 ISP 申請域名反解服務。

步驟2. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 17-6, 圖 17-7）

圖 17-6 第一條虛擬伺服器規則設定頁面

圖 17-7 第二條虛擬伺服器規則設定頁面

步驟3. 在【管制條例】>【外部至內部】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 17-8）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。（[連接埠對應]Web_Server(61.11.11.11)）
- 【服務名稱】選擇 HTTP(80)。
- 按下【確定】鈕。
- 再次按下【新增】鈕。（如圖 17-9）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。（[連接埠對應]Web_Server(211.22.22.22)）
- 【服務名稱】選擇 HTTP(80)。
- 按下【確定】鈕，完成設定。（如圖 17-10）

圖 17-8 設定第一條外部使用者存取內部伺服器服務之管制條例

圖 17-9 設定第二條外部使用者存取內部伺服器服務之管制條例

圖 17-10 完成管制條例設定

步驟4. 當 WAN1 斷線時，WAN2 將會接續對使用者提供 Web 服務。（如圖 17-11）

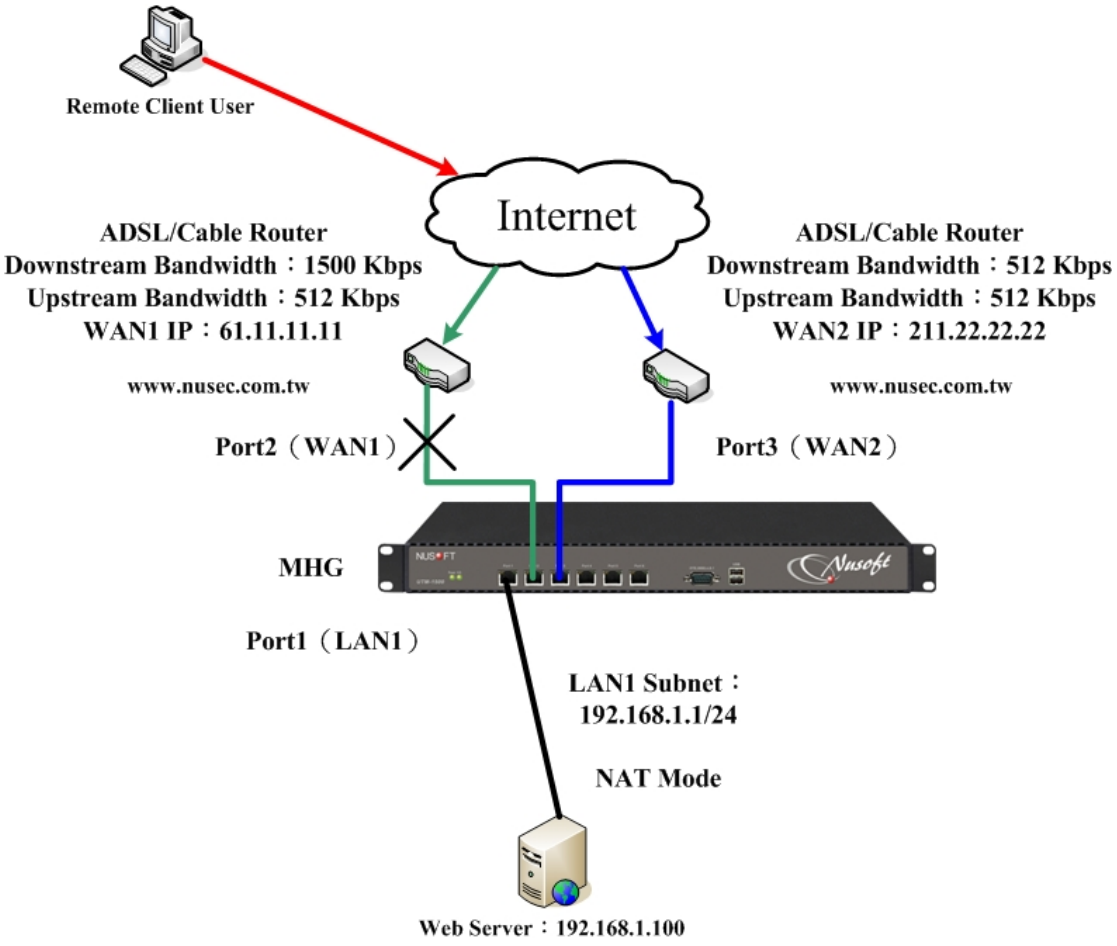


圖 17-11Web 伺服器透過 InBound 負載平衡斷線備援機制提供服務之架設環境

17.1.2 於 InBound 負載平衡設定 Web 伺服器採用 A（網路位址）

記錄的循環分配機制

步驟1. 在【進階功能】>【InBound 負載平衡】>【設定】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 17-12）
- 輸入申請的 DNS【網域名稱】。
- 勾選【啟動 DNS 設定】。
- 按下【新增】鈕。（如圖 17-13）
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 www。
- 【對應 IP 位址】選擇 WAN1 並輸入 61.11.11.11。
- 【平衡模式】選擇循環分配。
- 按下【確定】鈕，【權重】選擇 1、【優先權】選擇 1。
- 再次按下【新增】鈕。（如圖 17-14）
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 www。
- 【對應 IP 位址】選擇 WAN2 並輸入 211.22.22.22。
- 【平衡模式】選擇循環分配。
- 按下【確定】鈕，【權重】選擇 2、【優先權】選擇 2，完成設定。（如圖 17-15）

圖 17-12InBound 負載平衡網域名稱設定

圖 17-13 設定第一條 InBound 負載平衡規則

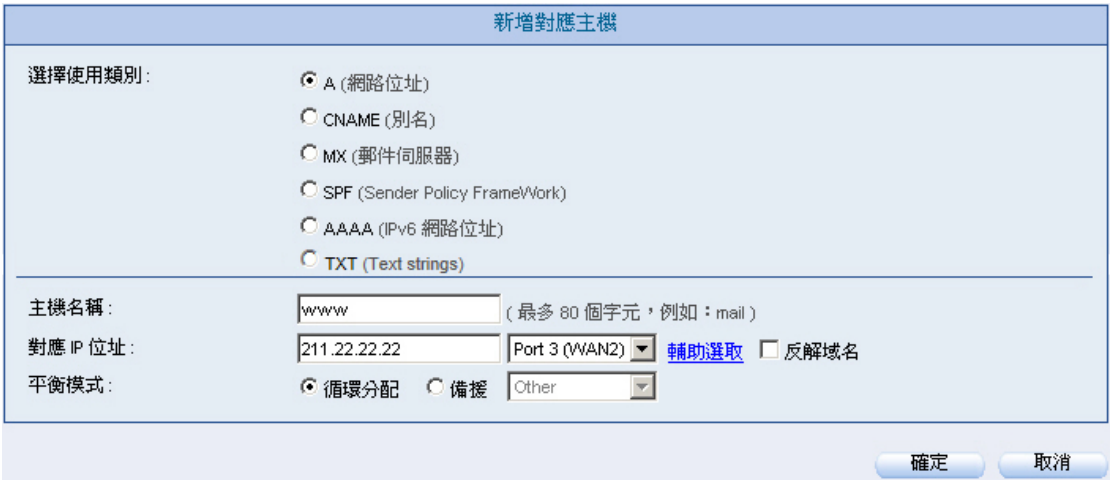


圖 17-14 設定第二條 InBound 負載平衡規則

圖 17-15 完成 InBound 負載平衡規則設定

步驟2. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：(如圖 17-16, 圖 17-17)

圖 17-16 第一條虛擬伺服器規則設定頁面

圖 17-17 第二條虛擬伺服器規則設定頁面

步驟3. 在【管制條例】>【外部至內部】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 17-18）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。（[連接埠對應]Web_Server(61.11.11.11)）
- 【服務名稱】選擇 HTTP(80)。
- 按下【確定】鈕。
- 再次按下【新增】鈕。（如圖 17-19）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。（[連接埠對應]Web_Server(211.22.22.22)）
- 【服務名稱】選擇 HTTP(80)。
- 按下【確定】鈕，完成設定。（如圖 17-20）

圖 17-18 設定第一條外部使用者存取內部伺服器服務之管制條例

圖 17-19 設定第二條外部使用者存取內部伺服器服務之管制條例

圖 17-20 完成管制條例設定

步驟4. 將尋求 Web 服務的連線分流於 WAN1 和 WAN2。（如圖 17-21）

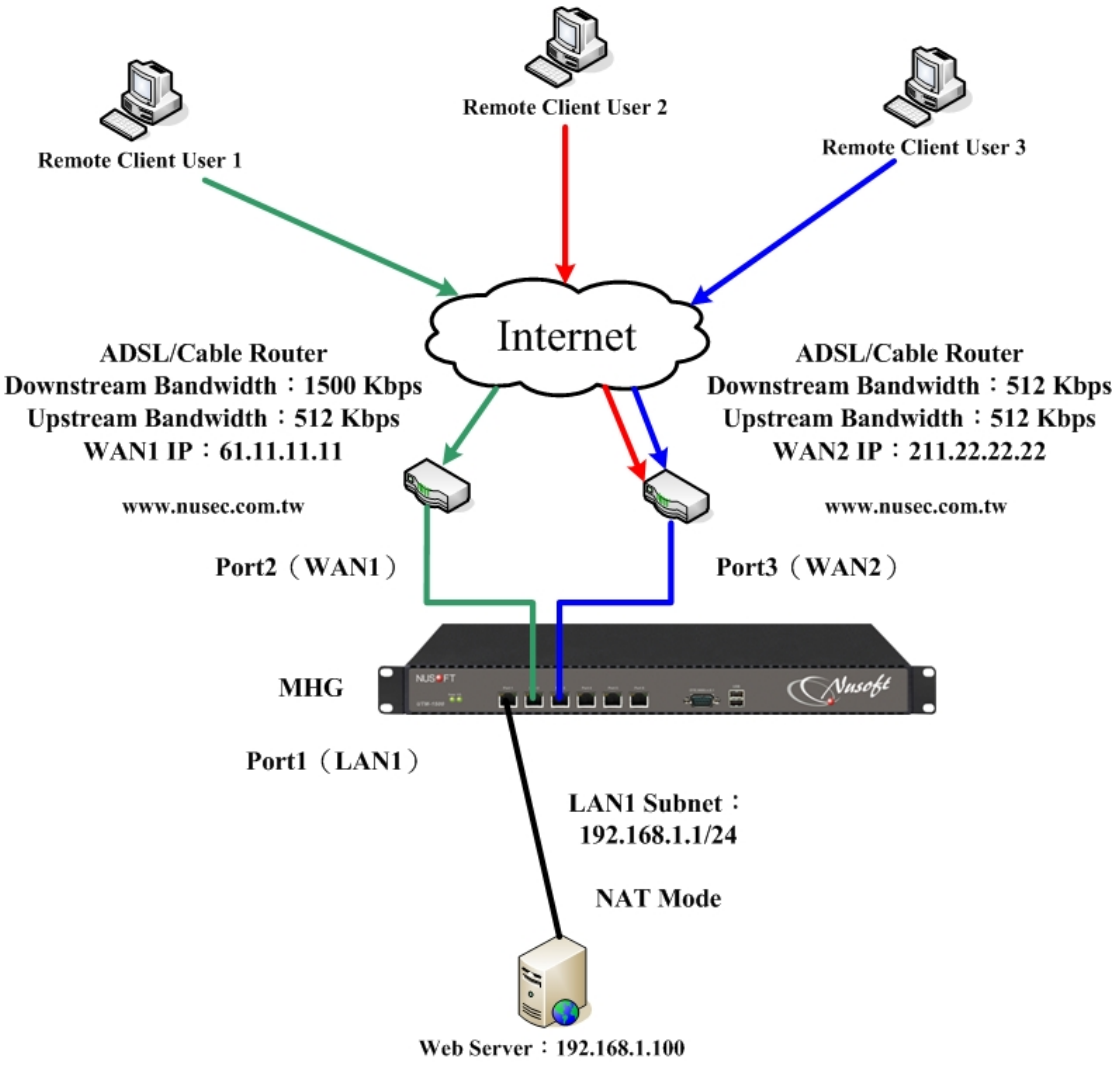


圖 17-21Web 伺服器透過 InBound 負載平衡循環分配機制提供服務之架設環境

說明：

1. 在 InBound 負載平衡功能設定下列資料：（如表 17-10）

名稱	類別	位址	權重	優先權
www.nusec.com.tw	A	61.11.11.11	1	1
www.nusec.com.tw	A	211.22.22.22	2	2

表 17-10www.nusec.com.tw 的 A 記錄

- 當使用者連線 www.nusec.com.tw 時，會依下列順序連到伺服器：
  - 第一位使用者透過 61.11.11.11 連到伺服器。
  - 第二位使用者透過 211.22.22.22 連到伺服器。
  - 第三位使用者透過 211.22.22.22 連到伺服器。（循環權重已分配完畢）
  - 第四位使用者透過 61.11.11.11 連到伺服器。（重新循環分配權重）

- 第五位使用者透過 211.22.22.22 連到伺服器。
- 第六位使用者透過 211.22.22.22 連到伺服器。

17.1.3 於 InBound 負載平衡設定 Web 伺服器採用 CNAME(別名)記錄的循環分配機制

步驟1. 在【進階功能】>【InBound 負載平衡】>【設定】頁面中，做下列設定：

- 按下【新增】鈕。(如圖 17-22)
- 輸入申請的 DNS【網域名稱】。
- 勾選【啟動 DNS 設定】。
- 按下【新增】鈕。(如圖 17-23)
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 web。
- 【對應 IP 位址】選擇 WAN1 並輸入 61.11.11.11。
- 【平衡模式】選擇循環分配。
- 按下【確定】鈕，【權重】選擇 1、【優先權】選擇 1。
- 再次按下【新增】鈕。(如圖 17-24)
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 web。
- 【對應 IP 位址】選擇 WAN2 並輸入 211.22.22.22。
- 【平衡模式】選擇循環分配。
- 按下【確定】鈕，【權重】選擇 2、【優先權】選擇 2。
- 再次按下【新增】鈕。(如圖 17-25)
- 【選擇使用類別】CNAME（別名）。
- 【別名】輸入 www。
- 【真實名稱】輸入 web.nusec.com.tw。
- 按下【確定】鈕，完成設定。(如圖 17-26)

圖 17-22InBound 負載平衡網域名稱設定

圖 17-23 設定第一條 InBound 負載平衡規則

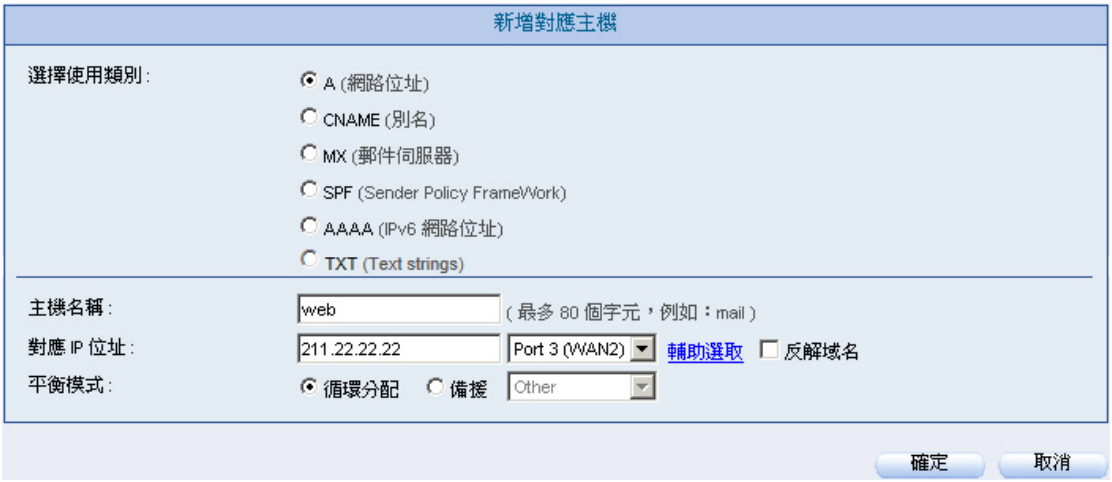


圖 17-24 設定第二條 InBound 負載平衡規則

圖 17-25 設定第三條 InBound 負載平衡規則

圖 17-26 完成 InBound 負載平衡規則設定

步驟2. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 17-27，圖 17-28）

圖 17-27 第一條虛擬伺服器規則設定頁面

圖 17-28 第二條虛擬伺服器規則設定頁面

步驟3. 在【管制條例】>【外部至內部】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 17-29）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。([連接埠對應]Web_Server(61.11.11.11))
- 【服務名稱】選擇 HTTP(80)。
- 按下【確定】鈕。
- 再次按下【新增】鈕。（如圖 17-30）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。([連接埠對應]Web_Server(211.22.22.22))
- 【服務名稱】選擇 HTTP(80)。
- 按下【確定】鈕，完成設定。（如圖 17-31）

圖 17-29 設定第一條外部使用者存取內部伺服器服務之管制條例

圖 17-30 設定第二條外部使用者存取內部伺服器服務之管制條例

圖 17-31 完成管制條例設定

步驟4. 將尋求 Web 服務的連線分流於 WAN1 和 WAN2。（如圖 17-32）

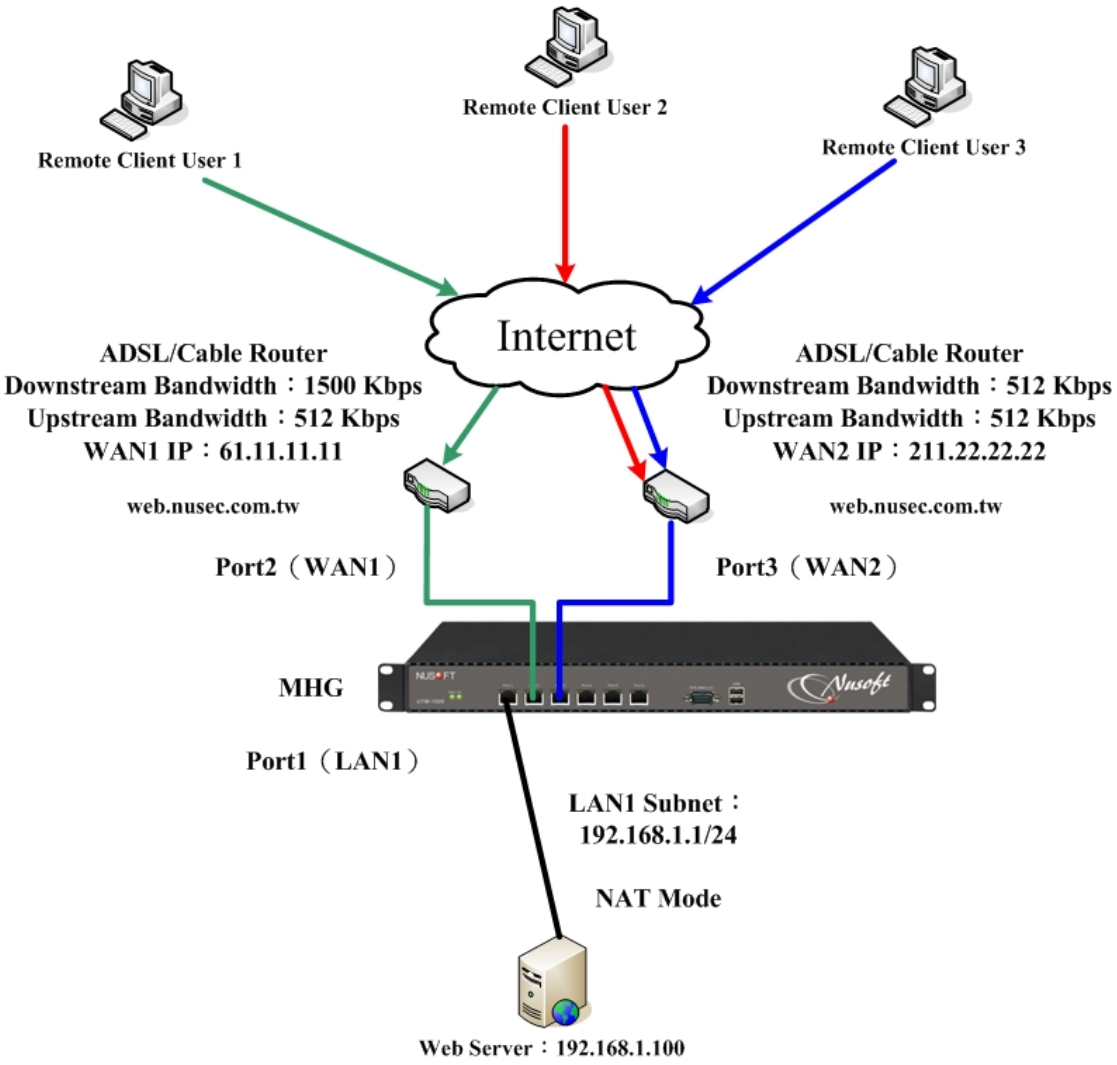


圖 17-32Web 伺服器透過 InBound 負載平衡循環分配機制提供服務之架設環境

說明：

1. 在 InBound 負載平衡功能設定下列資料：（如表 17-11）

名稱	類別	位址	權重	優先權
web.nusec.com.tw	A	61.11.11.11	1	1
web.nusec.com.tw	A	211.22.22.22	2	2
www.nusec.com.tw	CNAME	web.nusec.com.tw	--	--

表 17-11www.nusec.com.tw 的 CNAME 記錄

- 當使用者連線 www.nusec.com.tw 時，會依下列順序連到伺服器：
  - 第一位使用者透過 61.11.11.11 連到伺服器。
  - 第二位使用者透過 211.22.22.22 連到伺服器。
  - 第三位使用者透過 211.22.22.22 連到伺服器。（循環權重已分配完畢）

- 第四位使用者透過 61.11.11.11 連到伺服器。（重新循環分配權重）
- 第五位使用者透過 211.22.22.22 連到伺服器。
- 第六位使用者透過 211.22.22.22 連到伺服器。

17.1.4 於 InBound 負載平衡設定 MAIL 伺服器採用 MX（郵件伺服器）記錄的循環分配機制

步驟1. 在【進階功能】>【InBound 負載平衡】>【設定】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 17-33）
- 輸入申請的 DNS【網域名稱】。
- 勾選【啟動 DNS 設定】。
- 按下【新增】鈕。（如圖 17-34）
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 main。
- 【對應 IP 位址】選擇 WAN1 並輸入 61.11.11.11。
- 【平衡模式】選擇循環分配。
- 按下【確定】鈕，【權重】選擇 1、【優先權】選擇 1。
- 再次按下【新增】鈕。（如圖 17-35）
- 【選擇使用類別】A（網路位址）。
- 【主機名稱】輸入 main。
- 【對應 IP 位址】選擇 WAN2 並輸入 211.22.22.22。
- 【平衡模式】選擇循環分配。
- 按下【確定】鈕，【權重】選擇 2、【優先權】選擇 2。
- 再次按下【新增】鈕。（如圖 17-36）
- 【選擇使用類別】MX（郵件伺服器）。
- 【主機名稱】輸入 mail。
- 【郵件伺服器】輸入 main.nusec.com.tw。
- 按下【確定】鈕，完成設定。（如圖 17-37）

圖 17-33InBound 負載平衡網域名稱設定

圖 17-34 設定第一條 InBound 負載平衡規則

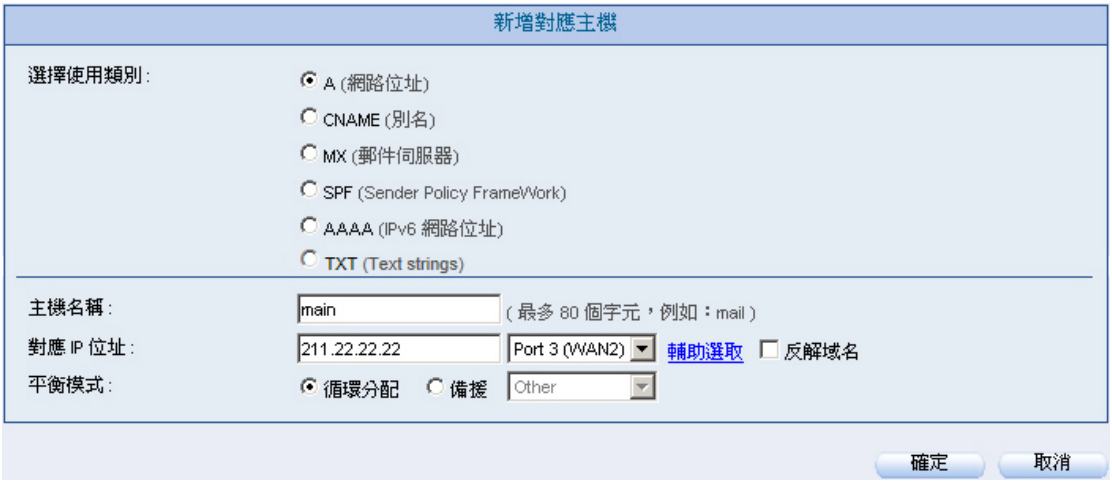


圖 17-35 設定第二條 InBound 負載平衡規則

圖 17-36 設定第三條 InBound 負載平衡規則

圖 17-37 完成 InBound 負載平衡規則設定

步驟2. 在【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 17-38, 圖 17-39, 圖 17-40, 圖 17-41）

圖 17-38 第一條虛擬伺服器規則設定頁面

圖 17-39 第二條虛擬伺服器規則設定頁面

圖 17-40 第三條虛擬伺服器規則設定頁面

圖 17-41 第四條虛擬伺服器規則設定頁面

步驟3. 在【管制條例】>【外部至內部】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 17-42）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。([連接埠對應]Mail_Server_POP3(61.11.11.11))
- 【服務名稱】選擇 POP3(110)。
- 按下【確定】鈕。
- 再次按下【新增】鈕。（如圖 17-43）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。([連接埠對應]Mail_Server_SMTP(61.11.11.11))
- 【服務名稱】選擇 SMTP(25)。
- 按下【確定】鈕。
- 再次按下【新增】鈕。（如圖 17-44）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。([連接埠對應]Mail_Server_POP3(211.22.22.22))
- 【服務名稱】選擇 POP3(110)。
- 按下【確定】鈕。
- 再次按下【新增】鈕。（如圖 17-45）
- 【目的網路位址】選擇所設定的虛擬伺服器規則。([連接埠對應]Mail_Server_SMTP(211.22.22.22))
- 【服務名稱】選擇 SMTP(25)。
- 按下【確定】鈕，完成設定。（如圖 17-46）

圖 17-42 設定第一條外部使用者存取內部伺服器服務之管制條例

圖 17-43 設定第二條外部使用者存取內部伺服器服務之管制條例

圖 17-44 設定第三條外部使用者存取內部伺服器服務之管制條例

圖 17-45 設定第四條外部使用者存取內部伺服器服務之管制條例

圖 17-46 完成管制條例設定

步驟4. 將尋求 E-mail 服務的連線分流於 WAN1 和 WAN2。（如圖 17-47）

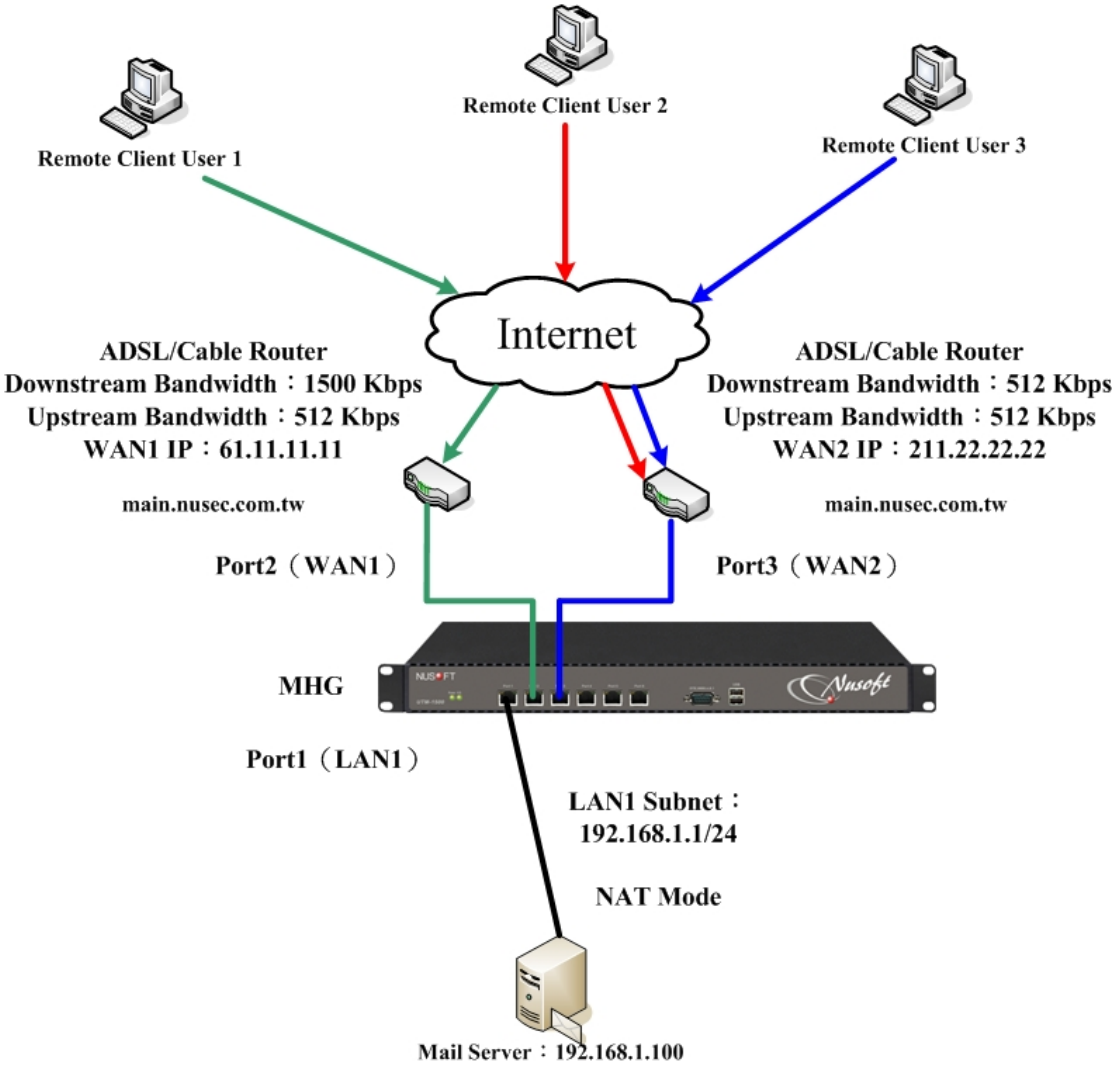


圖 17-47MAIL 伺服器透過 InBound 負載平衡循環分配機制提供服務之架設環境

說明：

1. 在 InBound 負載平衡功能設定下列資料：（如表 17-12）

名稱	類別	位址	權重	優先權
main.nusec.com.tw	A	61.11.11.11	1	1
main.nusec.com.tw	A	211.22.22.22	2	2
mail.nusec.com.tw.	MX	main.nusec.com.tw	--	--

表 17-12mail.nusec.com.tw 的 MX 記錄

- 當使用者連線 mail.nusec.com.tw 時，會依下列順序連到伺服器：
  - 第一位使用者透過 61.11.11.11 連到伺服器。
  - 第二位使用者透過 211.22.22.22 連到伺服器。

- 第三位使用者透過 211.22.22.22 連到伺服器。(循環權重已分配完畢)
- 第四位使用者透過 61.11.11.11 連到伺服器。(重新循環分配權重)
- 第五位使用者透過 211.22.22.22 連到伺服器。
- 第六位使用者透過 211.22.22.22 連到伺服器。

第18章　高可用性

MHG-2000 的硬體備援機制，採 Active/Standby 模式，系統正常運作的情況下網路存取皆透過指定的 MASTER 主機，同時會有一台 BACKUP 主機即時備份來自 MASTER 主機的所有資料；當目前運作中的 MAST 主機發生故障情形時，BACKUP 主機會即時取而代之成為 MASTER 主機，來保持內/外部網路不斷線，避免錯失商機。

【設定】功能概述：

本機模式 說明如下：

- 用來設定 MHG-2000 為 MASTER 或 BACKUP 主機。

高可用性連接埠 / 管理位址 說明如下：

- 用來設定 MASTER 和 BACKUP 設備，即時同步資料、軟體使用的介面位址。

高可用性連線狀態 說明如下：

- 用來顯示目前 MASTER 和 BACKUP 設備間的連線和同步狀態。

18.1 高可用性功能使用範例

18.1.1 建立一個高可用性（High Availability）的環境

環境設定

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接（可用的 IP 範圍：61.11.11.10 ~ 61.11.11.14），連上網際網路。

Port3 設為 WAN2（211.22.22.22）和 ATU-R 對接（可用的 IP 範圍：211.22.22.18 ~ 211.22.22.30），連上網際網路。

Port4 設為 DMZ1（透通路由模式）連接對外服務的伺服器。

步驟1. 先擬定一台 MHG-2000 做為 MASTER 主機，將其啟動並配置於網路環境中。（如圖 18-1）

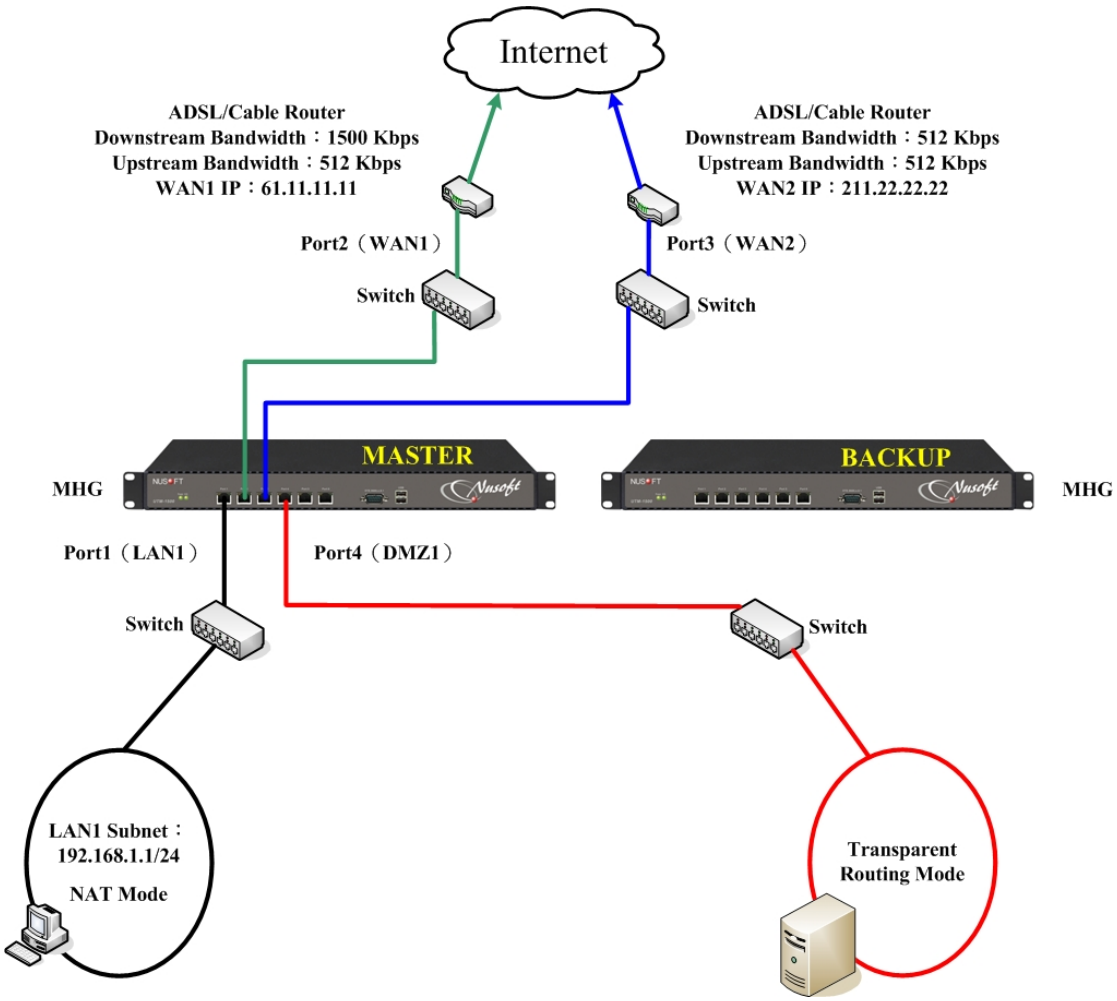


圖 18-1MASTER 主機之架設環境

步驟2. 在 MASTER 主機的【網路介面】>【介面位址】設定：（如圖 18-2）

埠號	名稱	模式	IP位址 / 子網路遮罩	飽和連線數	變更	優先權
1	LAN1	NAT / 路由	192.168.1.1 / 255.255.255.0	---	修改	---
2	WAN1	固定IP	61.11.11.11 / 255.255.255.0	---	修改	1
3	WAN2	固定IP	211.22.22.22 / 255.255.255.0	---	修改	2
4	DMZ1	透通路由模式	0.0.0.0 / 0.0.0.0	---	修改	---
5	Port5	---	0.0.0.0 / 0.0.0.0	---	修改	---
6	Port6	---	0.0.0.0 / 0.0.0.0	---	修改	---
7	Port7	---	0.0.0.0 / 0.0.0.0	---	修改	---

圖 18-2 網路介面位址設定

步驟3. 在 MASTER 主機的【進階功能】>【高可用性】>【設定】頁面中，做下列設定：

- 勾選【啟動高可用性功能】。
- 【本機模式】選擇主機。
- 【高可用性連接埠】選擇 Port1。
- 輸入指定的【高可用性管理位址】。（不可為 MHG-2000 其他功能、介面已採用的網段 IP）
- 按下【確定】鈕，完成設定。**（如圖 18-3）**

圖 18-3 高可用性 MASTER 主機設定頁面

步驟4. 將另一台尚未設定的 MHG-2000 BACKUP 主機（請確認其目前在關機狀態），和 MASTER 主機配置於同一網路環境（MASTER 主機與 BACKUP 主機的內部網路、外部網路和非軍事區網路埠需分別接在不同的交換器上），然後開啟電源。（如圖 18-4）

- 此時 MSATER 設備的高可用性，會呈現立即同步的連線狀態。（如圖 18-5）
- BACKUP 主機的【高可用性管理位址】（不可藉其登入 MHG-2000 的 Web UI），會於資料同步的時候依據 MASTER 主機的設定，配發一指定 IP。

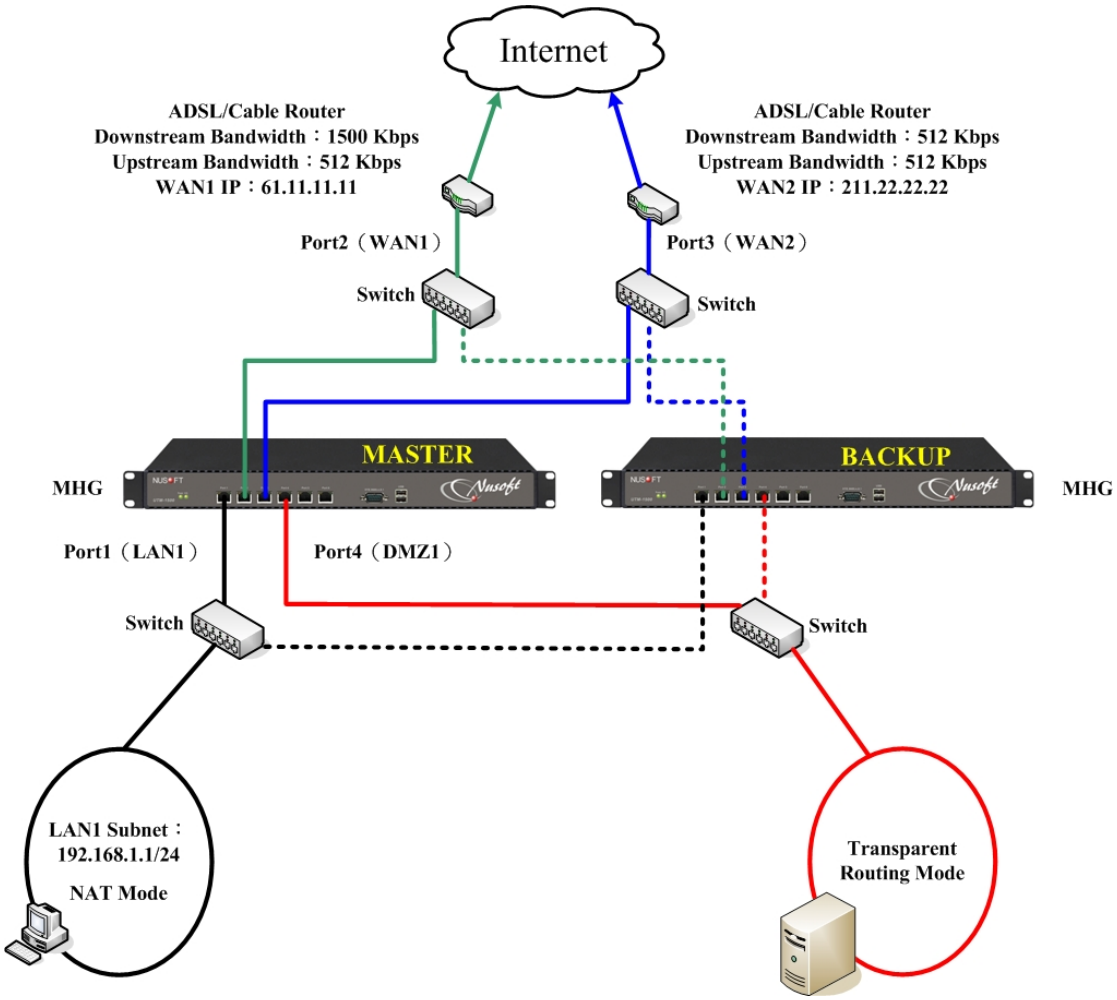


圖 18-4 高可用性的整體架設環境

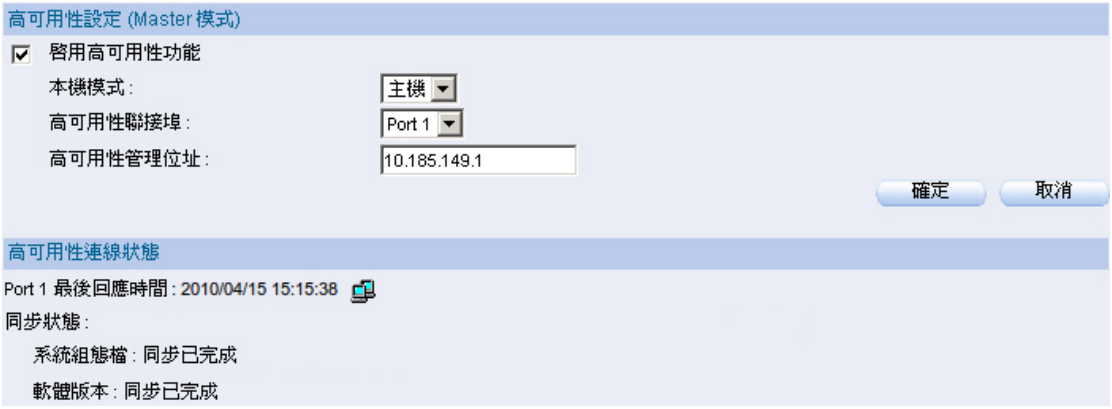


圖 18-5MASTER 主機連線同步狀態

注意：

1. MASTER 主機設定的【高可用性連接埠】，要和 BACKUP 主機相映的網路介面連接。
2. 在架設完高可用性環境後，MASTER 和 BACKUP 主機間的第一次資料立即同步作業，若是在完成前，為不可抗拒之因素而中斷。此時，必須先將 BACKUP 主機從網路環境中獨立出來，做恢復原廠預設值和格式化硬碟的動作，然後再依循上述的步驟完成同步作業。同步的狀態可於高可用性功能介面查看。

說明：

1. 在配置高可用性環境時，做為 MASTER 的設備一定要先完成開機動作，確定其管理介面可登入後，再將 BACKUP 設備開啟，避免資料同步異常的問題。
2. MHG-2000 內建硬碟，可由使用者自行更換。要特別注意的是，更換時所使用的硬碟一定要等於或大於目前使用的容量，以避免資料同步時，遺失資料的情形發生。(最好是先更換 BACKUP 主機的硬碟，於其向 MASTER 主機同步完資料後；再行更換 MASTER 主機的硬碟，讓其向 BACKUP 主機同步資料)
3. 在架設完成後，MASTER 主機會直接運作，BACKUP 主機則呈待命狀態，隨時偵測 MASTER 主機的運作狀況。
4. 當 MASTER 主機有資料的寫入、異動或軟體更新時，會立即透過【高可用性連接埠】將更動的資料寫入 BACKUP 主機中。
5. 當 MASTER 主機發生故障狀況時，BACKUP 主機會備援為 MASTER 模式運作；當排除 MASTER 主機的故障問題，並將其配置回 HA 環境時，MASTER 主機會先向 BACKUP 主機取得維修期間系統運作的相關資料，然後再接手控管網路的使用。**(如圖 18-6)**

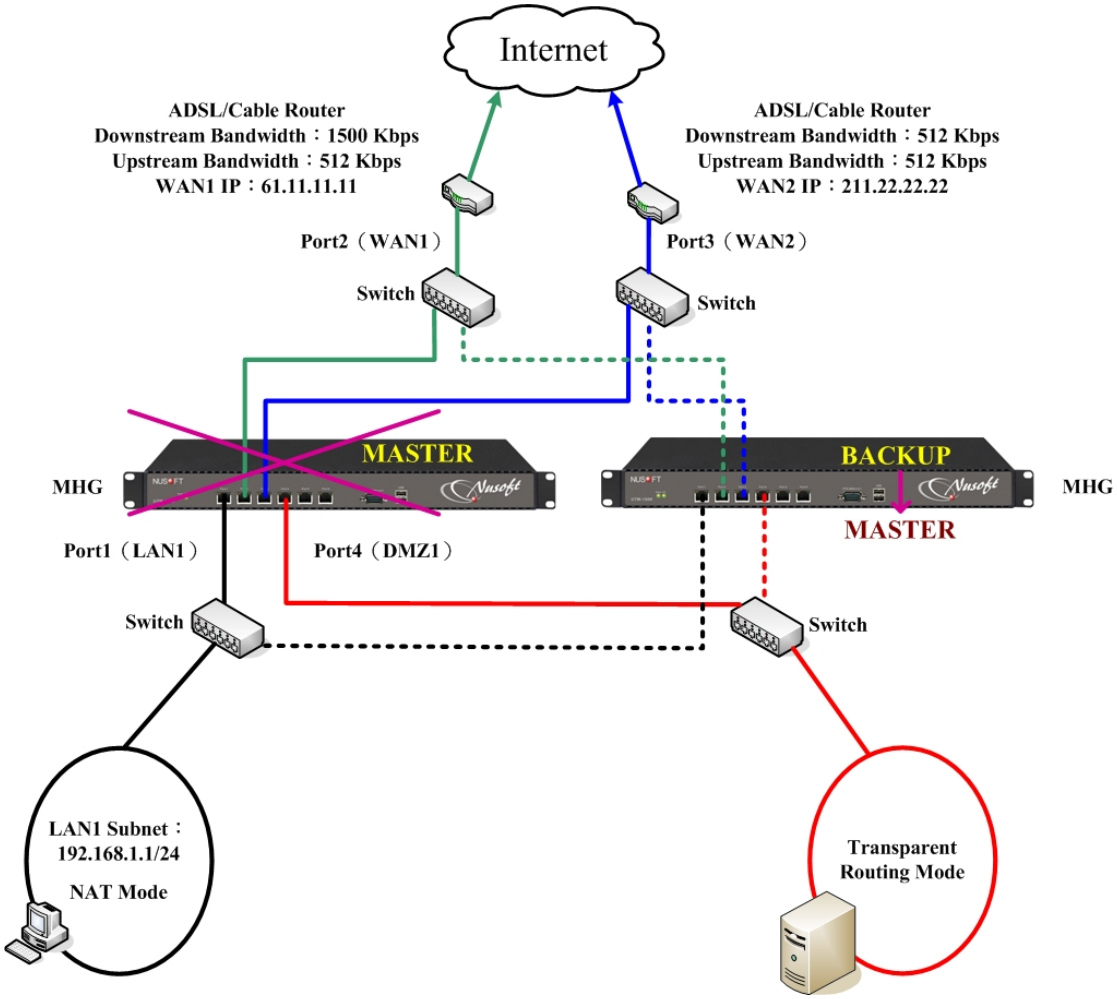


圖 18-6 高可用性 MASTER 主機故障時之備援狀態

6. 高可用性（High Availability）注意事項：

- 非固接 IP 外部網路介面：於 HA 備援重新取得 IP 前，無法透過此介面存取網路資源。
- IPSec VPN 連線：要設定保持連線 IP，才可在 HA 備援後，於短時間內自動建起 VPN 連線。
- PPTP VPN 連線：於 HA 備援時連線會中斷，外部終端使用者需自行重新建立連線。

第19章　聯合防禦系統

透過特定交換器（Switch），即時監控內部網路設備的分部狀況，並於內部網路發出大量異常封包時，阻擋此類封包的傳送，協助管理人員盡速排除異常狀態，避免企業網路癱瘓。

【核心交換器】功能概述：

名稱 說明如下：

- 交換器的連線名稱。

交換器型號 說明如下：

- 選擇欲建立連線的交換器類型。

網際協定 說明如下：

- 交換器連線位址採用的網際網路協定，可為 IPv4 或 IPv6。

核心交換器 IP 位址 說明如下：

- 核心交換器的連線、登入位址。

埠號 說明如下：

- 系統以 TELNET 方式連入核心交換器時所使用的埠號。

帳戶名稱 說明如下：

- 系統以 TELNET 方式連入核心交換器時所使用的帳號。

密碼 說明如下：

- 系統以 TELNET 方式連入核心交換器時所使用的密碼。

MAC 位址格式 說明如下：

- 設定核心交換器所接受的 MAC 格式，常見格式如下：
  - XX : XX : XX : XX : XX : XX
  - XX – XX – XX – XX – XX – XX
  - XXXXXXXXXXXX
  - XXXXXX - XXXXXX

阻擋指令 說明如下：

- 系統用來告知核心交換器要阻擋的異常流量 IP/MAC。

刪除阻擋指令 說明如下：

- 用來刪除核心交換器已阻擋的 IP/MAC。

檢視阻擋清單指令 說明如下：

- 用來檢視核心交換器已阻擋的 IP/MAC。

說明：

1. 系統會將偵測到的內部異常流量資訊，透過下列變數進行交換器阻擋、刪除已阻擋和檢視已阻擋 IP/MAC 的指令設定：
   - _ip_：代表阻擋的 IP 位址。
   - _mac_：代表阻擋的 MAC 位址。
   - _port_：代表交換器的埠號。

【交換器 MAC 表】功能概述：

搜尋 說明如下：

- 可依照交換器名稱、交換器埠和 MAC 位址等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【進階功能】>【聯合防禦系統】>【交換器 MAC 表】的【搜尋】頁面中，做下列設定：
    - 【交換器名稱】輸入所連線交換器的指定代稱。
    - 按下【搜尋】鈕。（如圖 19-1）

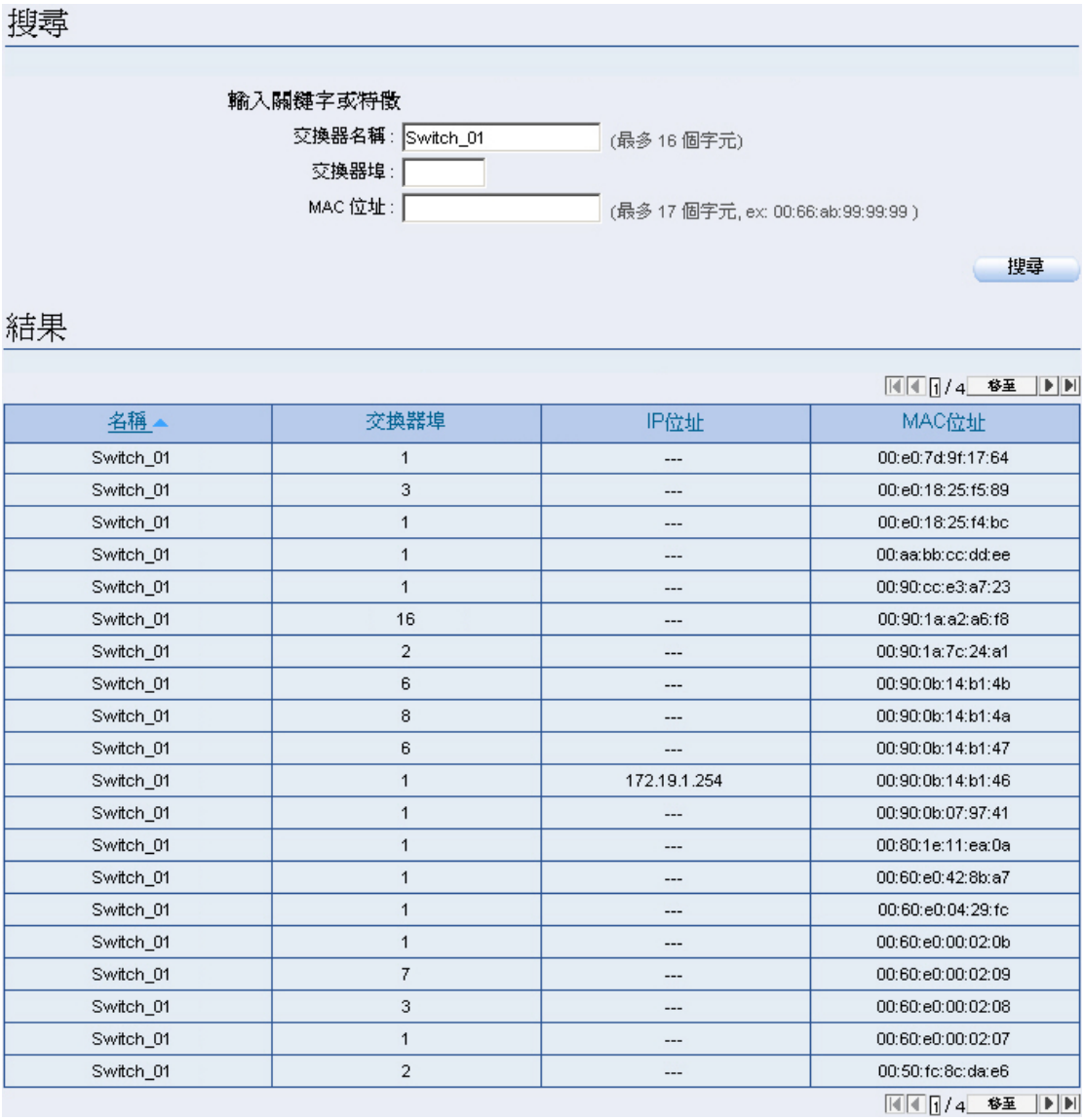

搜尋
輸入關鍵字或特徵
交換器名稱 : Switch_01 (最多 16 個字元)
交換器埠 :
MAC 位址 : (最多 17 個字元, ex: 00:66:ab:99:99:99)
搜尋
結果
1 / 4 移至
名稱 交換器埠 IP位址 MAC位址
Switch_01 1 --- 00:e0:7d:9f:17:64
Switch_01 3 --- 00:e0:18:25:f5:89
Switch_01 1 --- 00:e0:18:25:f4:bc
Switch_01 1 --- 00:aa:bb:cc:dd:ee
Switch_01 1 --- 00:90:cc:e3:a7:23
Switch_01 16 --- 00:90:1a:a2:a6:f8
Switch_01 2 --- 00:90:1a:7c:24:a1
Switch_01 6 --- 00:90:0b:14:b1:4b
Switch_01 8 --- 00:90:0b:14:b1:4a
Switch_01 6 --- 00:90:0b:14:b1:47
Switch_01 1 172.19.1.254 00:90:0b:14:b1:46
Switch_01 1 --- 00:90:0b:07:97:41
Switch_01 1 --- 00:80:1e:11:ea:0a
Switch_01 1 --- 00:60:e0:42:8b:a7
Switch_01 1 --- 00:60:e0:04:29:fc
Switch_01 1 --- 00:60:e0:00:02:0b
Switch_01 7 --- 00:60:e0:00:02:09
Switch_01 3 --- 00:60:e0:00:02:08
Switch_01 1 --- 00:60:e0:00:02:07
Switch_01 2 --- 00:50:fc:8c:da:e6
1 / 4 移至

圖 19-1 搜尋特定記錄

19.1 聯合防禦系統功能使用範例

19.1.1 透過指定的核心交換器和監控的邊緣交換器，迅速隔離、排除內部網路異常狀況

步驟1. 在【進階功能】>【聯合防禦系統】>【核心交換器】頁面中，做下列設定：（如圖 19-2）

- 【名稱】輸入欲連線交換器的指定代稱。
- 選擇指定的【交換器型號】、【網際協定】。
- 輸入【核心交換器 IP 位址】。
- 輸入和核心交換器建立連線的【埠號】、【帳戶名稱】、【密碼】。
- 按下【確定】鈕，完成設定。（如圖 19-3）
  - 按下【檢視】鈕，可察看核心交換器阻擋的 IP/MAC 位址。（如圖 19-4）
  - 按下【修改】鈕，可修改核心交換器連線設定。（如圖 19-5）
  - 按下【刪除】鈕，可刪除指定核心交換器連線設定。（如圖 19-6）
  - 點擊【刪除被阻擋位址】連結，可清除已被核心交換器阻擋的指定 IP/MAC 位址。（如圖 19-7）

圖 19-2 設定核心交換器連線

圖 19-3 完成核心交換器連線設定

圖 19-4 檢視核心交換器阻擋指令

圖 19-5 修改核心交換器連線設定

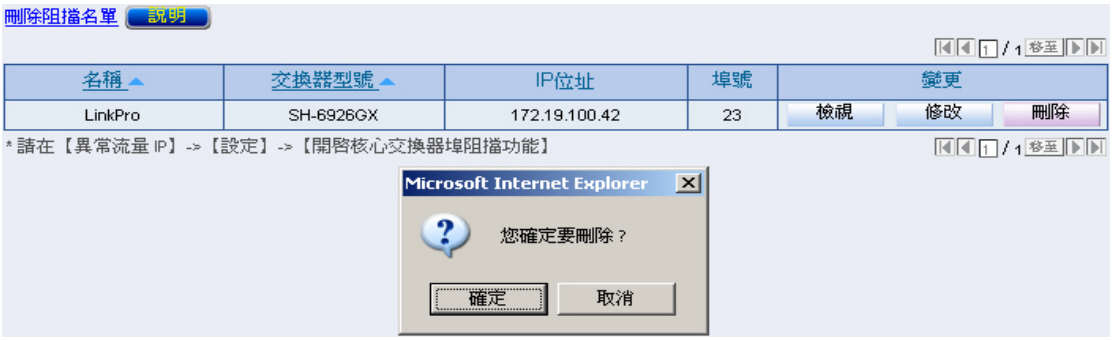


圖 19-6 刪除核心交換器連線設定

圖 19-7 刪除被阻擋的指定 IP/MAC 位址

⚠ 注意：

1. 要在【異常流量 IP】>【設定】頁面中【開啟聯合防禦系統】功能：**（如圖 19-8）**

圖 19-8 異常流量 IP 設定頁面

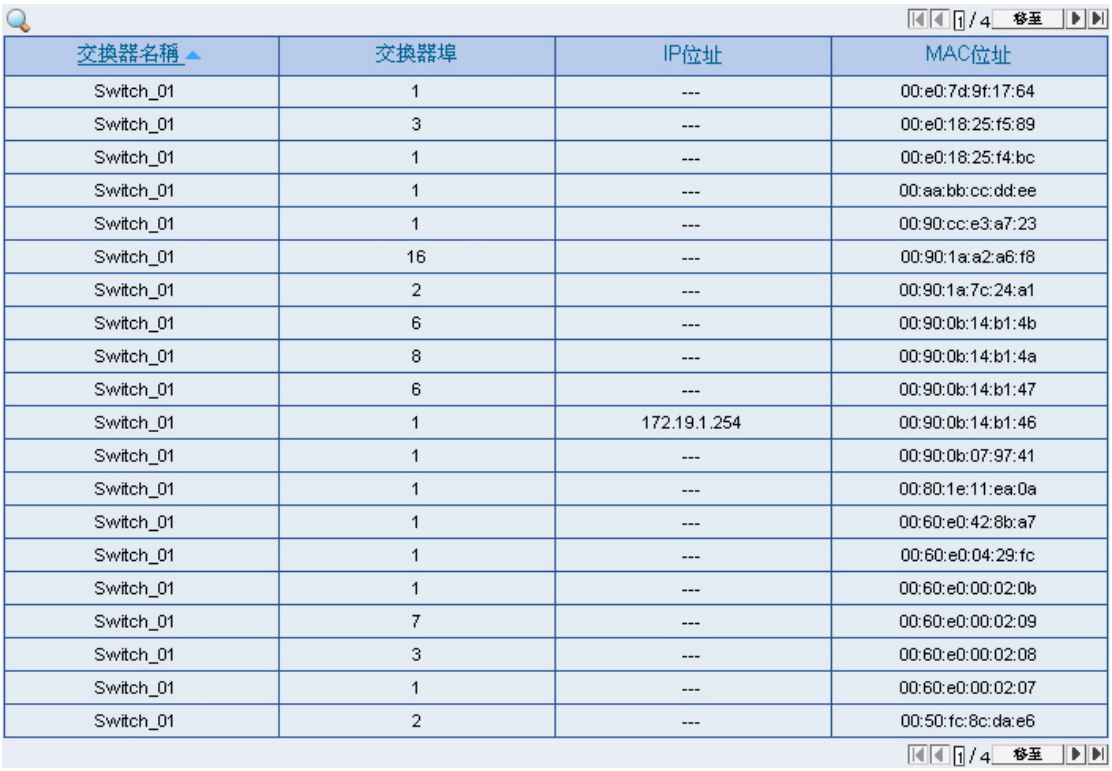
步驟2. 在【進階功能】>【聯合防禦系統】>【邊緣交換器】頁面中，做下列設定：（如圖 19-9）

- 【交換器名稱】輸入欲連線交換器的指定代稱。
- 選擇指定的【網際協定】。
- 輸入交換器的【IP 位址】、【SNMP 登入名稱】。
- 按下【確定】鈕，完成設定。（如圖 19-10）

圖 19-9 設定邊緣交換器連線

圖 19-10 完成邊緣交換器連線設定

步驟3. 在【進階功能】>【聯合防禦系統】>【交換器 MAC 表】頁面中，可透過 SNMP 服務，取得經由邊緣交換器傳送封包的設備 MAC 清單。（如圖 19-11）



1 / 4 移至

交換器名稱	交換器埠	IP位址	MAC位址
Switch_01	1	---	00:e0:7d:9f:17:64
Switch_01	3	---	00:e0:18:25:f5:89
Switch_01	1	---	00:e0:18:25:f4:bc
Switch_01	1	---	00:aa:bb:cc:dd:ee
Switch_01	1	---	00:90:cc:e3:a7:23
Switch_01	16	---	00:90:1a:a2:a6:f8
Switch_01	2	---	00:90:1a:7c:24:a1
Switch_01	6	---	00:90:0b:14:b1:4b
Switch_01	8	---	00:90:0b:14:b1:4a
Switch_01	6	---	00:90:0b:14:b1:47
Switch_01	1	172.19.1.254	00:90:0b:14:b1:46
Switch_01	1	---	00:90:0b:07:97:41
Switch_01	1	---	00:80:1e:11:ea:0a
Switch_01	1	---	00:60:e0:42:8b:a7
Switch_01	1	---	00:60:e0:04:29:fc
Switch_01	1	---	00:60:e0:00:02:0b
Switch_01	7	---	00:60:e0:00:02:09
Switch_01	3	---	00:60:e0:00:02:08
Switch_01	1	---	00:60:e0:00:02:07
Switch_01	2	---	00:50:fc:8c:da:e6

1 / 4 移至

圖 19-11 透過邊緣交換器傳送封包的設備 MAC 清單

說明：

1. 在【進階功能】>【聯合防禦系統】>【週邊交換器】頁面中，按下設定清單的【內容】鈕，可為交換器的每一埠做註解。（如圖 19-12，圖 19-13）

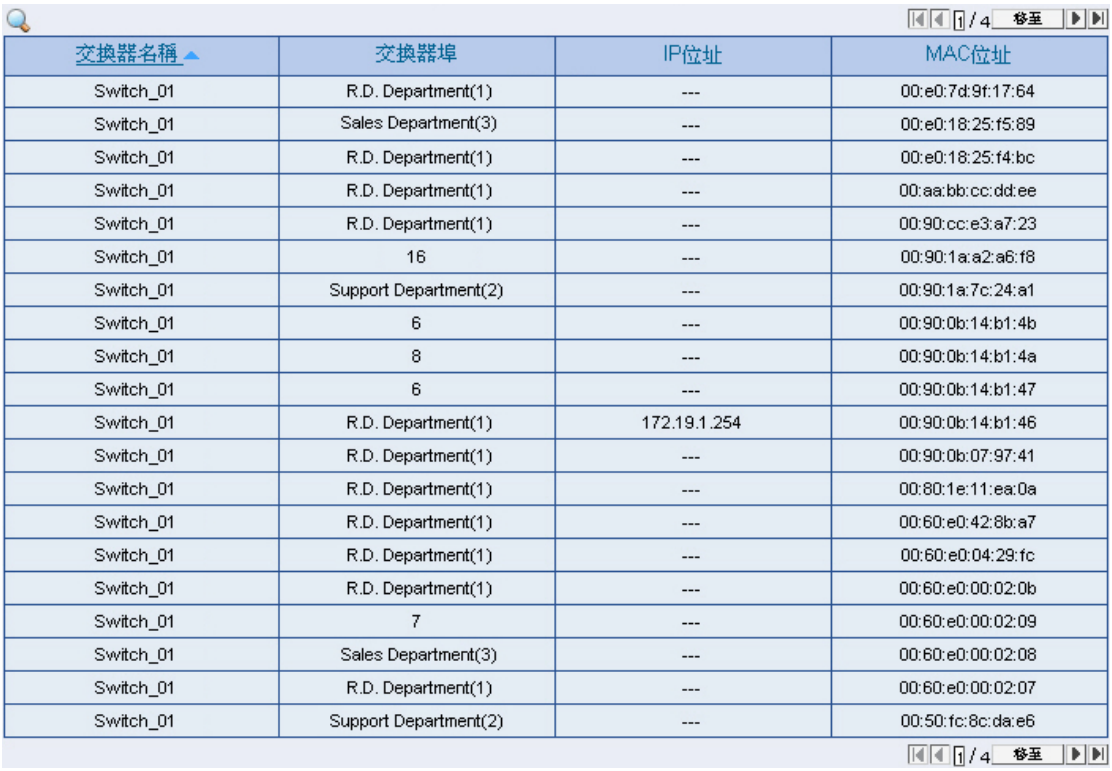
名稱 : Switch_01

交換器埠總數 : 27

交換器埠	ID	交換器資訊	註解
1	1	Port 1 on Unit 1	R.D. Department
2	2	Port 2 on Unit 1	Support Department
3	3	Port 3 on Unit 1	Sales Department
4	4	Port 4 on Unit 1	
5	5	Port 5 on Unit 1	
6	6	Port 6 on Unit 1	
7	7	Port 7 on Unit 1	
8	8	Port 8 on Unit 1	
9	9	Port 9 on Unit 1	
10	10	Port 10 on Unit 1	
11	11	Port 11 on Unit 1	
12	12	Port 12 on Unit 1	
13	13	Port 13 on Unit 1	
14	14	Port 14 on Unit 1	
15	15	Port 15 on Unit 1	
16	16	Port 16 on Unit 1	
17	17	Port 17 on Unit 1	
18	18	Port 18 on Unit 1	
19	19	Port 19 on Unit 1	
20	20	Port 20 on Unit 1	
21	21	Port 21 on Unit 1	
22	22	Port 22 on Unit 1	
23	23	Port 23 on Unit 1	
24	24	Port 24 on Unit 1	
25	25	Port 25 on Unit 1	
26	26	Port 26 on Unit 1	
27	27	ethernet switch low driver	

取消

圖 19-12 為邊緣交換器埠做註解



1 / 4 移至

交換器名稱	交換器埠	IP位址	MAC位址
Switch_01	R.D. Department(1)	---	00:e0:7d:9f:17:64
Switch_01	Sales Department(3)	---	00:e0:18:25:f5:89
Switch_01	R.D. Department(1)	---	00:e0:18:25:f4:bc
Switch_01	R.D. Department(1)	---	00:aa:bb:cc:dd:ee
Switch_01	R.D. Department(1)	---	00:90:cc:e3:a7:23
Switch_01	16	---	00:90:1a:a2:a6:f8
Switch_01	Support Department(2)	---	00:90:1a:7c:24:a1
Switch_01	6	---	00:90:0b:14:b1:4b
Switch_01	8	---	00:90:0b:14:b1:4a
Switch_01	6	---	00:90:0b:14:b1:47
Switch_01	R.D. Department(1)	172.19.1.254	00:90:0b:14:b1:46
Switch_01	R.D. Department(1)	---	00:90:0b:07:97:41
Switch_01	R.D. Department(1)	---	00:80:1e:11:ea:0a
Switch_01	R.D. Department(1)	---	00:60:e0:42:8b:a7
Switch_01	R.D. Department(1)	---	00:60:e0:04:29:fc
Switch_01	R.D. Department(1)	---	00:60:e0:00:02:0b
Switch_01	7	---	00:60:e0:00:02:09
Switch_01	Sales Department(3)	---	00:60:e0:00:02:08
Switch_01	R.D. Department(1)	---	00:60:e0:00:02:07
Switch_01	Support Department(2)	---	00:50:fc:8c:da:e6

1 / 4 移至

圖 19-13 顯示交換器埠註解訊息的 MAC 表

步驟4. 當 MHG-2000 收到超過內定偵測標準的異常封包時，【異常流量 IP】>【異常流量報告】：（如圖 19-14）

- 會被指定的【核心交換器】阻擋，大幅將低 MHG-2000 的負荷量。
- 同時可透過【邊緣交換器】的監控訊息，迅速針對明確的目標，做即時的異常排除作業。

圖 19-14 異常流量報告

第20章　證書管理

用來匯入或產生電子憑證，以供連線 MHG-2000（WebUI、IPSec VPN、SSL Web VPN）驗證所需。

【證書管理】功能概述：

本地 CA 憑證 說明如下：

- MHG-2000 簽核憑證申請的驗證檔，即 Local 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。

遠端 CA 憑證 說明如下：

- 外部主機簽核憑證申請的驗證檔，即 Remote 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。

授權憑證 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。

PEM 說明如下：

- 通常特指支援 PEM（Privacy Enhanced Mail）格式的金鑰或者憑證檔案。
- 此種格式可存放多張憑證於一個檔案中(支援憑證鏈)；當有多張憑證時，發行者的憑證，將依序放置於被發行的憑證之下。

PKCS#12 說明如下：

- 即公開金鑰密碼編譯標準（Public Key Cryptography Standards, PKCS），通常特指帶有私鑰（採密碼保護）的憑證檔案，因此具有可攜帶、交換的特性。
- 可以將相關憑證匯入到某個 KeyStore 中，便可以在該 KeyStore 中使用原有的憑證與私密金鑰(不需重新申請)。

說明：

1. KeyStore：指的是存放私密金鑰（Private Key）與憑證的地方。

【本地 CA 憑證】列表概述：

名稱 說明如下：

- 於 MHG-2000 建立的 CA 憑證名稱。

主旨 說明如下：

■ 於 MHG-2000 建立的 CA 憑證設定資訊。

變更 說明如下：

■ 可檢視憑證詳細資料、下載或刪除已建置於 MHG-2000 的憑證。（如圖 20-1）

圖 20-1 本地 CA 憑證列表

說明：

1. 系統預設的 default_ca 憑證不可刪除，僅能檢視或下載。

【遠端 CA 憑證】列表概述：

名稱 說明如下：

■ 匯入 MHG-2000 的 CA 憑證名稱。

主旨 說明如下：

■ 匯入 MHG-2000 的 CA 憑證設定資訊。

變更 說明如下：

■ 可檢視憑證詳細資料、下載或刪除已建置於 MHG-2000 的憑證。（如圖 20-2）

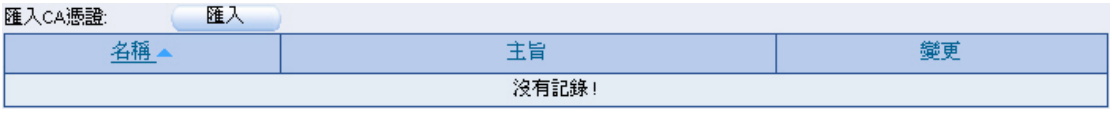


圖 20-2 遠端 CA 憑證列表

【授權憑證】列表概述：

L 說明如下：

■ 可分為兩種情形：

◆ --：代表匯入經由 CA Server 簽署非本機設定 CSR（Certificate Signing Request）所取回之憑證。

◆ V：代表在本機設定之 CSR（Certificate Signing Request），再匯入其經由 CA Server 簽署後所取回之憑證、經 MHG-2000 的 CA 憑證簽核。

名稱 說明如下：

■ 經 MHG-2000 簽核、匯入經由 CA Server 簽署之憑證或在本機設定之 CSR（Certificate Signing Request）名稱。

主旨 說明如下：

■ 經 MHG-2000 簽核、匯入經由 CA Server 簽署之憑證或在本機設定之 CSR（Certificate Signing Request）設定資訊。

變更 說明如下：

■ 可檢視憑證或在本機設定之 CSR（Certificate Signing Request）詳細資料、下載或刪除已建置於 MHG-2000 的憑證、CSR（Certificate Signing Request）。**（如圖 20-3）**

圖 20-3 授權憑證列表

說明：

1. 系統預設的 default_server、default_client 憑證不可刪除，僅能檢視或下載。

20.1 證書管理功能使用範例

20.1.1 透過自訂 CA 和授權憑證，提供連線 MHG-2000（WebUI、IPSec VPN、SSL Web VPN）驗證所需

步驟1. 在【進階功能】>【證書管理】>【本地 CA 憑證】頁面中，做下列設定：（如圖 20-4）

- 【名稱】輸入 CA_Certificate。
- 【憑證公用名稱】輸入 CA。
- 【國家】選擇 Taiwan。
- 【州/省】輸入 Taiwan。
- 【地區（城市）】輸入 Taipei。
- 【公司】輸入 Nusoft。
- 【單位】輸入 Authorization。
- 【電子郵件】輸入 auth@nusoft.com.tw。
- 【金鑰長度】選擇 2048。
- 輸入指定的【有效時間】。
- 按下【確定】鈕，完成設定。（如圖 20-5）

圖 20-4 設定本地 CA 憑證

圖 20-5 完成本地 CA 憑證設定

步驟2. 在【進階功能】>【證書管理】>【授權憑證】頁面中，做下列設定：

- 按下【新增】鈕。（如圖 20-6）
- 【名稱】輸入 Signed_Certificate_1。
- 【憑證公用名稱】輸入 MHG-2000 網路介面位址（或其對應的網域名稱）。
- 【國家】選擇 Taiwan。
- 【州/省】輸入 Taiwan。
- 【地區（城市）】輸入 Taipei。
- 【公司】輸入 Nusoft。
- 【單位】輸入 Support。
- 【電子郵件】輸入 support@nusoft.com.tw。
- 【金鑰長度】選擇 2048。
- 輸入指定的【有效時間】。
- 按下【確定】鈕。（如圖 20-7）
- 按下【簽章】鈕。
- 選擇 CA 憑證 CA_Certificate 來進行【簽章】。（如圖 20-8）
- 輸入指定的【有效時間】。
- 按下【確定】鈕。（如圖 20-9）
- 再次按下【新增】鈕。（如圖 20-10）
- 【名稱】輸入 Signed_Certificate_2。
- 【憑證公用名稱】輸入 MHG-2000 網路介面位址（或其對應的網域名稱）。
- 【國家】選擇 Taiwan。
- 【州/省】輸入 Taiwan。
- 【地區（城市）】輸入 Taipei。
- 【公司】輸入 Nusoft。
- 【單位】輸入 Sales。
- 【電子郵件】輸入 sales@nusoft.com.tw。
- 【金鑰長度】選擇 2048。
- 輸入指定的【有效時間】。
- 按下【確定】鈕。（如圖 20-11）
- 按下【簽章】鈕。
- 選擇 CA 憑證 CA_Certificate 來進行【簽章】。（如圖 20-12）
- 輸入指定的【有效時間】。
- 按下【確定】鈕，完成設定。（如圖 20-13）

圖 20-6 設定第一筆 CSR

圖 20-7 完成第一筆 CSR 設定

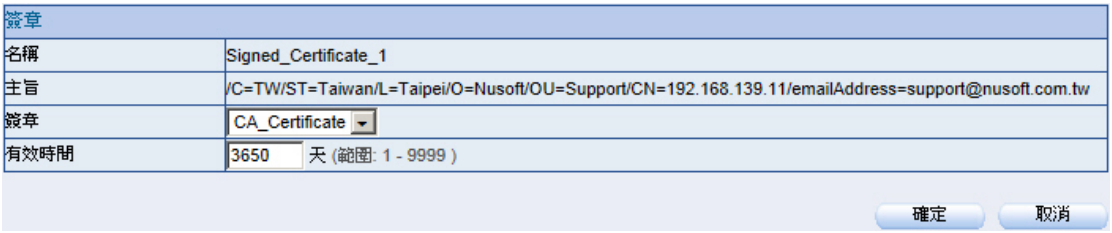


圖 20-8 簽核第一筆 CSR

圖 20-9 產生第一筆授權憑證

圖 20-10 設定第二筆 CSR

圖 20-11 完成第二筆 CSR 設定

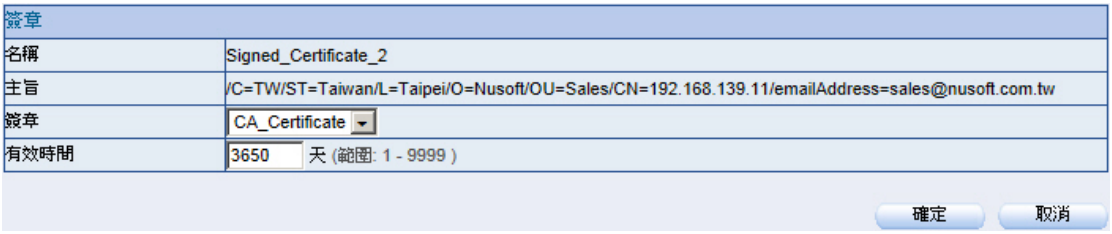


圖 20-12 簽核第二筆 CSR

圖 20-13 產生第二筆授權憑證

步驟3. 在【系統管理】>【組態】>【系統設定】頁面的【系統管理介面登入設定】欄位中，做下列設定：**（如圖 20-14）**

- 【SSL 憑證】選擇所建置的授權憑證。（Signed_Certificate_1(CA_Certificate)或 Signed_Certificate_2(CA_Certificate)）

圖 20-14 設定以 HTTPS 協定登入系統管理介面所採用的安全性憑證

步驟4. 以 HHTPS 協定登入系統管理介面時，會採用指定的電子憑證做安全性驗證。**（如圖 20-15）**

圖 20-15 以 HTTPS 協定登入系統管理介面的安全性驗證

步驟5. 在【SSL Web VPN】>【設定】頁面的【SSL Web VPN 組態設定】欄位中，做下列設定：（如圖 20-16）

- 【CA 憑證】選擇所建置的本地 CA 憑證。（CA_Certificate）
- 【本地授權憑證】選擇所建置的授權憑證。（Signed_Certificate_1）
- 【遠端授權憑證】選擇所建置的授權憑證。（Signed_Certificate_2）

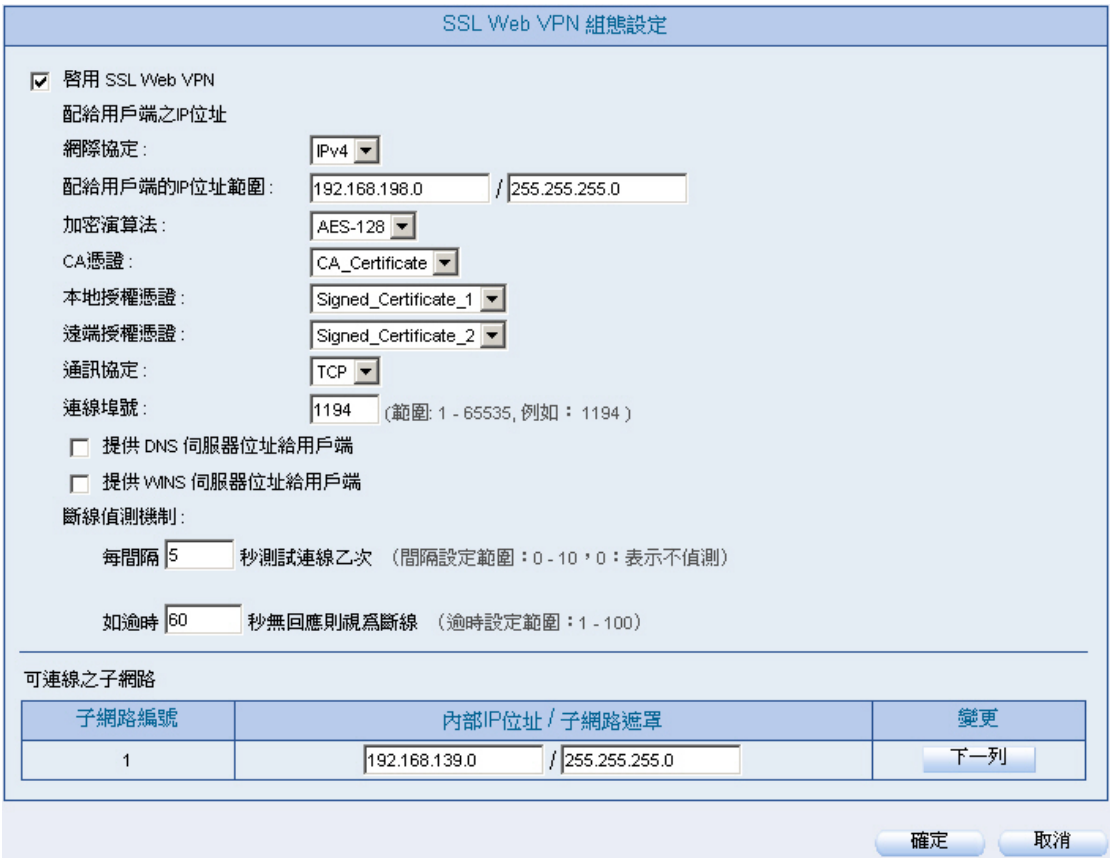


圖 20-16 設定和 MHG-2000 建立 SSL Web VPN 連線所採用的安全性憑證

步驟6. 和 MHG-2000 建立 SSL Web VPN 連線時，會採用指定的電子憑證做安全性驗證。（如圖 20-17）

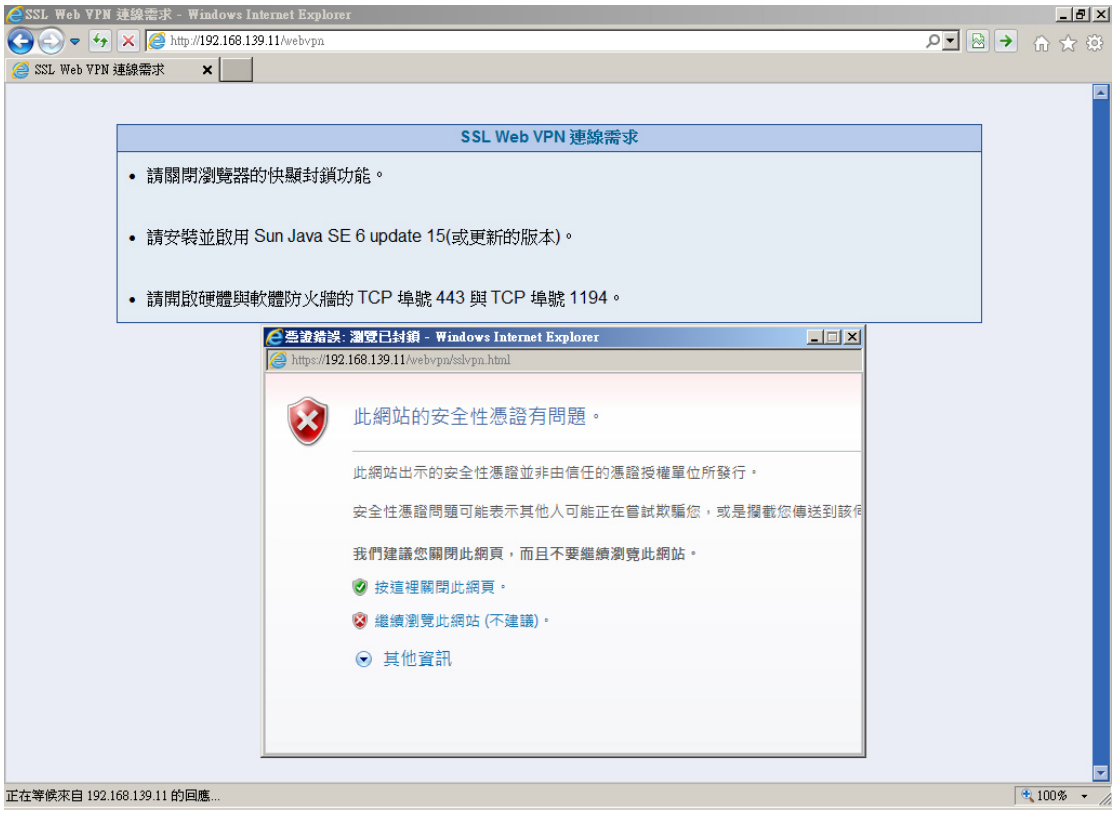


圖 20-17 和 MHG-2000 建立 SSL Web VPN 連線的安全性驗證

說明：

1. 關於【遠端 CA 憑證】的應用可參閱第十一章的範例 4。
2. 若要將目前建置的【本地 CA 憑證】簽核之【授權憑證】應用於 IPSec VPN。(環境設定：目前完成【授權憑證】設定的設備為甲端，另一方為乙端，以此兩端建立 IPSec VPN 連線)
   - ■ 於甲端，要做下列設定：
     - ◆ 在【進階功能】>【證書管理】>【本地 CA 憑證】頁面中，【下載】所自訂的 CA 憑證 CA_Certificate。（如圖 20-18）
     - ◆ 在【進階功能】>【證書管理】>【授權憑證】頁面中，【下載】所自訂的授權憑證 Signed_Certificate_1（PEM 編碼格式）。（如圖 20-19）
     - ◆ 在【進階功能】>【證書管理】>【授權憑證】頁面中，【下載】所自訂的授權憑證 Signed_Certificate_2（PEM 編碼格式）。（如圖 20-20）
     - ◆ 在【進階功能】>【證書管理】>【授權憑證】頁面中，【刪除】所自訂的授權憑證 Signed_Certificate_2。（如圖 20-21）
     - ◆ 在【進階功能】>【證書管理】>【授權憑證】頁面中，【匯入】所備份的 Signed_Certificate_2 憑證（PEM 編碼格式）。（如圖 20-22, 圖 20-23）

- ◆ 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，【CA 憑證】選擇 CA_Certificate、【本地授權憑證】選擇 Signed_Certificate_1、【遠端授權憑證】選擇 Signed_Certificate_2。**（如圖 20-24）**

■ 於乙端，要做下列設定：

- ◆ 在【進階功能】>【證書管理】>【遠端 CA 憑證】頁面中，【匯入】自甲端備份的 CA_Certificate 憑證。**（如圖 20-25，圖 20-26）**
- ◆ 在【進階功能】>【證書管理】>【授權憑證】頁面中，【新增】Signed_Certificate_2 CSR。**（如圖 20-27，圖 20-28）**
- ◆ 在【進階功能】>【證書管理】>【授權憑證】頁面中，【匯入】自甲端備份的 Signed_Certificate_2 憑證（PEM 編碼格式）。**（如圖 20-29，圖 20-30）**
- ◆ 在【進階功能】>【證書管理】>【授權憑證】頁面中，【匯入】自甲端備份的 Signed_Certificate_1 憑證（PEM 編碼格式）。**（如圖 20-31，圖 20-32）**
- ◆ 在【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，【CA 憑證】選擇 CA_Certificate、【本地授權憑證】選擇 Signed_Certificate_2、【遠端授權憑證】選擇 Signed_Certificate_1。**（如圖 20-33）**

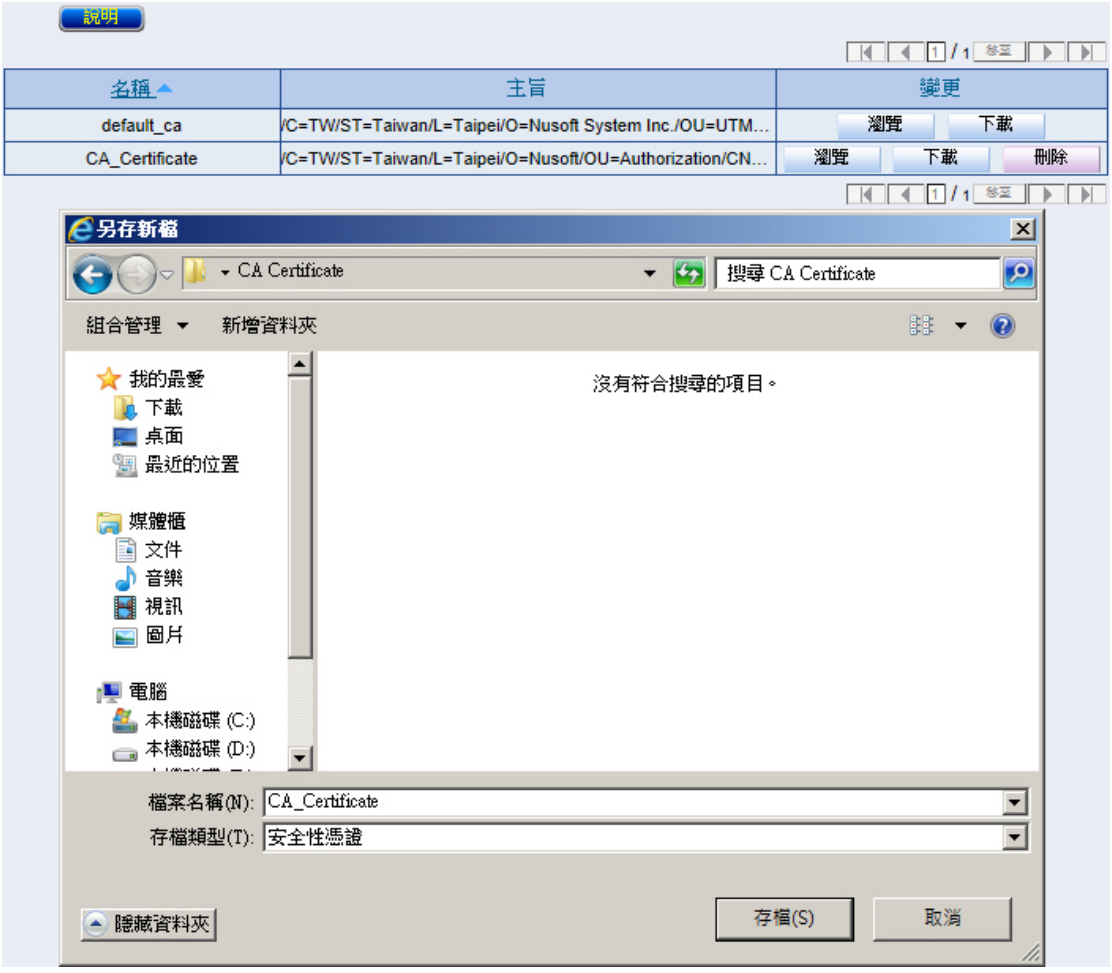


圖 20-18 下載本地 CA 憑證

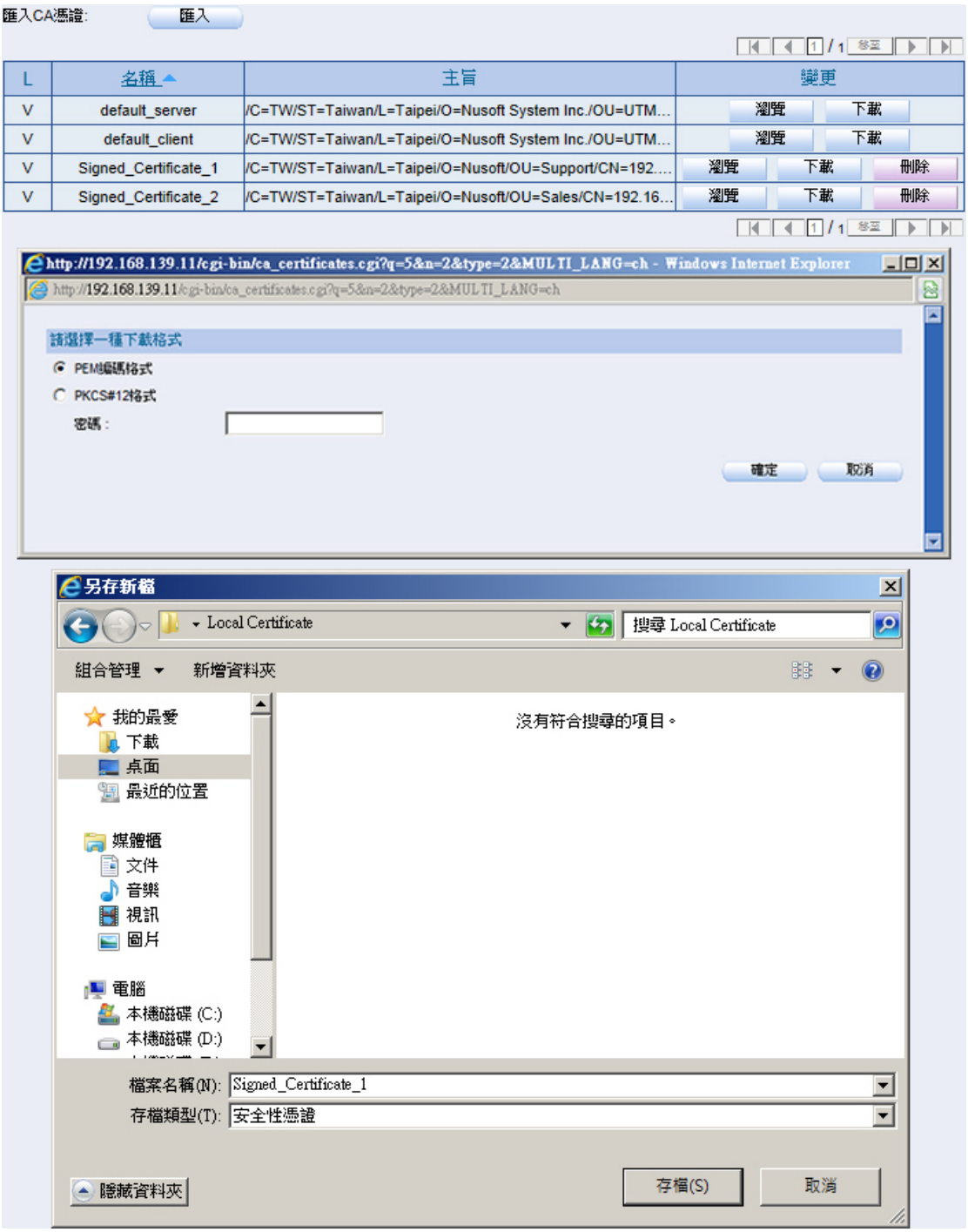


圖 20-19 下載第一筆授權憑證

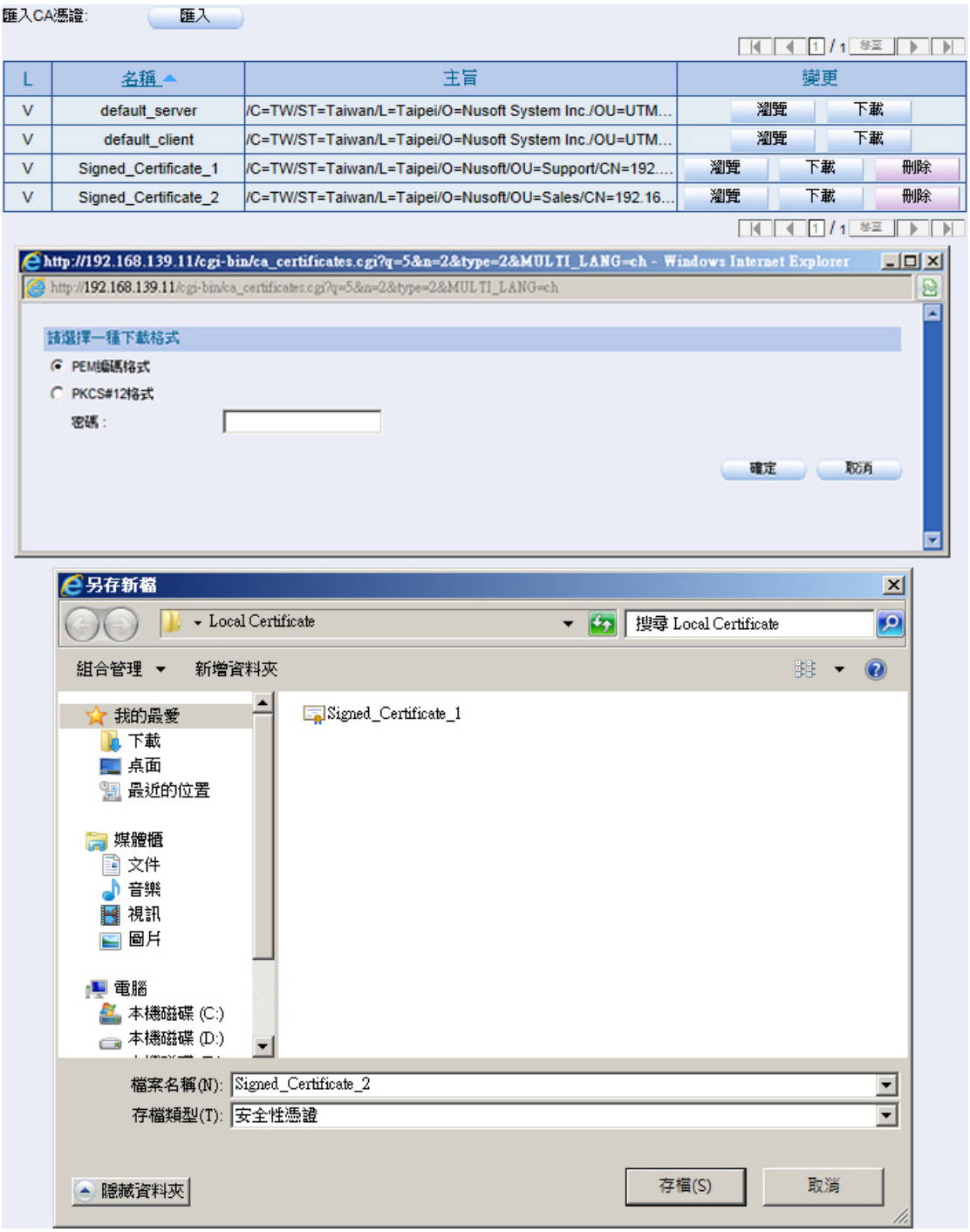


圖 20-20 下載第二筆授權憑證

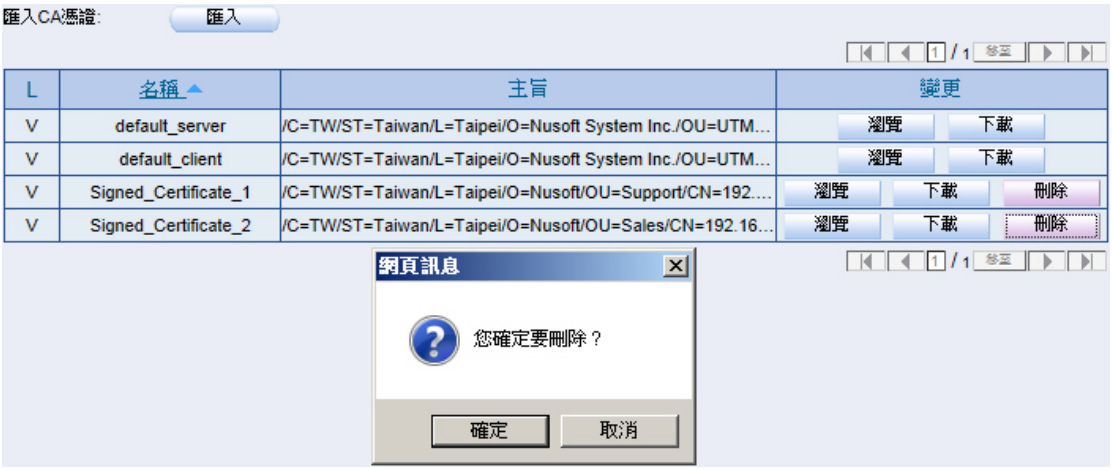


圖 20-21 刪除第二筆授權憑證

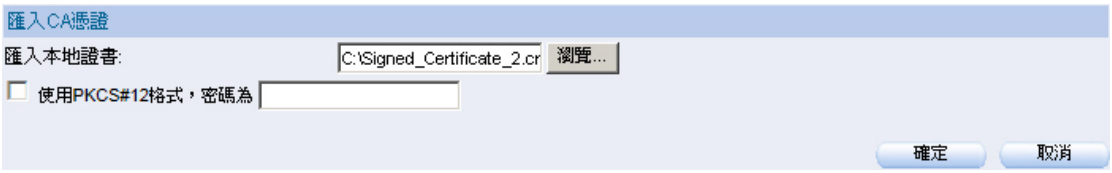


圖 20-22 匯入備份的第二筆授權憑證

圖 20-23 完成備份的第二筆授權憑證匯入

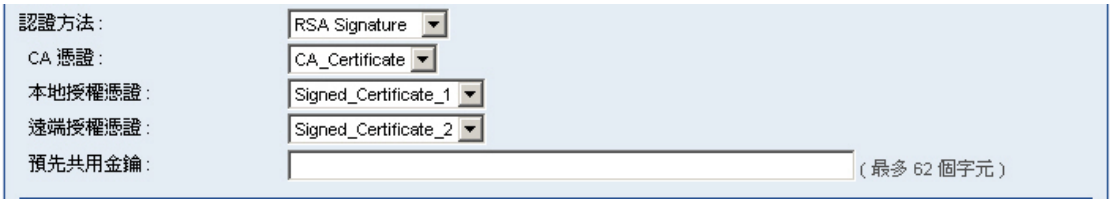


圖 20-24 將建置的憑證套用至 IPSec VPN

圖 20-25 匯入甲端 CA 憑證

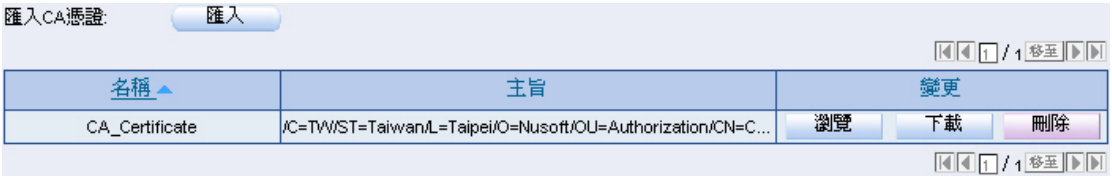


圖 20-26 完成甲端 CA 憑證匯入

圖 20-27 設定 CSR

圖 20-28 完成 CSR 設定

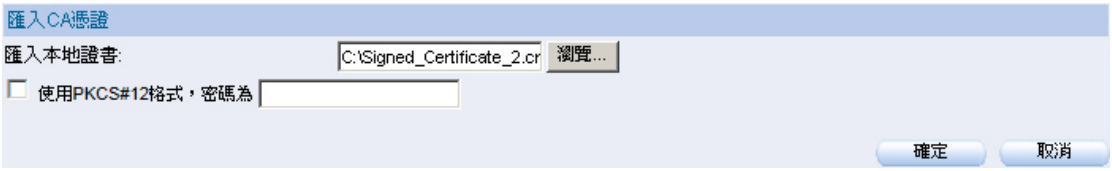


圖 20-29 匯入甲端備份的第二筆授權憑證

圖 20-30 完成甲端備份的第二筆授權憑證匯入

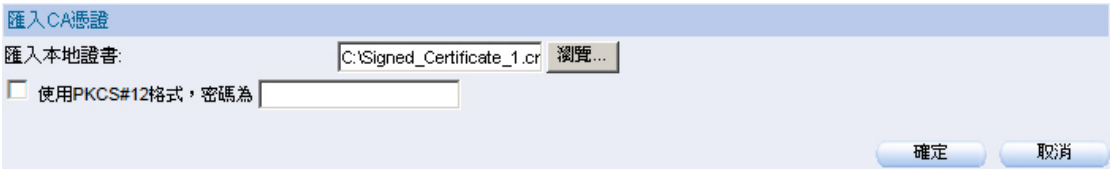


圖 20-31 匯入甲端備份的第一筆授權憑證

圖 20-32 完成甲端備份的第一筆授權憑證匯入

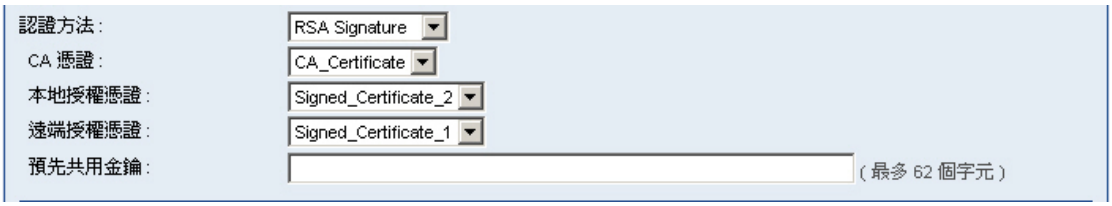


圖 20-33 將建置的憑證套用至 IPSec VPN

3. 下載自訂的【進階功能】>【證書管理】>【本地 CA 憑證】並將其匯入網頁瀏覽器（以 IE 為例，做相關說明）後，當連線 SSL Web VPN、採用加密方式連線 WebUI 時，皆可直接套用此安全憑證，不會出現安全性警告視窗。

- 在【工具】>【網際網路選項】視窗中，做下列設定：**（如圖 20-34）**
  - 在【網際網路選項】>【內容】視窗中，按下【憑證】鈕：**（如圖 20-35）**
    - 在【憑證】>【受信任的根憑證授權單位】視窗中，按下【匯入】鈕：**（如圖 20-36）**
      - 在【憑證匯入精靈】視窗中：
        - 按【下一步】鈕。**（如圖 20-37）**
        - 【檔案名稱】輸入自訂 CA 憑證的儲存路徑。
        - 按【下一步】鈕。**（如圖 20-38）**
        - 選擇指定【憑證存放區】。
        - 按【下一步】鈕。**（如圖 20-39）**
        - 按下【完成】鈕，完成設定。**（如圖 20-40）**
      - 在【安全性警告】視窗中，按下【是】鈕。**（如圖 20-41）**
      - 在確認視窗中，【確定】CA 憑證匯入成功。**（如圖 20-42）**

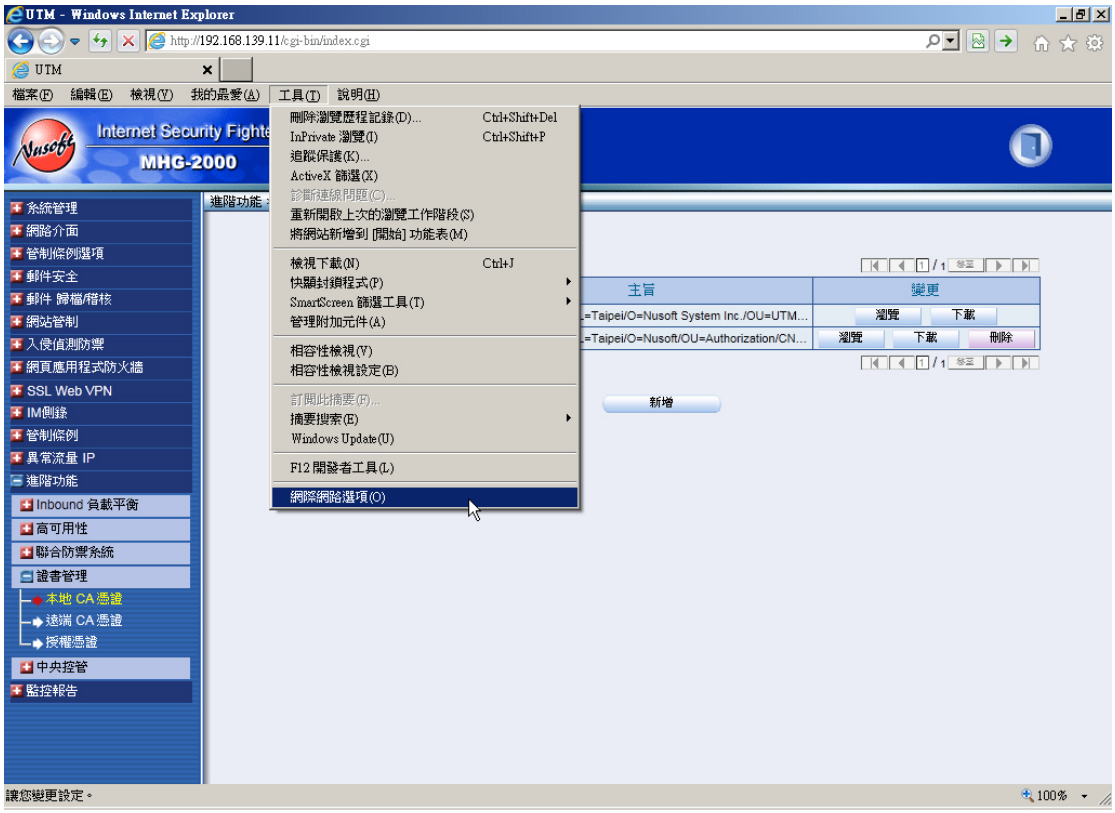


圖 20-34 開啟網際網路選項視窗

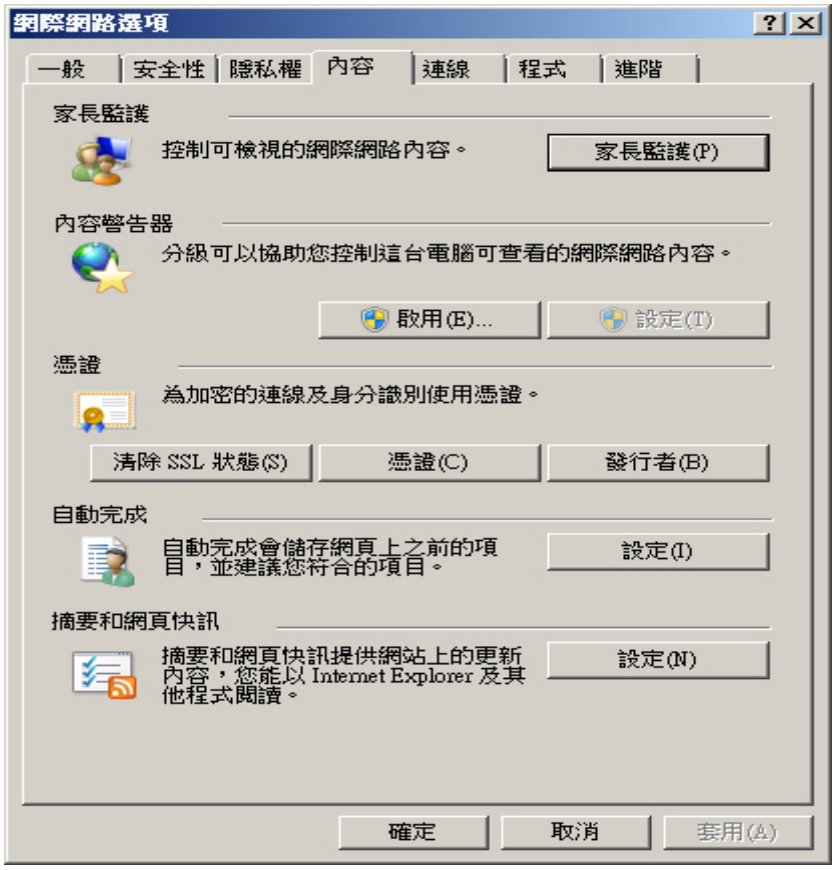


圖 20-35 開啟憑證視窗

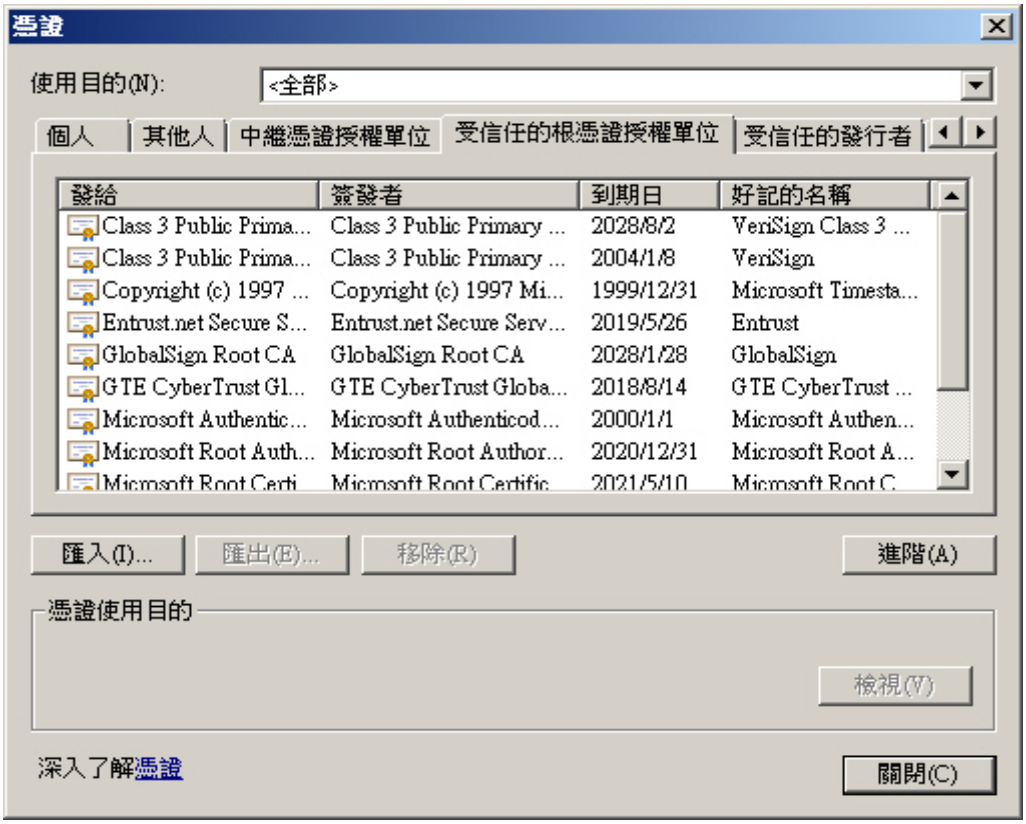


圖 20-36 開啟憑證匯入精靈視窗

圖 20-37 憑證匯入精靈歡迎訊息

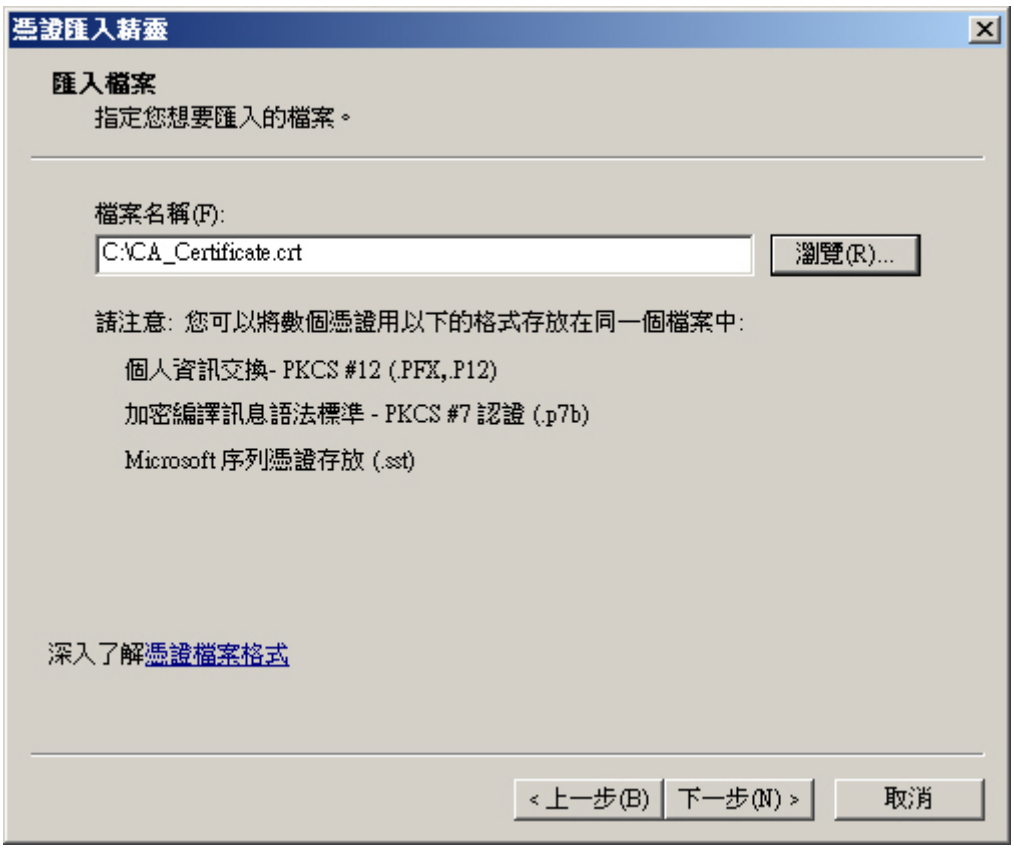


圖 20-38 匯入檔案設定

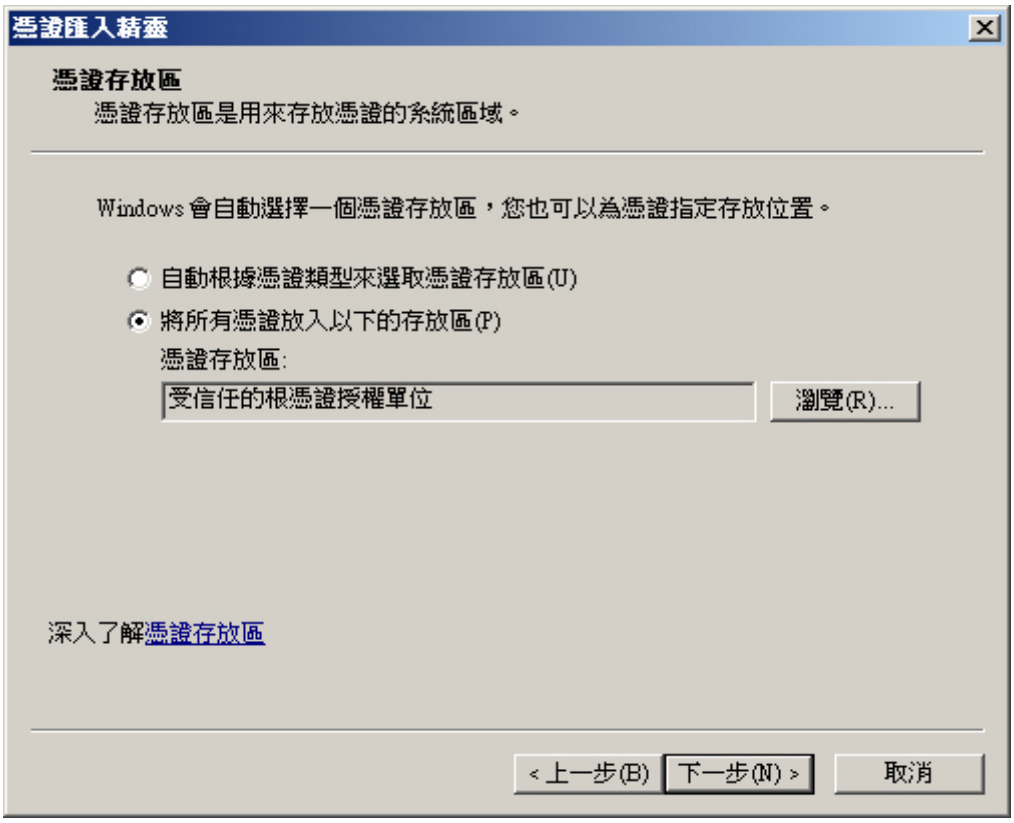


圖 20-39 憑證存放區設定

圖 20-40 完成憑證匯入設定

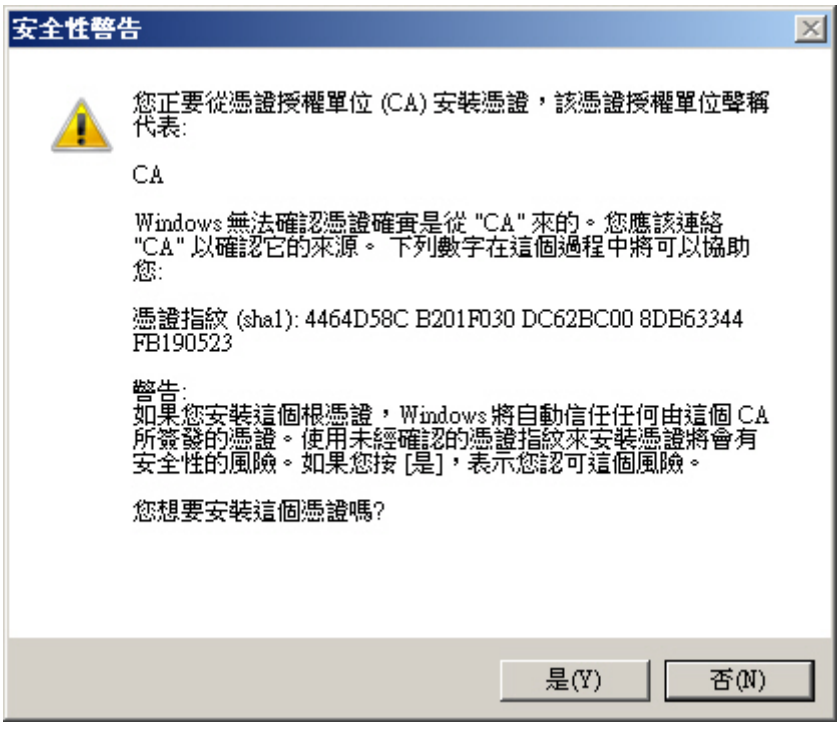


圖 20-41 安全性警告視窗

圖 20-42 憑證匯入確認視窗

第21章　中央控管

用來連線遠端集中管理設備，並透過該設備記錄系統運作所產生的報表，和直接維護系統設定。

【設定】功能概述：

中央控管設定 說明如下：

- 用來連線指定的遠端集中管理設備，並透過該設備直接維護系統設定。

本機記錄傳送至 CMS 設定 說明如下：

- 用來將系統運作所產生的網站管制報告、封包記錄、事件記錄、連線記錄、應用程式管制記錄、連線數限制記錄、傳輸量限制記錄傳送到指定的遠端集中管理設備儲存、瀏覽。

21.1 中央控管功能使用範例

21.1.1 連線新軟 CMS 主機，以遠端集中管理、監控 MHG-2000

步驟1. 在【進階功能】>【中央控管】>【設定】頁面中，做下列設定：（如圖 21-1）

- 勾選【啟動中央控管伺服器】。
- 【中央控管伺服器 IP 位址】輸入指定 CMS IP 位址。
- 【中央控管連線埠號】輸入指定 CMS 連線埠號。（預設為 11235）
- 勾選【啟動網站管制報告】、【啟動封包記錄】、【啟動事件記錄】、【啟動連線記錄】、【啟動應用程式管制記錄】、【啟動連線數限制記錄】、【啟動傳輸量限制記錄】。
- 按下【確定】鈕，完成設定。

圖 21-1 中央控管設定頁面

步驟2. 新軟 CMS 主機偵測到來自 MHG-2000 的連線時，會自動顯示其狀態資訊。（如圖 21-2）

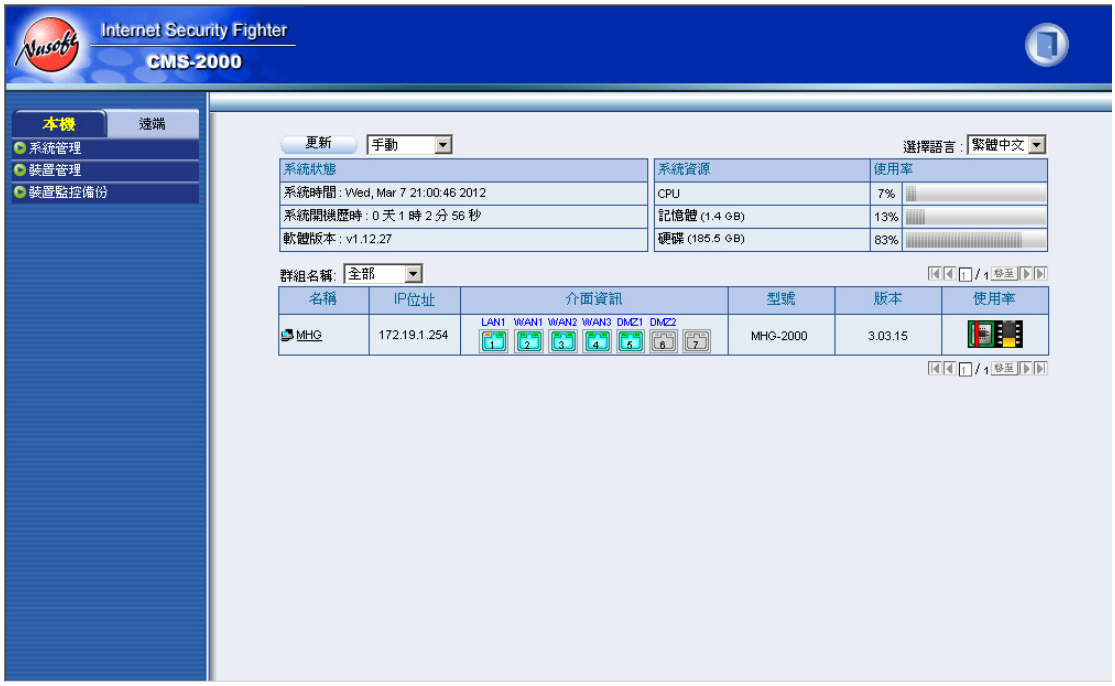


圖 21-2 新軟 CMS 連線控管設備清單

步驟3. 用新軟 CMS 檢視 MHG-2000 傳送過來並儲存的報表。**（如圖 21-3, 圖 21-4, 圖 21-5, 圖 21-6, 圖 21-7, 圖 21-8, 圖 21-9）**

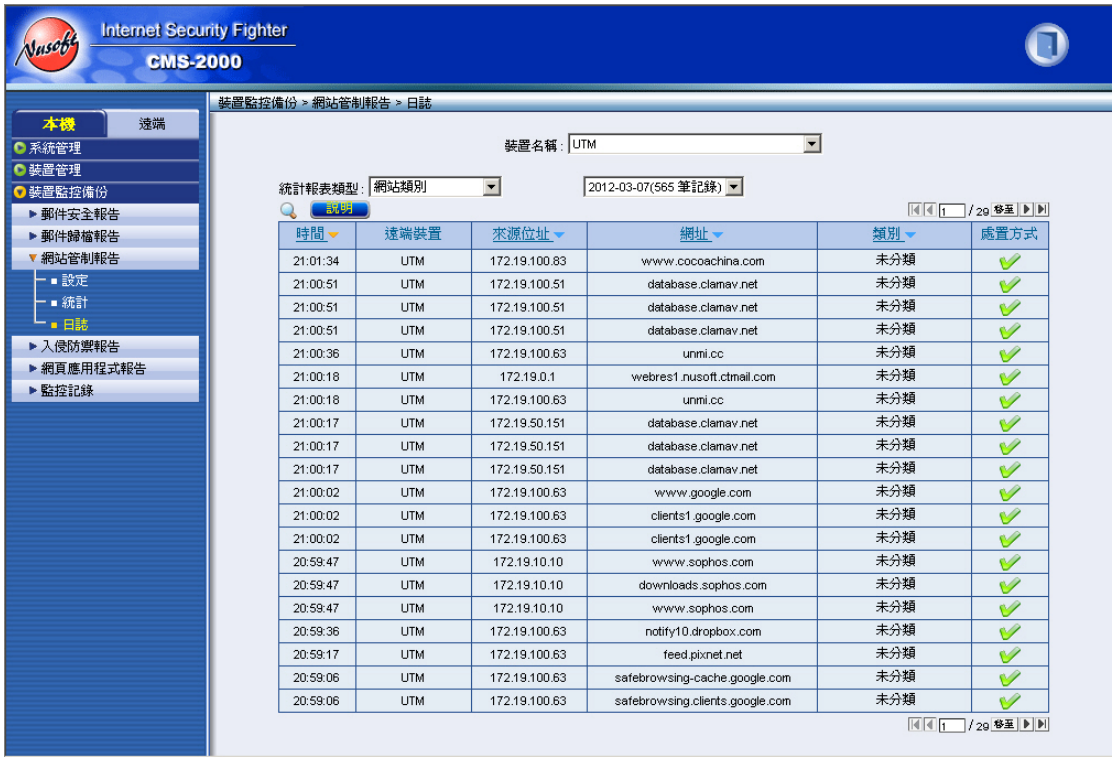


圖 21-3 檢視新軟 CMS 儲存的 MHG-2000 網站管制報告

圖 21-4 檢視新軟 CMS 儲存的 MHG-2000 封包記錄

圖 21-5 檢視新軟 CMS 儲存的 MHG-2000 事件記錄

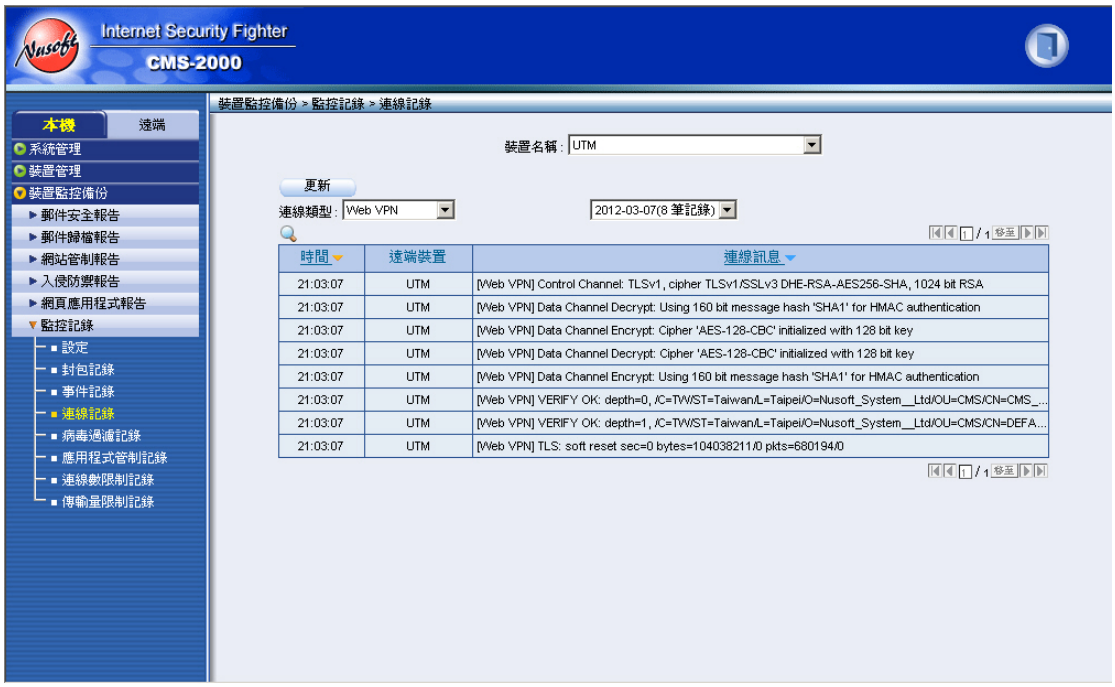


圖 21-6 檢視新軟 CMS 儲存的 MHG-2000 連線記錄

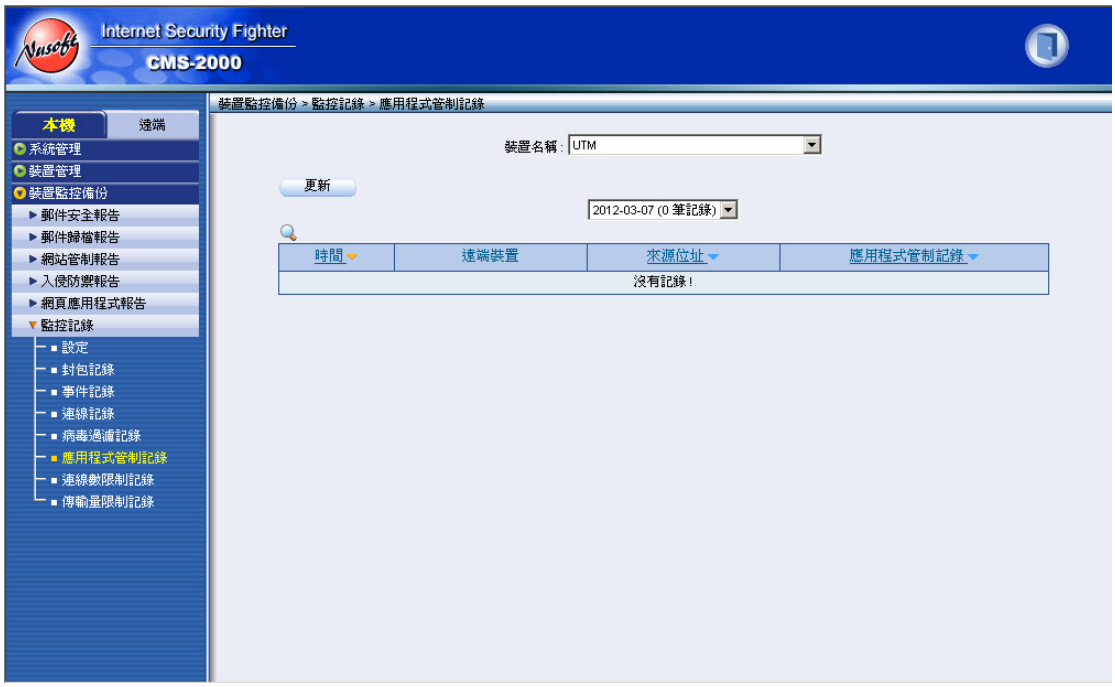


圖 21-7 檢視新軟 CMS 儲存的 MHG-2000 應用程式管制記錄

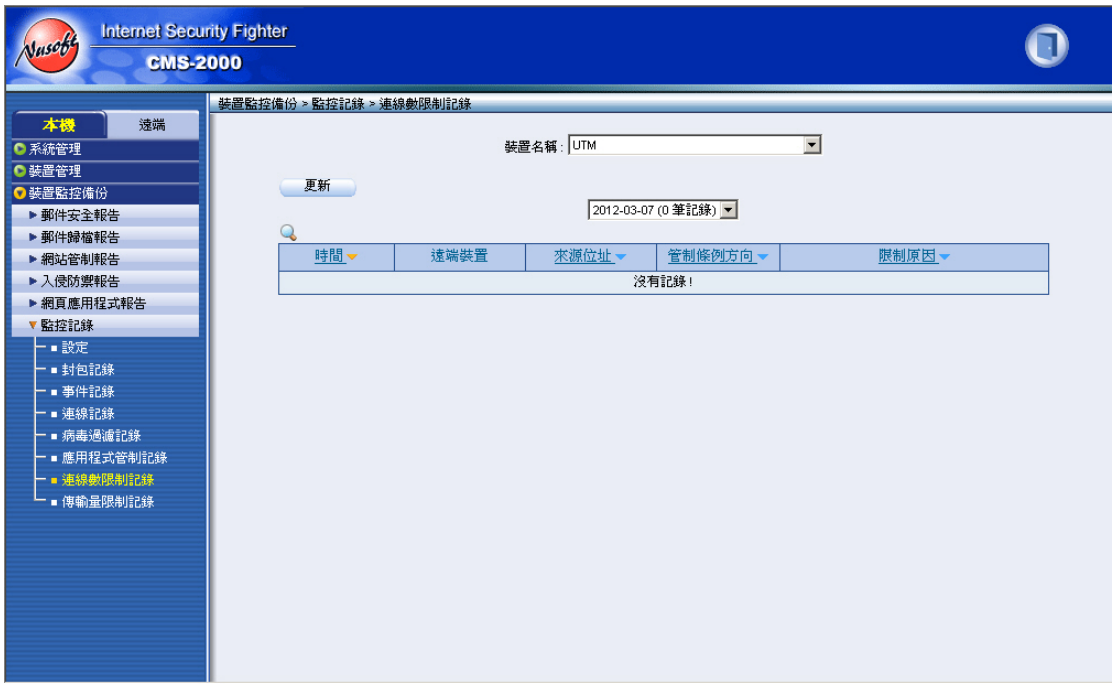


圖 21-8 檢視新軟 CMS 儲存的 MHG-2000 連線數限制記錄

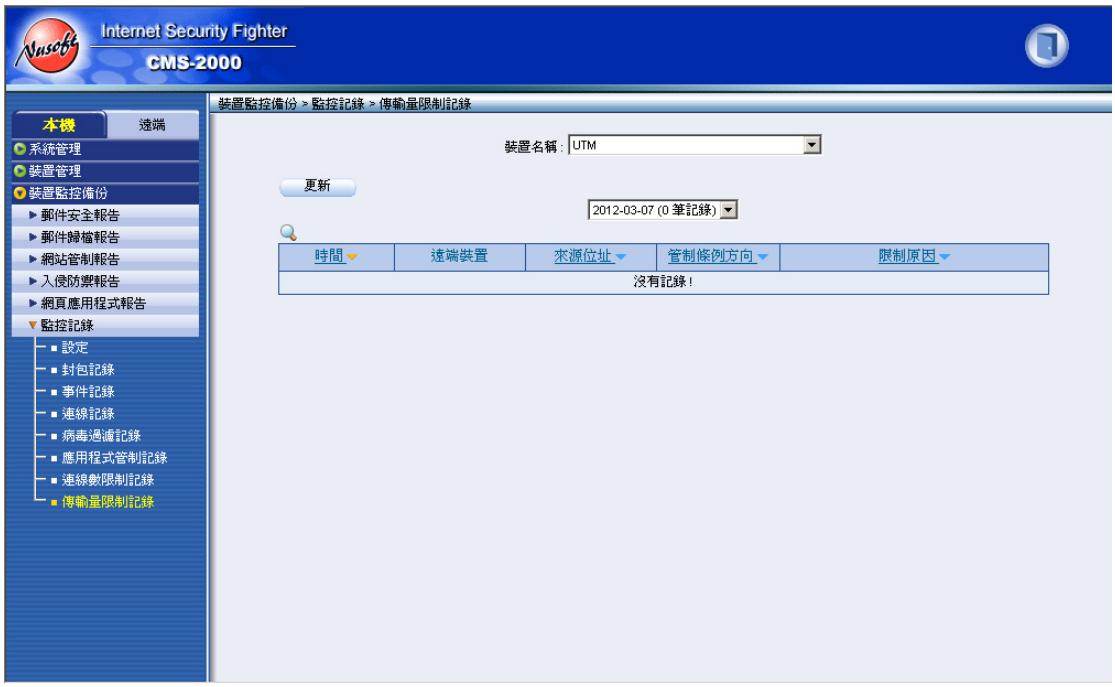


圖 21-9 檢視新軟 CMS 儲存的 MHG-2000 傳輸量限制記錄

步驟4. 用新軟 CMS 管理 MHG-2000 系統設定。（如圖 21-10）

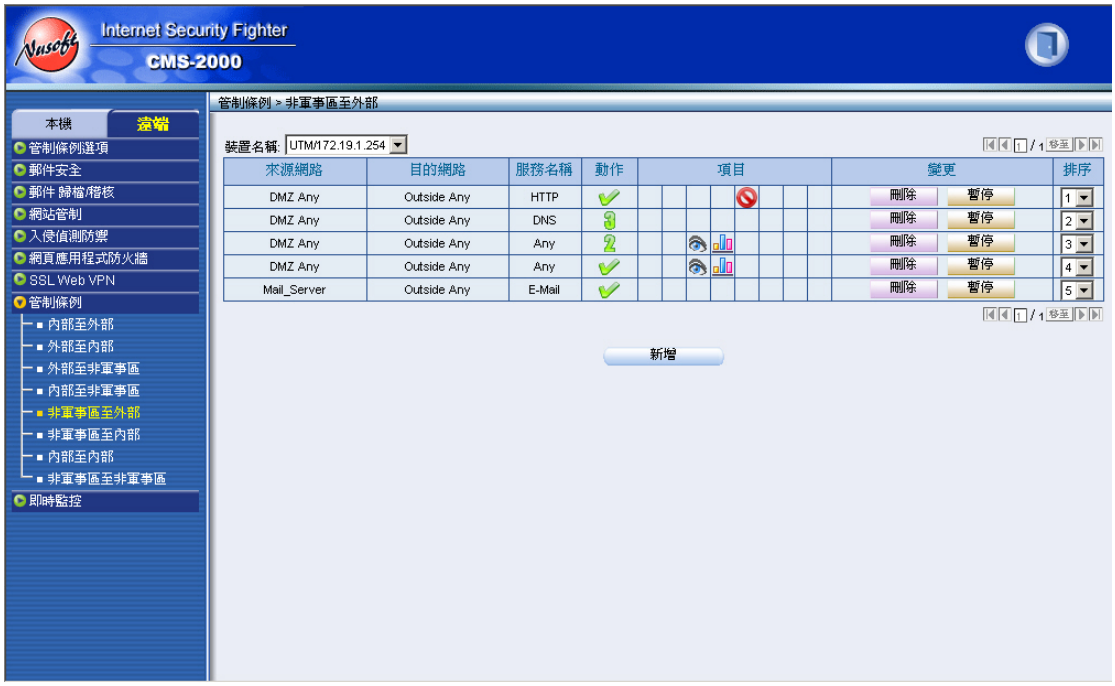


圖 21-10 透過新軟 CMS 管理 MHG-2000 系統設定

監控報告

第22章　監控記錄

用來保存和顯示 MHG-2000 的封包記錄、事件記錄、連線記錄、應用程式管制記錄、連線數限制記錄、傳輸量限制記錄報表。可由系統自動發送電子郵件告知管理員監控訊息，亦可即時備份 MHG-2000 的監控記錄至遠端主機。

- 【封包記錄】：可在制定【管制條例】時啟用，會詳細記錄通過管制條例傳送的封包資訊。
- 【事件記錄】：MHG-2000 系統運作、登入、組態參數值（System Configurations）更改…記錄。
- 【連線記錄】：記錄 MHG-2000 的 VPN、PPPoE、…連線資訊；若連線發生問題時，系統管理員可憑藉此資訊，了解問題的所在。
- 【應用程式管制記錄】：記錄被 MHG-2000 阻擋的應用程式存取資訊。
- 【連線數限制記錄】：記錄達到 MHG-2000 管制條例連線數限制的資訊。
- 【傳輸量限制記錄】：記錄達到 MHG-2000 管制條例傳輸量限制的資訊。

【設定】功能概述：

監控記錄設定 說明如下：

- 監控記錄每達 300 Kbytes，MHG-2000 就可將其郵寄給指定的收件者。
- 可將監控記錄傳送至指定的遠端記錄主機、安裝 RSS 收訊軟體或 SNMP Trap 用戶端軟體之電腦。
- 封包、事件、連線、應用程式管制、連線數限制和傳輸量限制監控記錄設定：
  - 可分別啟動電子郵件報告、Syslog 遠端記錄、SNMP Trap 警訊通知、RSS feeds 功能。

【封包記錄】功能概述：

搜尋 說明如下：

- 可依照日期、管制條例方向、排序、來源位址、目的位址和目的埠號等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【監控記錄】>【封包記錄】的【搜尋】頁面中，做下列設定：
    - 開啟並設定搜尋指定時間區間內的記錄。
    - 選擇指定【管制條例方向】、【排序】。
    - 按下【搜尋】鈕。（如圖 22-1）
    - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 22-2）

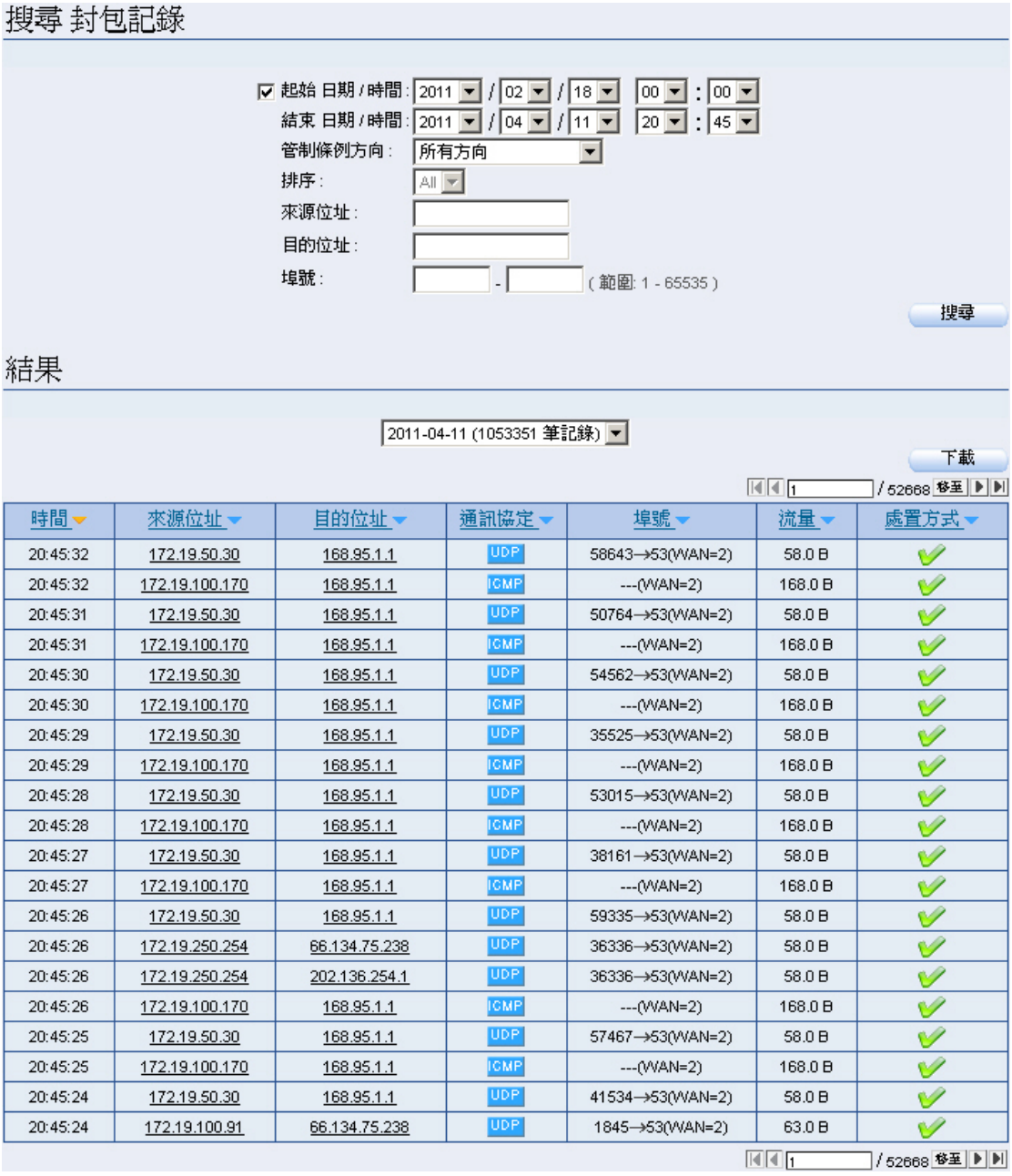
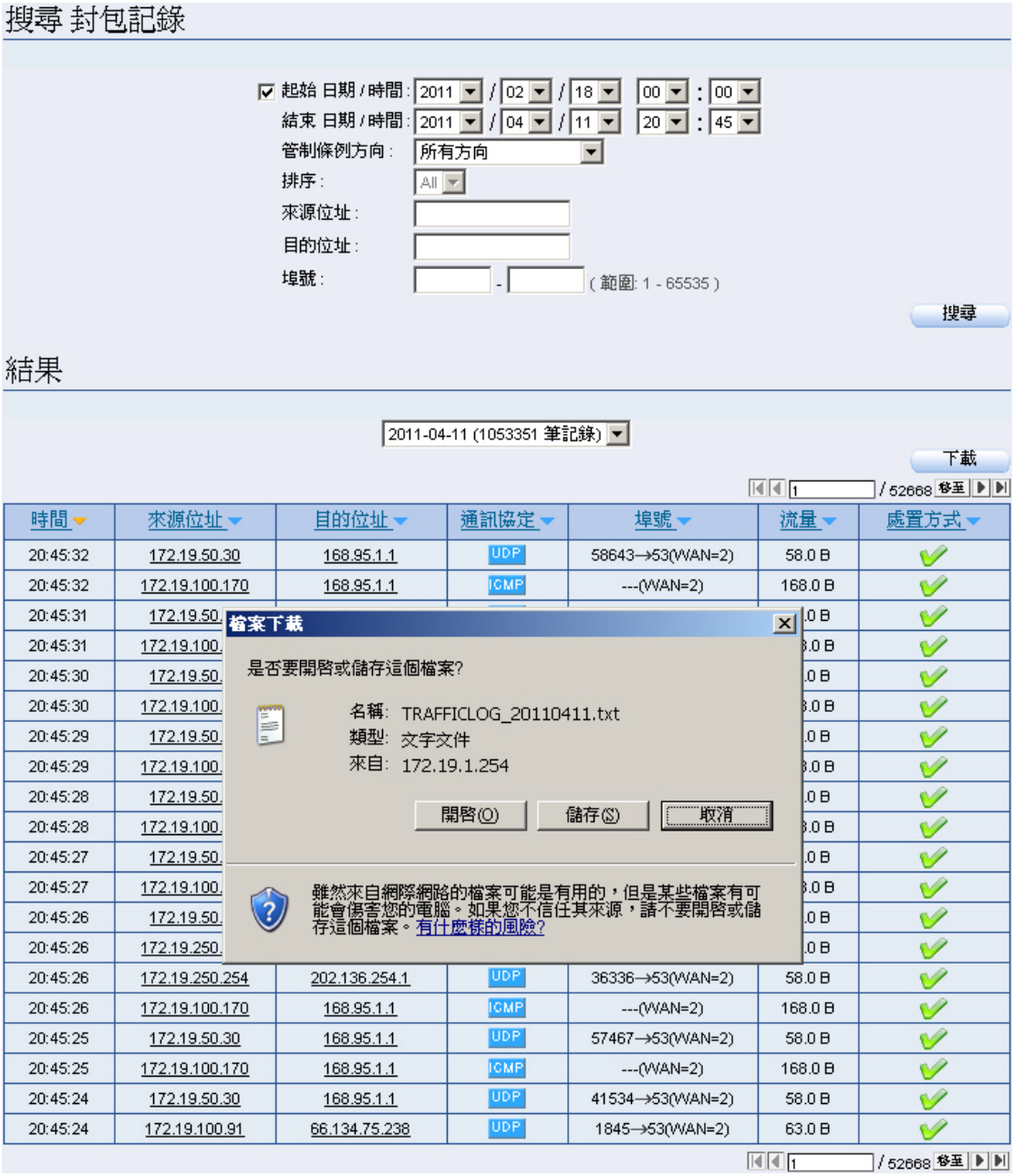

搜尋 封包記錄
起始 日期 / 時間 : 2011 / 02 / 18 00 : 00
結束 日期 / 時間 : 2011 / 04 / 11 20 : 45
管制條例方向 : 所有方向
排序 : All
來源位址 :
目的位址 :
埠號 : - (範圍: 1 - 65535)
搜尋
結果
2011-04-11 (1053351 筆記錄)
下載
1 / 52668 移至
時間 來源位址 目的位址 通訊協定 埠號 流量 處置方式
20:45:32 172.19.50.30 168.95.1.1 UDP 58643→53(WAN=2) 58.0 B
20:45:32 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:31 172.19.50.30 168.95.1.1 UDP 50764→53(WAN=2) 58.0 B
20:45:31 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:30 172.19.50.30 168.95.1.1 UDP 54562→53(WAN=2) 58.0 B
20:45:30 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:29 172.19.50.30 168.95.1.1 UDP 35525→53(WAN=2) 58.0 B
20:45:29 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:28 172.19.50.30 168.95.1.1 UDP 53015→53(WAN=2) 58.0 B
20:45:28 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:27 172.19.50.30 168.95.1.1 UDP 38161→53(WAN=2) 58.0 B
20:45:27 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:26 172.19.50.30 168.95.1.1 UDP 59335→53(WAN=2) 58.0 B
20:45:26 172.19.250.254 66.134.75.238 UDP 36336→53(WAN=2) 58.0 B
20:45:26 172.19.250.254 202.136.254.1 UDP 36336→53(WAN=2) 58.0 B
20:45:26 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:25 172.19.50.30 168.95.1.1 UDP 57467→53(WAN=2) 58.0 B
20:45:25 172.19.100.170 168.95.1.1 ICMP ---(WAN=2) 168.0 B
20:45:24 172.19.50.30 168.95.1.1 UDP 41534→53(WAN=2) 58.0 B
20:45:24 172.19.100.91 66.134.75.238 UDP 1845→53(WAN=2) 63.0 B
1 / 52668 移至

圖 22-1 搜尋特定記錄



時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
20:45:32	172.19.50.30	168.95.1.1	UDP	58643→53(WAN=2)	58.0 B	
20:45:32	172.19.100.170	168.95.1.1	ICMP	---(WAN=2)	168.0 B	
20:45:31	172.19.50.				.0 B	
20:45:31	172.19.100.				.0 B	
20:45:30	172.19.50.				.0 B	
20:45:30	172.19.100.				.0 B	
20:45:29	172.19.50.				.0 B	
20:45:29	172.19.100.				.0 B	
20:45:28	172.19.50.				.0 B	
20:45:28	172.19.100.				.0 B	
20:45:27	172.19.50.				.0 B	
20:45:27	172.19.100.				.0 B	
20:45:26	172.19.50.				.0 B	
20:45:26	172.19.250.				.0 B	
20:45:26	172.19.250.254	202.136.254.1	UDP	36336→53(WAN=2)	58.0 B	
20:45:26	172.19.100.170	168.95.1.1	ICMP	---(WAN=2)	168.0 B	
20:45:25	172.19.50.30	168.95.1.1	UDP	57467→53(WAN=2)	58.0 B	
20:45:25	172.19.100.170	168.95.1.1	ICMP	---(WAN=2)	168.0 B	
20:45:24	172.19.50.30	168.95.1.1	UDP	41534→53(WAN=2)	58.0 B	
20:45:24	172.19.100.91	66.134.75.238	UDP	1845→53(WAN=2)	63.0 B	

/ 52668 移至

圖 22-2 下載搜尋的記錄

【事件記錄】功能概述：

搜尋 說明如下：

- 可依照日期、管理員名稱、IP 位址、事件類型和僅顯示有詳細內容之事件記錄等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【監控記錄】>【事件記錄】的【搜尋】頁面中，做下列設定：
    - 開啟並設定搜尋指定時間區間內的記錄。
    - 選擇指定【事件類型】。
    - 按下【搜尋】鈕。（如圖 22-3）

時間	管理員名稱	IP位址	事件	內容
17:30:56	admin	172.19.100.76	登入成功	---
17:30:55	admin	172.19.100.76	登入成功	---
16:51:21	admin	172.19.100.91	登入成功	---
16:11:10	admin	172.19.50.25	登入成功	---
15:56:14	admin	172.19.100.85	登入成功	---
15:48:46	admin	172.19.20.12	[管制條例→內部至外部] 移除	
15:34:43	admin	172.19.50.25	[管制條例→內部至外部] 移除	
15:33:49	admin	172.19.50.25	登入成功	---
15:33:48	admin	172.19.50.25	[管制條例→內部至外部] 移除	
15:33:39	admin	172.19.50.25	登入成功	---
15:26:23	admin	172.19.20.12	[管制條例→內部至外部] 修改	
15:22:47	admin	172.19.20.12	[管制條例→內部至外部] 修改	
15:22:30	admin	172.19.20.12	[管制條例→內部至外部] 修改	
15:22:03	admin	172.19.20.12	[管制條例→內部至外部] 修改	
15:21:38	admin	172.19.20.12	[管制條例→內部至外部] 排序調整	
15:21:35	admin	172.19.20.12	[管制條例→內部至外部] 新增	
15:21:08	admin	172.19.20.12	登入成功	---
15:21:06	admin	172.19.100.86	登入成功	---
15:10:12	admin	172.19.100.100	登入成功	---
15:04:53	admin	172.19.100.85	[管制條例→內部至外部] 修改	

1 / 4 移至

圖 22-3 搜尋特定記錄

【連線記錄】功能概述：

搜尋 說明如下：

- 撥號連線：可依照日期等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- 動態 IP 位址：可依照日期等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- DHCP：可依照日期等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- PPTP Server：可依照日期等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- PPTP Client：可依照日期等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- IPSec：可依照日期等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
- Web VPN：可依照日期等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【監控記錄】>【連線記錄】的【IPSec】>【搜尋】頁面中，做下列設定：
    - 開啟並設定搜尋指定時間區間內的記錄。
    - 按下【搜尋】鈕。（如圖 22-4）

搜尋 連線記錄
起始 日期 / 時間 : 2011 / 02 / 18 00 : 00
結束 日期 / 時間 : 2011 / 04 / 12 18 : 04
搜尋
結果
2011-04-12(68 recorders)
1 / 4 移至
時間
連線訊息
17:32:29 packet from 210.177.210.178:500: initial Main Mode message received on 203.69.6.19:500 but no connection has been a...
17:32:28 packet from 210.177.210.178:500: af+type of ISAKMP Oakley attribute has an unknown value: 16384
17:32:28 packet from 210.177.210.178:500: ignoring Vendor ID payload [Vid-Initial-Contact]
17:32:28 packet from 210.177.210.178:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] method set to=106
17:32:28 packet from 210.177.210.178:500: ignoring Vendor ID payload [FRAGMENTATION]
17:32:28 packet from 210.177.210.178:500: ignoring Vendor ID payload [MS NT5 ISAKMPOAKLEY 00000004]
17:32:21 packet from 210.177.210.178:500: initial Main Mode message received on 203.69.6.19:500 but no connection has been a...
17:32:21 packet from 210.177.210.178:500: af+type of ISAKMP Oakley attribute has an unknown value: 16384
17:32:21 packet from 210.177.210.178:500: ignoring Vendor ID payload [Vid-Initial-Contact]
17:32:21 packet from 210.177.210.178:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] method set to=106
17:32:21 packet from 210.177.210.178:500: ignoring Vendor ID payload [FRAGMENTATION]
17:32:21 packet from 210.177.210.178:500: ignoring Vendor ID payload [MS NT5 ISAKMPOAKLEY 00000004]
17:32:17 packet from 210.177.210.178:500: initial Main Mode message received on 203.69.6.19:500 but no connection has been a...
17:32:17 packet from 210.177.210.178:500: af+type of ISAKMP Oakley attribute has an unknown value: 16384
17:32:17 packet from 210.177.210.178:500: ignoring Vendor ID payload [Vid-Initial-Contact]
17:32:17 packet from 210.177.210.178:500: ignoring Vendor ID payload [MS NT5 ISAKMPOAKLEY 00000004]
17:32:17 packet from 210.177.210.178:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] method set to=106
17:32:17 packet from 210.177.210.178:500: ignoring Vendor ID payload [FRAGMENTATION]
17:32:15 packet from 210.177.210.178:500: initial Main Mode message received on 203.69.6.19:500 but no connection has been a...
17:32:15 packet from 210.177.210.178:500: af+type of ISAKMP Oakley attribute has an unknown value: 16384
1 / 4 移至

圖 22-4 搜尋特定記錄

【應用程式管制記錄】功能概述：

搜尋 說明如下：

- 可依照日期和來源位址等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【監控記錄】>【應用程式管制記錄】的【搜尋】頁面中，做下列設定：
    - 開啟並設定搜尋指定時間區間內的記錄。
    - 按下【搜尋】鈕。（如圖 22-5）

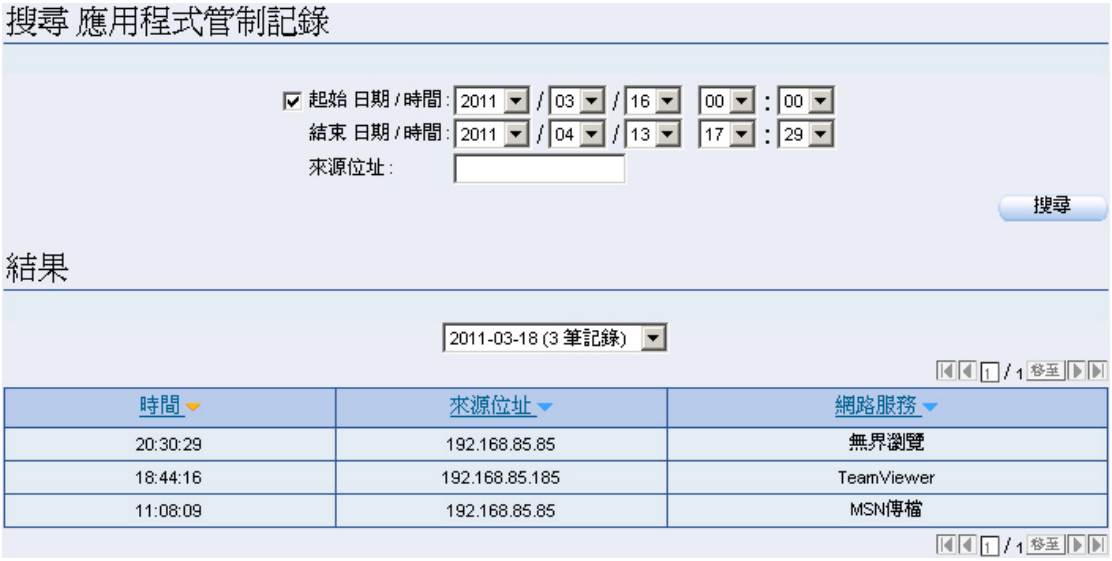


圖 22-5 搜尋特定記錄

【連線數限制記錄】功能概述：

搜尋 說明如下：

- 可依照日期和來源位址等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【監控記錄】>【連線數限制記錄】的【搜尋】頁面中，做下列設定：
    - 開啟並設定搜尋指定時間區間內的記錄。
    - 按下【搜尋】鈕。（如圖 22-6）

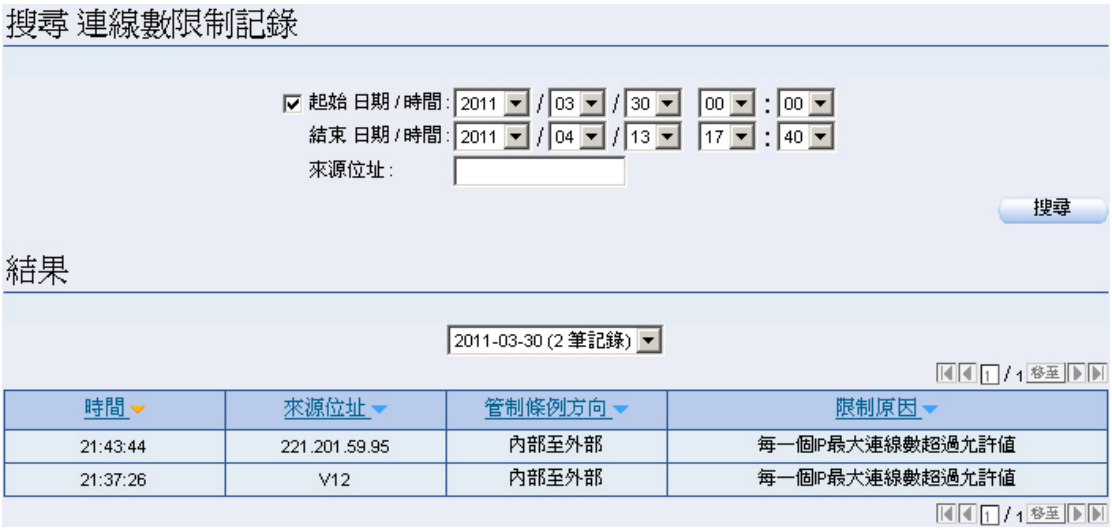


圖 22-6 搜尋特定記錄

【傳輸量限制記錄】功能概述：

搜尋 說明如下：

- 可依照日期和來源位址等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【監控記錄】>【傳輸量限制記錄】的【搜尋】頁面中，做下列設定：
    - 開啟並設定搜尋指定時間區間內的記錄。
    - 按下【搜尋】鈕。（如圖 22-7）

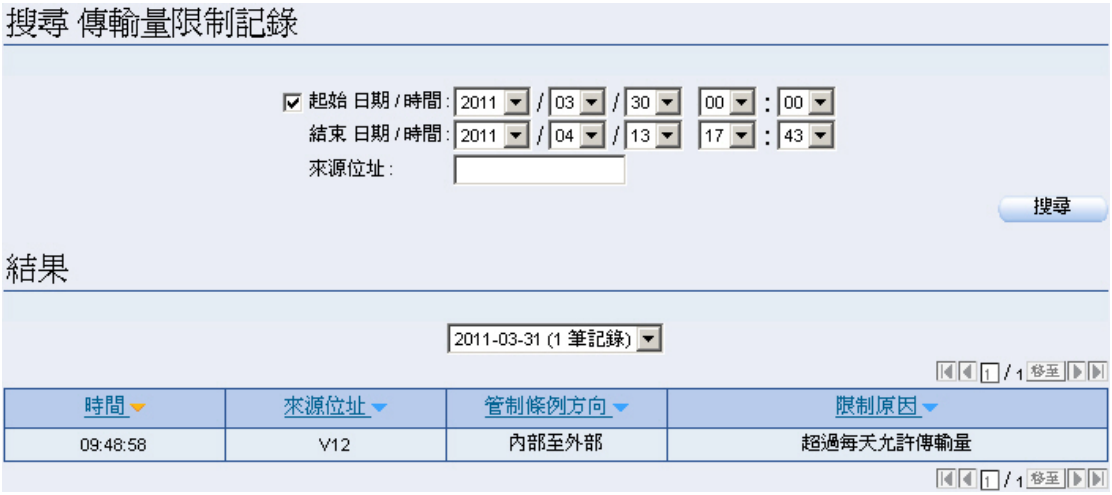


圖 22-7 搜尋特定記錄

22.1 封包記錄

22.1.1 檢視使用者透過 MHG-2000 存取內、外部網路資源，使用的協定及埠號

步驟1. 在【管制條例】>【非軍事區至外部】頁面中，做下列設定：（如圖 22-8）

- 開啟【封包記錄】。
- 按下【確定】鈕，完成設定。（如圖 22-9）

圖 22-8 管制條例啟用封包記錄

圖 22-9 完成管制條例設定

步驟2. 在【監控報告】>【監控記錄】>【封包記錄】頁面中，可顯示所有通過管制條例監控的封包記錄。（如圖 22-10）

- 點擊【來源位址】或【目的位址】連結，會彈出一視窗列出所選擇之 IP 存取網路資源時，透過之通訊協定、埠號和所使用之流量。（如圖 22-11）
- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由 MHG-2000 上清除。（如圖 22-12）

圖 22-10 封包記錄頁面

圖 22-11 封包記錄過濾視窗

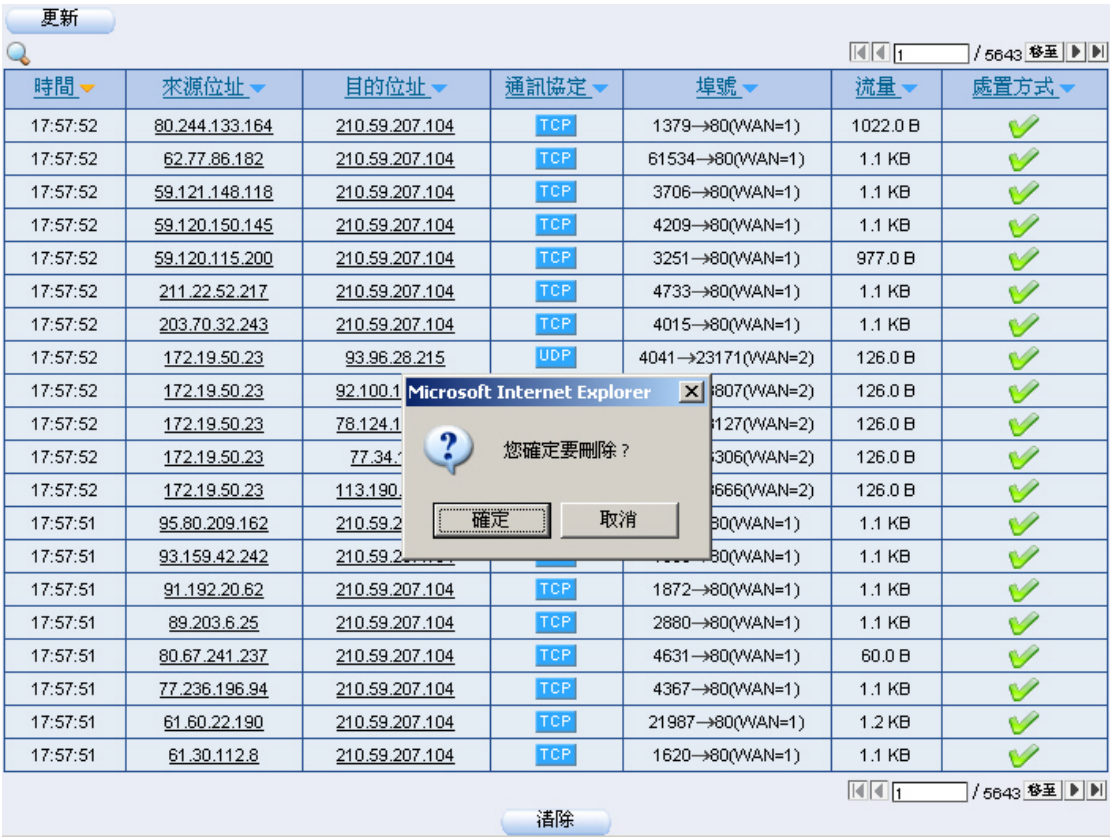


圖 22-12 清除封包記錄

22.2 事件記錄

22.2.1 檢視系統管理員登入和管理 MHG-2000，及 MHG-2000 寄送報表、外部網路介面運作之狀況

步驟1. 在【監控報告】>【監控記錄】>【事件記錄】頁面中，可顯示系統管理員登入和管理 MHG-2000 的事件記錄，及 MHG-2000 寄送報表、外部網路介面運作的狀態。（如圖 22-13）

- 按下鈕，會顯示該筆記錄的詳細訊息。（如圖 22-14）

時間	管理員名稱	IP位址	事件	內容
21:29:01	admin	220.135.197.227	[監控報告→監控記錄→封包記錄] 清除封包記錄 (日期: 2012/08/14)	---
21:28:52	system	127.0.0.1	WAN2(Port3) 連線	---
21:28:51	system	127.0.0.1	WAN2(Port3) 斷線	---
21:28:51	system	127.0.0.1	WAN1(Port2) 連線	---
21:28:49	system	127.0.0.1	WAN1(Port2) 斷線	---
21:28:48	admin	220.135.197.227	[網路介面→設定] 修改	
21:28:20	admin	220.135.197.227	登入成功	---
21:27:01	system	127.0.0.1	WAN1(Port2) 連線	---
21:27:00	system	127.0.0.1	WAN1(Port2) 斷線	---
21:27:00	system	127.0.0.1	WAN2(Port3) 連線	---
21:26:59	system	127.0.0.1	WAN2(Port3) 斷線	---
21:26:57	admin	220.135.197.227	[網路介面→設定] 修改	
21:24:21	admin	220.135.197.227	登入成功	---
21:24:21	admin	220.135.197.227	登入成功	---
21:24:20	admin	220.135.197.227	登入成功	---
21:24:20	admin	220.135.197.227	登入成功	---
21:24:20	admin	220.135.197.227	登入成功	---
21:24:20	admin	220.135.197.227	登入成功	---

圖 22-13 事件記錄

圖 22-14 事件記錄內容

22.3 連線記錄

22.3.1 檢視 MHG-2000 的系統連線記錄

步驟1. 在【監控報告】>【監控記錄】>【連線記錄】頁面中，可顯示 MHG-2000 撥號連線、動態 IP 位址、DHCP、PPTP Server、PPTP Client、IPSec、Web VPN 的連線狀況。（如圖 22-15）

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由 MHG-2000 上清除。（如圖 22-16）

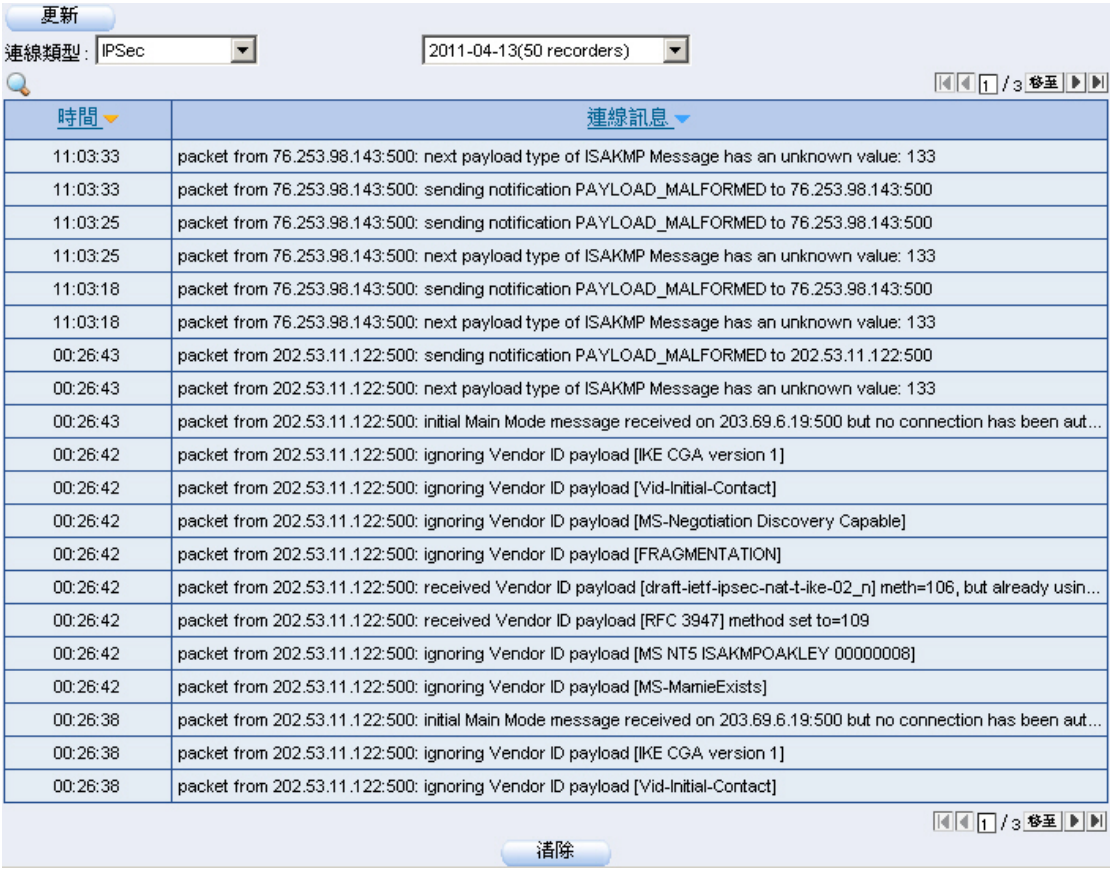


圖 22-15 連線記錄

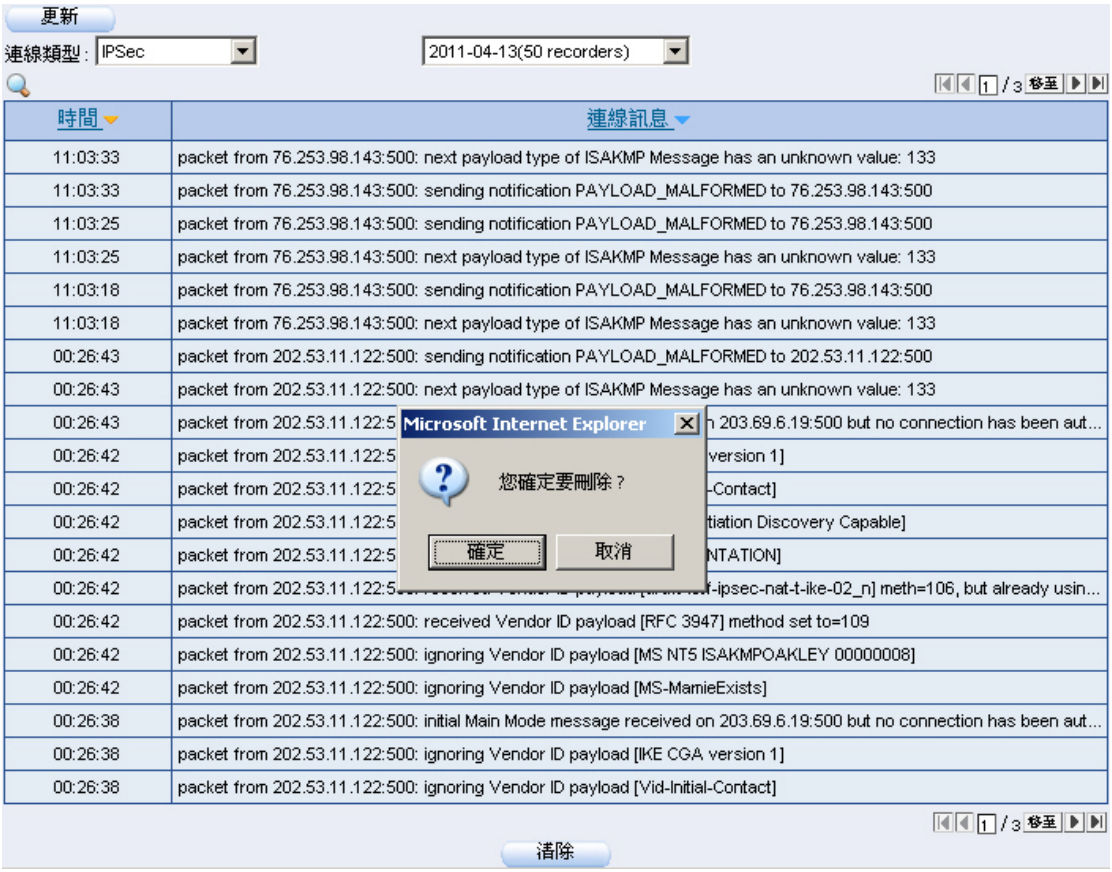


圖 22-16 清除連線記錄

22.4 應用程式管制記錄

22.4.1 檢視 MHG-2000 阻擋的應用程式存取記錄

步驟1. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 22-17）

- 選擇所設定的【應用程式管制】規則。
- 按下【確定】鈕，完成設定。（如圖 22-18）

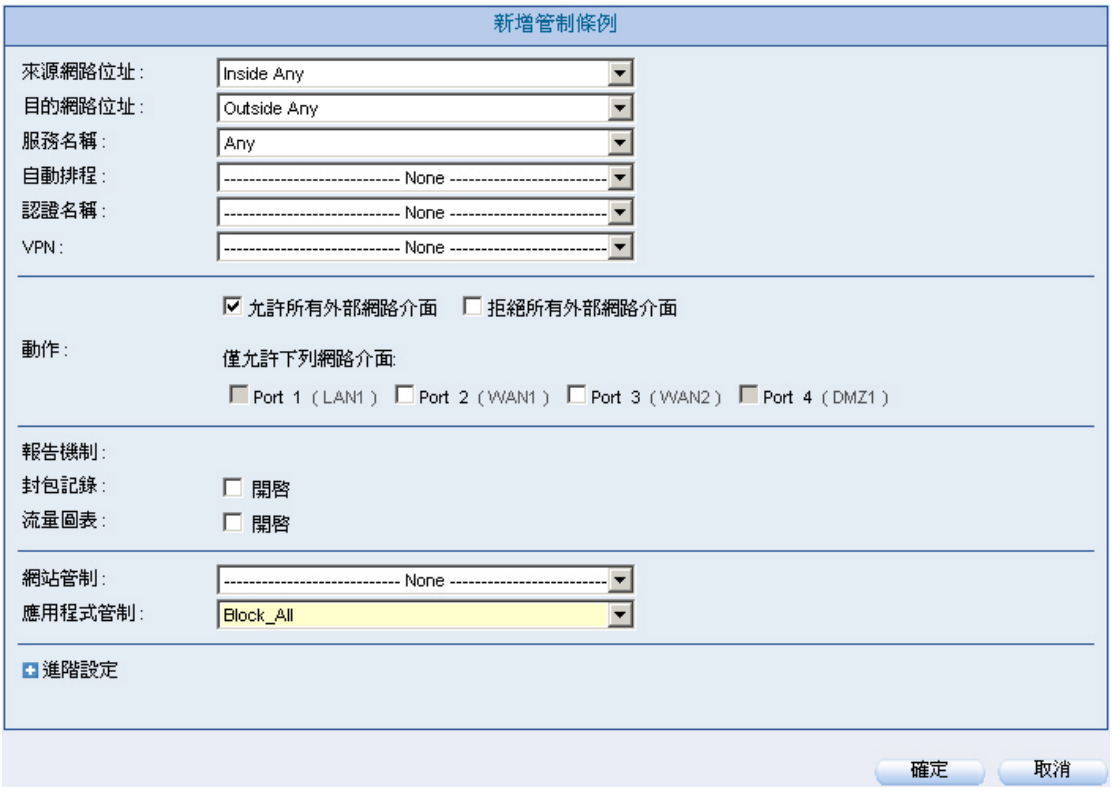


圖 22-17 管制條例套用應用程式管制規則

圖 22-18 完成管制條例設定

步驟2. 在【監控報告】>【監控記錄】>【應用程式管制記錄】頁面中，可顯示被 MHG-2000 阻擋的應用程式存取記錄。（如圖 22-19）

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由 MHG-2000 上清除。（如圖 22-20）

圖 22-19 應用程式管制記錄

圖 22-20 清除應用程式管制記錄

22.5 連線數限制記錄

22.5.1 檢視達到 MHG-2000 限制的連線數存取記錄

步驟1. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 22-21）

- 輸入指定的【每個來源 IP 最大連線數限制】。
- 按下【確定】鈕，完成設定。（如圖 22-22）

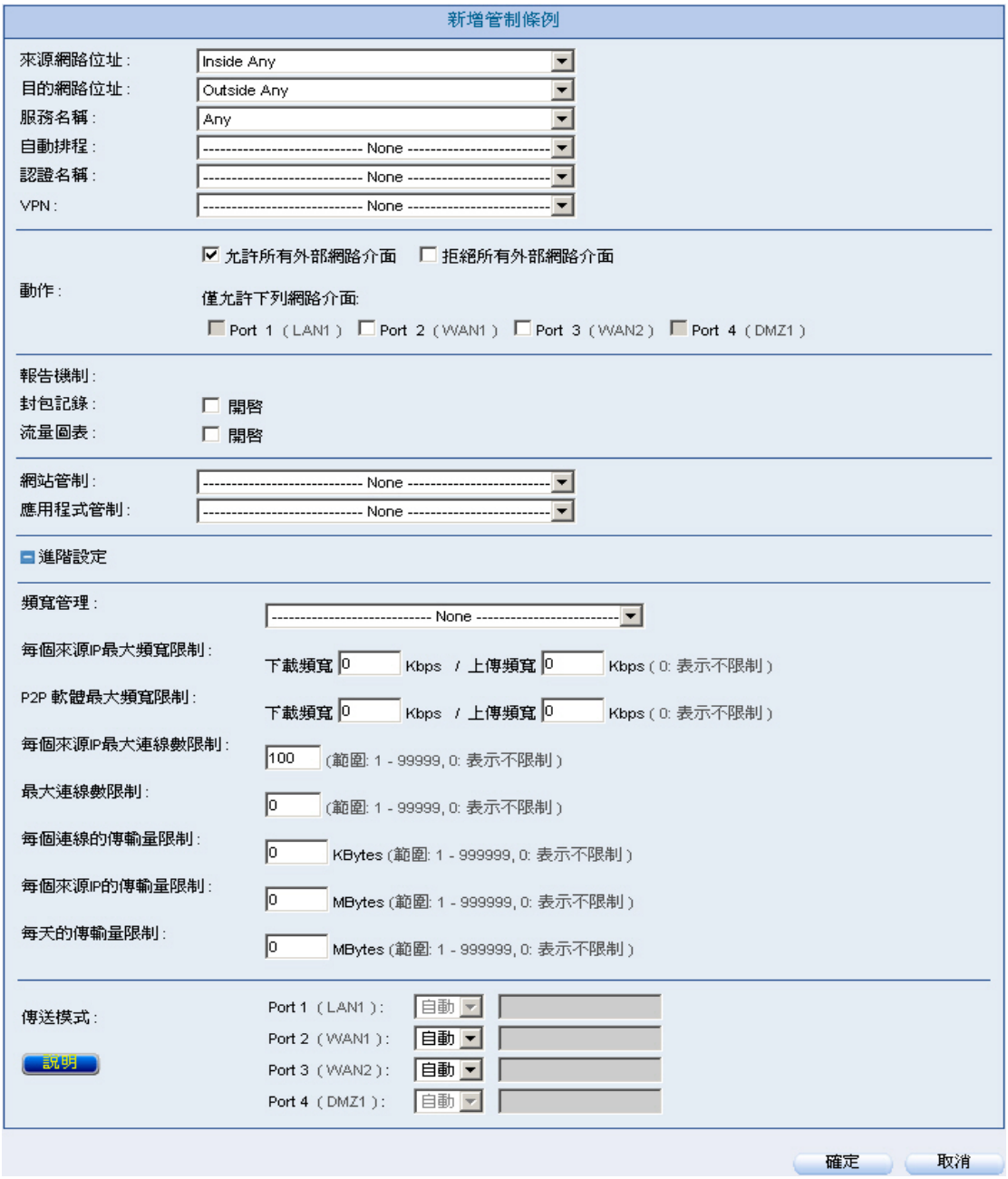


圖 22-21 設定限制連線數之管制條例

圖 22-22 完成管制條例設定

步驟2. 在【監控報告】>【監控記錄】>【連線數限制記錄】頁面中，可顯示達到 MHG-2000 限制的連線數存取記錄。（如圖 22-23）

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由 MHG-2000 上清除。（如圖 22-24）

圖 22-23 連線數限制記錄

圖 22-24 清除連線數限制記錄

22.6 傳輸量限制記錄

22.6.1 檢視達到 MHG-2000 限制的傳輸量存取記錄

步驟1. 在【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 22-25）

- 輸入指定的【每個來源 IP 的傳輸量限制】。
- 按下【確定】鈕，完成設定。（如圖 22-26）

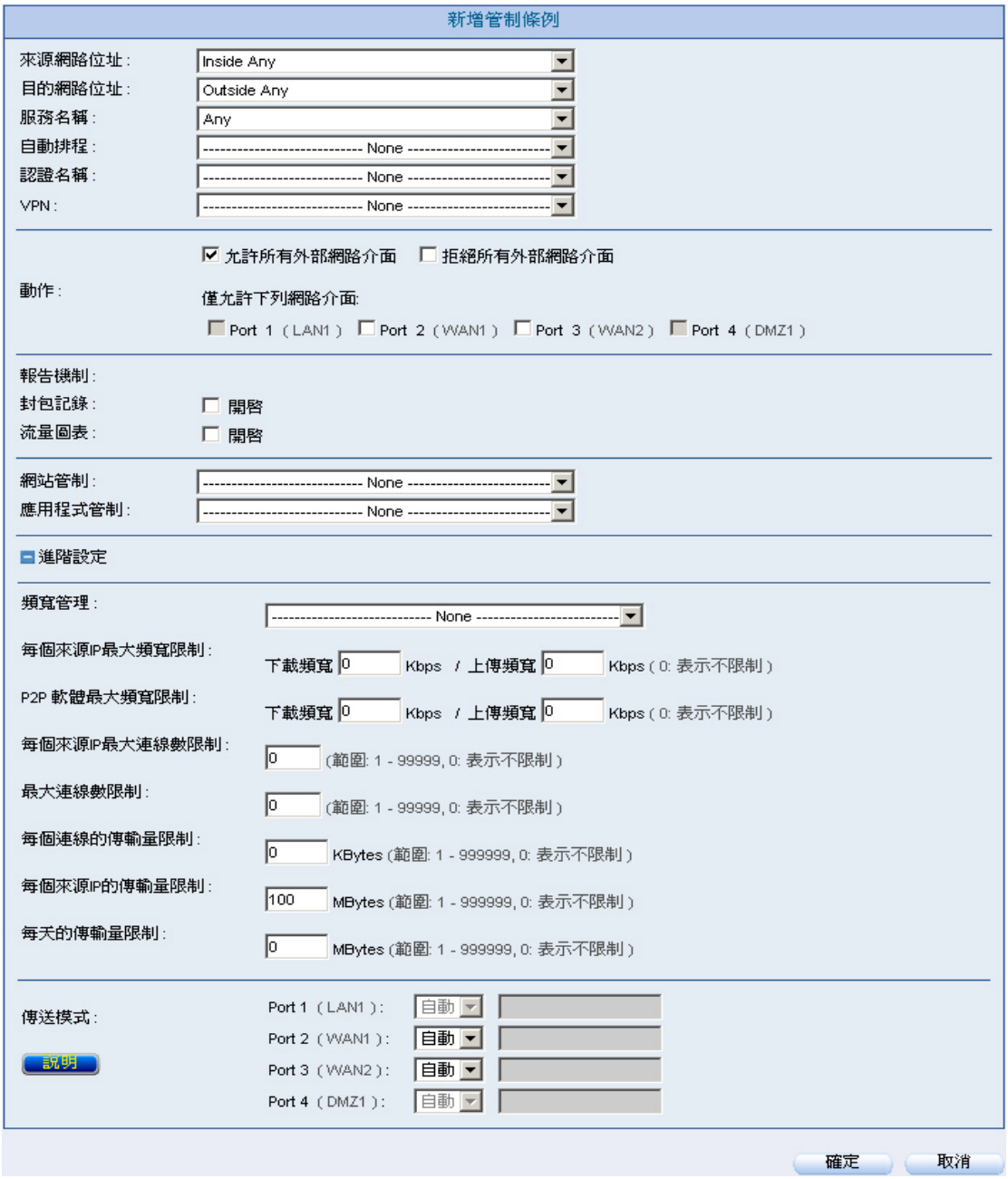


圖 22-25 設定限制傳輸量之管制條例

圖 22-26 完成管制條例設定

步驟2. 在【監控報告】>【監控記錄】>【傳輸量限制記錄】頁面中，可顯示達到 MHG-2000 限制的傳輸量存取記錄。（如圖 22-27）

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由 MHG-2000 上清除。（如圖 22-28）

圖 22-27 傳輸量限制記錄

圖 22-28 清除傳輸量限制記錄

22.7 監控備份

22.7.1 系統管理員儲存或接收由 MHG-2000 所發送出來的運作記錄

步驟1. 在【系統管理】>【組態】>【系統設定】頁面中，做下列設定：

- 啟動並進行【電子郵件警告 / 報告設定】。（如圖 22-29）
- 啟動並進行【Syslog 遠端記錄設定】。（如圖 22-30）

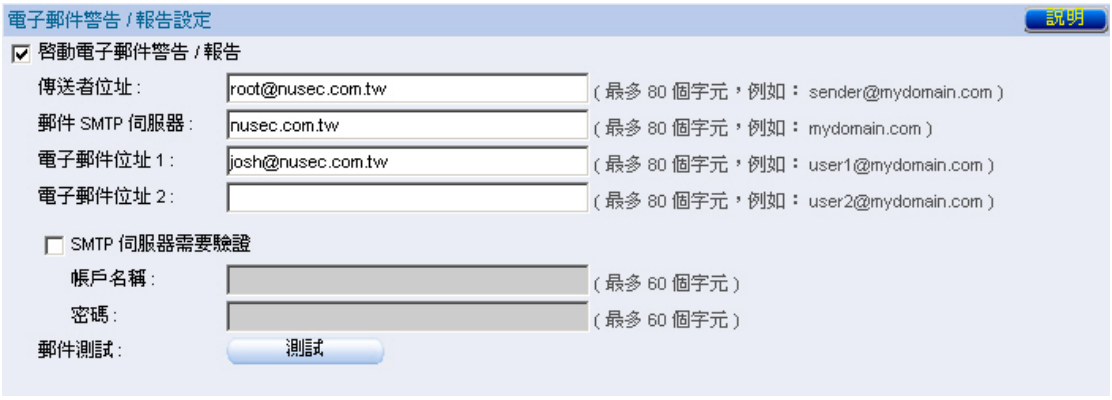


圖 22-29 開啟 MHG-2000 發送警告/報告信函功能

圖 22-30 開啟 MHG-2000 Syslog 遠端記錄功能

步驟2. 在【系統管理】>【組態】>【SNMP】頁面中，做下列設定：（如圖 22-31）

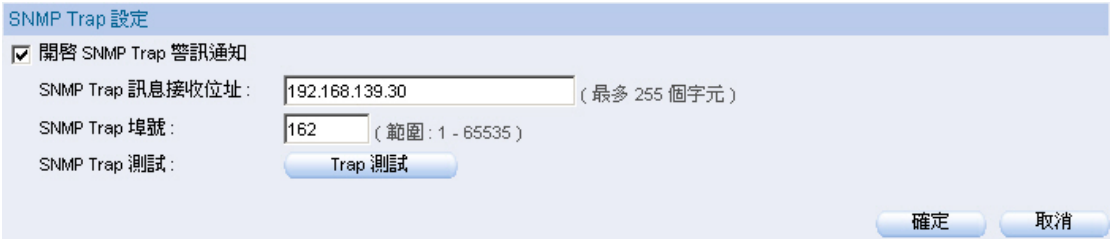


圖 22-31SNMP Trap 設定

步驟3. 在【監控報告】>【監控記錄】>【設定】頁面中，做下列設定：（如圖 22-32）

圖 22-32 監控記錄設定頁面

說明：

1. 【啟動電子郵件報告】後，每當監控記錄到達 300 Kbytes 時，會郵寄所累積的記錄資訊給系統管理員。（如圖 22-33）

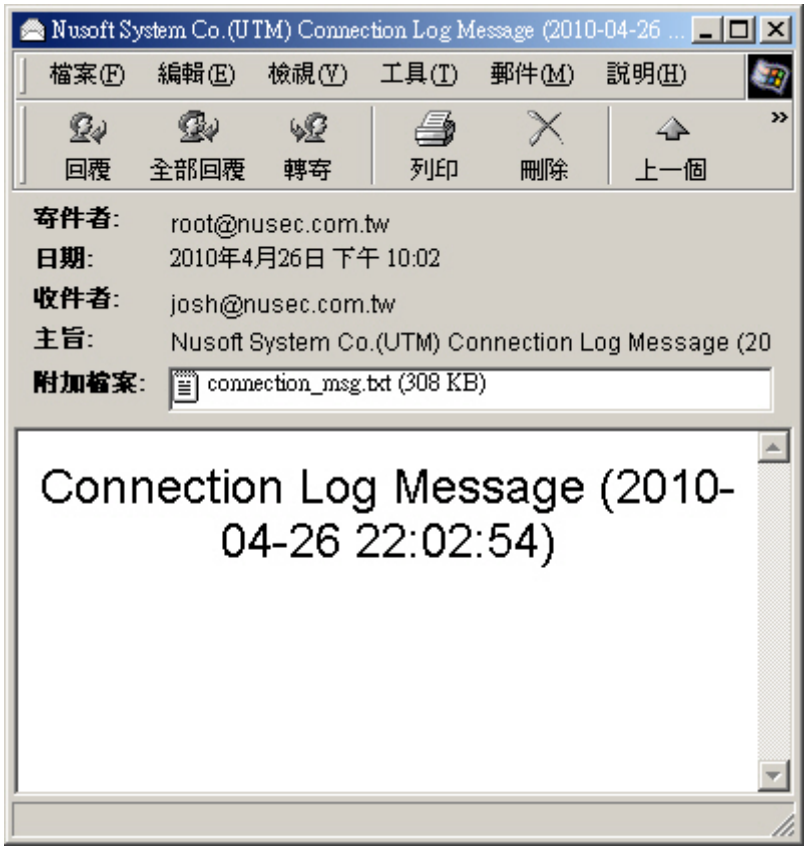


圖 22-33 郵寄監控記錄

2. 【啟動 Syslog 遠端記錄】後，會將監控記錄即時傳送至連線的指定外部記錄設備。
3. 【啟動 SNMP Trap 警訊通知】後，會將監控記錄即時傳送至指定的安裝 SNMP Trap 用戶端軟體之電腦。（如圖 22-34）

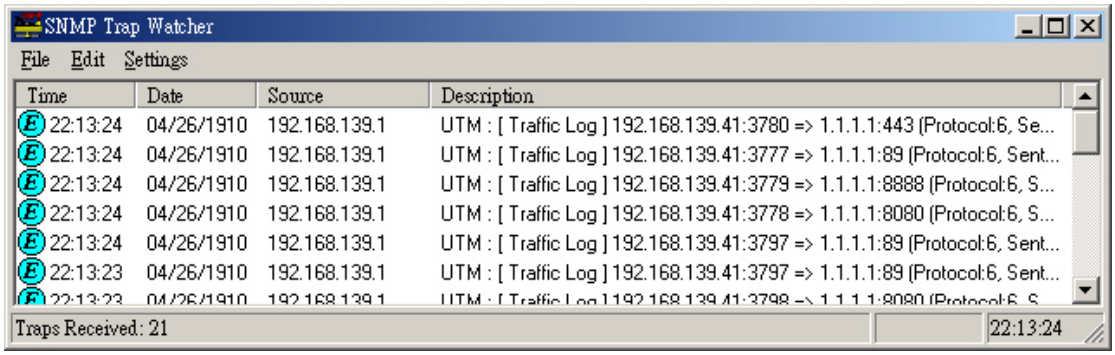


圖 22-34 傳送 SNMP Trap 警訊

4. 【啟動 RSS feeds】後，可透過所安裝 RSS 收訊軟體，訂閱即時監控記錄。（如圖 22-35，圖

22-36, 圖 22-37）

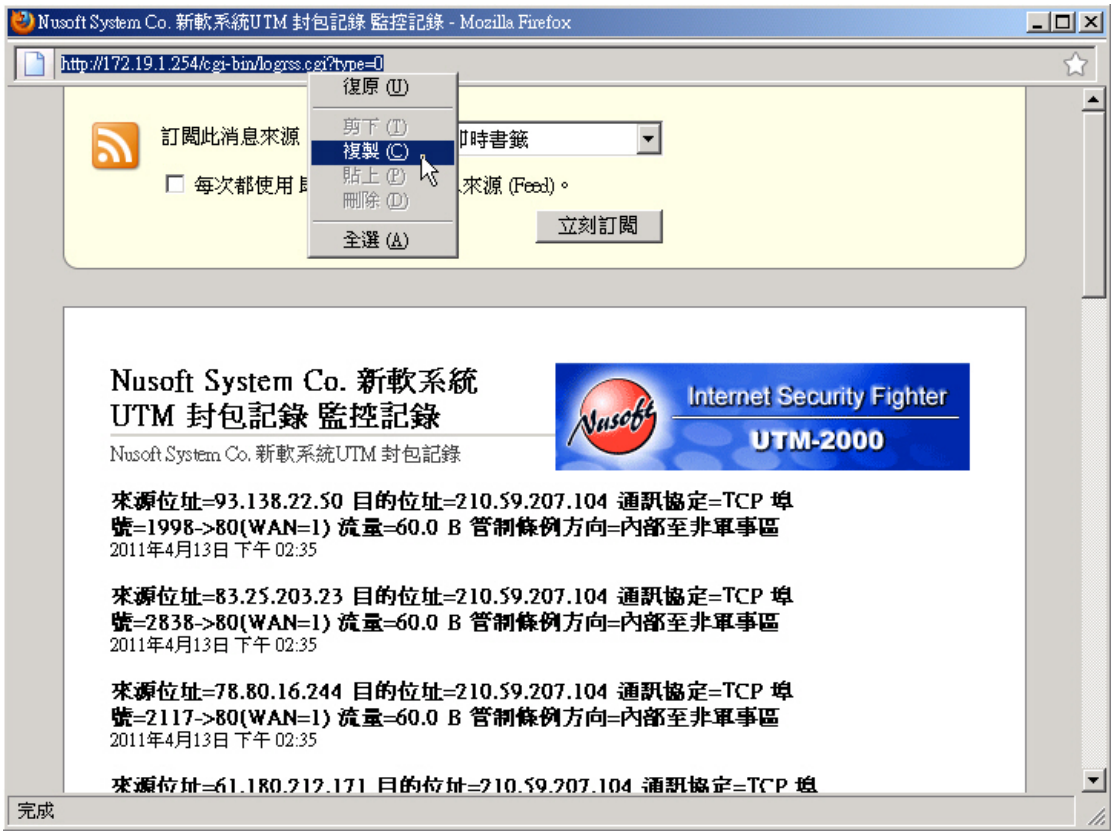


圖 22-35 瀏覽 RSS 即時監控記錄

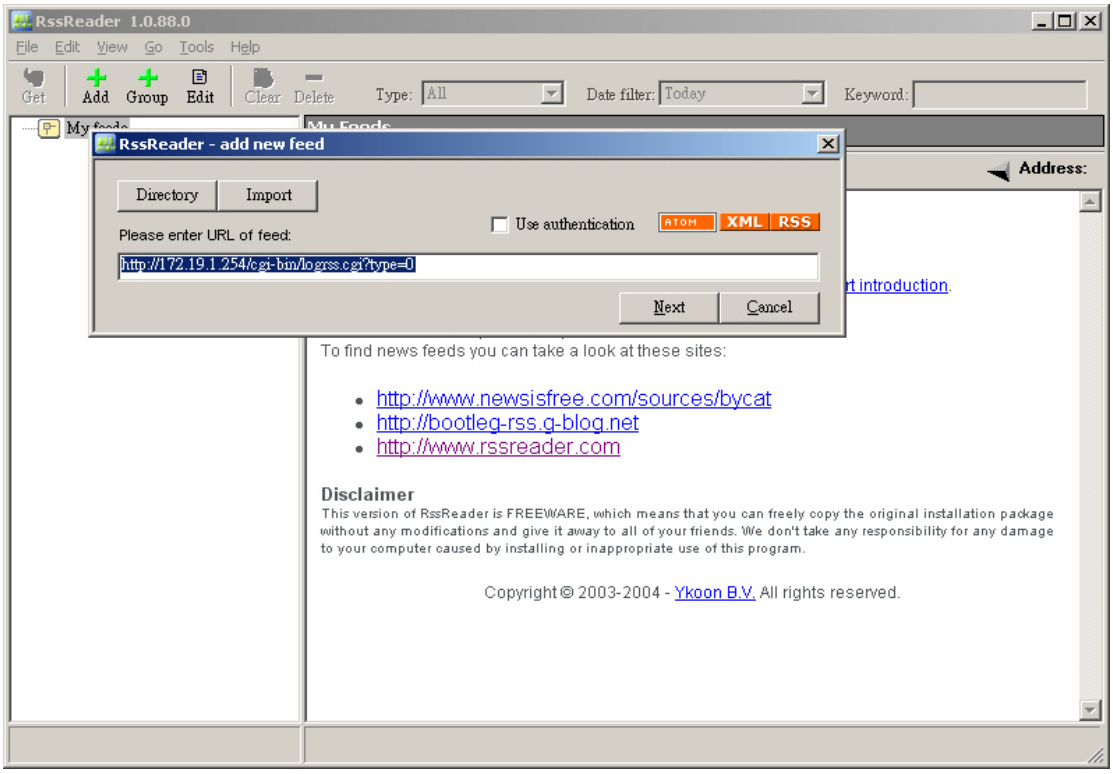


圖 22-36 將 RSS 即時監控連結加入 RSS 收訊軟體

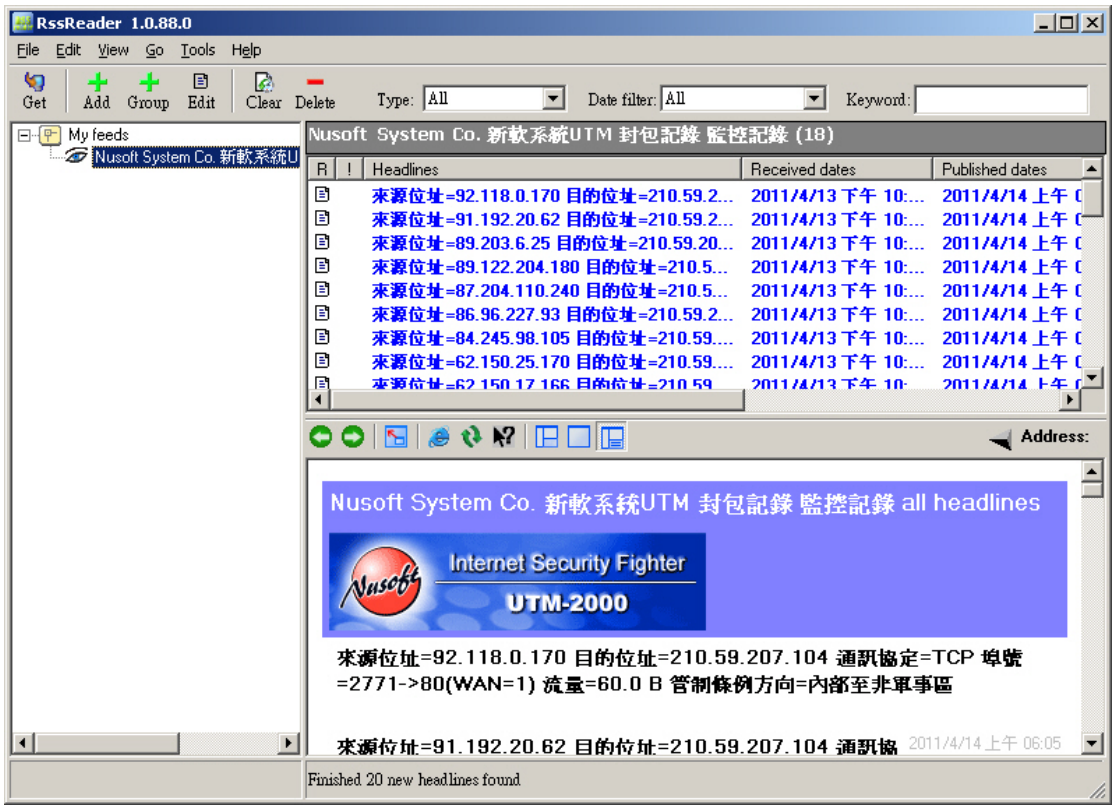


圖 22-37 以 RSS 收訊軟體訂閱即時監控記錄

第23章　流量排行

系統管理員可利用即時流量分析、今日排行榜和歷史排行榜功能，來了解使用者透過 MHG-2000 傳輸的網路流量和進行的網路活動。

- 【即時流量分析】：可顯示進行傳輸的來源位址、網路服務之即時流量。
- 【今日排行榜】：可顯示當天特定時段內進行傳輸的來源位址、目的位址、網路服務之累積流量。
- 【歷史排行榜】：可顯示指定時間範圍內進行傳輸的日期、來源位址、目的位址、網路服務之累積流量。

【設定】功能概述：

流量排行設定 說明如下：

- 用來記錄內部和外部電腦間進行傳輸的來源位址、目的位址、網路服務流量。
  - 在【監控報告】>【流量排行】>【設定】頁面的【流量排行設定】欄位中，做下列設定：
    - 勾選【記錄內部（含非軍事區）至外部流量】的來源位址、目的位址、網路服務項目。
    - 勾選【記錄外部至內部（含非軍事區）流量】的來源位址、目的位址、網路服務項目。
    - 按下【確定】鈕，完成設定。（如圖 23-1）

圖 23-1 流量排行設定頁面

【即時流量分析】功能概述：

來源位址 說明如下：

- 可顯示經 MHG-2000 進行傳輸的來源位址之即時流量。
- 來源位址：表示封包傳輸時的來源位址。
- 流量：表示該來源位址傳輸的資料量。
- 可將來源位址的資料傳輸總量，與其個別資料傳輸量列出比例值。

網路服務 說明如下：

- 可顯示經 MHG-2000 進行傳輸的網路服務之即時流量。
- 網路服務：表示封包傳輸時採用的通訊協定和埠號。
- 流量：表示透過該網路服務傳輸的資料量。
- 可將網路服務的資料傳輸總量，與其個別資料傳輸量列出比例值。

【今日排行榜】功能概述：

您可以拖曳 游標 / 游標間紅色區塊 來選擇欲統計的時間 說明如下：

- 可方便觀察特定時段內的流量統計資料。

來源位址 說明如下：

- 可顯示當天特定時段內，經 MHG-2000 進行傳輸的來源位址之累積流量。
- 來源位址：表示封包傳輸時的來源位址。
- 下載流量 / 上傳流量：表示該來源位址上傳/下載的資料量。
- 可將來源位址的資料傳輸總量，與其個別資料傳輸量列出比例值。

目的位址 說明如下：

- 可顯示當天特定時段內，經 MHG-2000 進行傳輸的目的位址之累積流量。
- 目的位址：表示封包傳輸時的目的位址。
- 下載流量 / 上傳流量：表示該目的位址上傳/下載的資料量。
- 可將目的位址的資料傳輸總量，與其個別資料傳輸量列出比例值。

網路服務 說明如下：

- 可顯示當天特定時段內，經 MHG-2000 進行傳輸的網路服務之累積流量。
- 網路服務：表示封包傳輸時採用的通訊協定和埠號。
- 下載流量 / 上傳流量：表示透過該網路服務上傳/下載的資料量。
- 可將網路服務的資料傳輸總量，與其個別資料傳輸量列出比例值。

【歷史排行榜】功能概述：

更新 說明如下：

- 可依照日期、來源位址、目的位址或網路服務等條件，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【流量排行】>【歷史排行榜】頁面中，做下列設定：
    - 選擇【來源位址】。
    - 設定搜尋指定時間區間內的記錄。
    - 按下【更新】鈕。
    - 按【下載】鈕，將目前搜尋到的記錄清單即時備份到本機電腦。（如圖 23-2）
    - 按下【清除全部】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由 MHG-2000 上清除。（如圖 23-3）

圖 23-2 下載搜尋的記錄

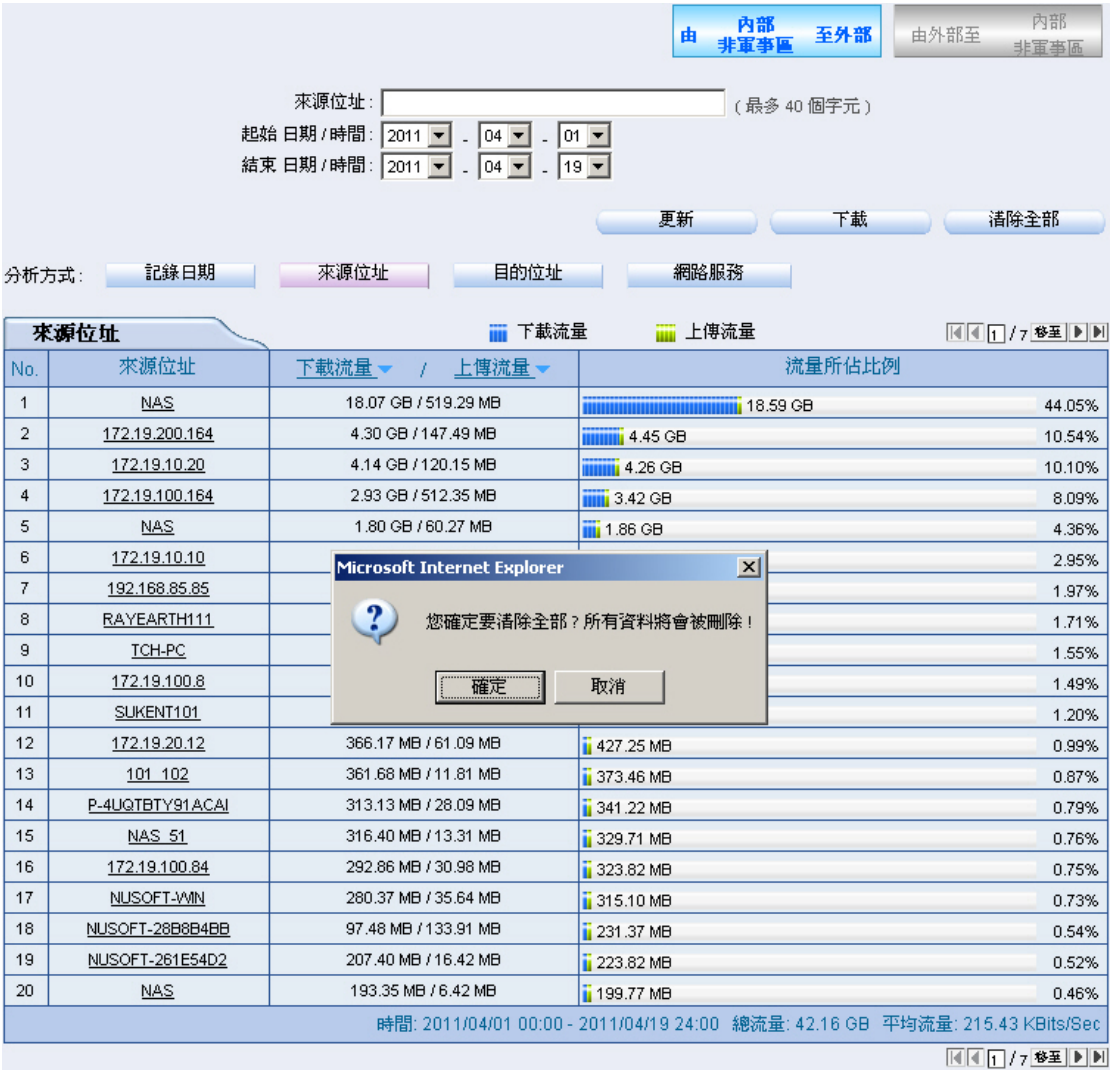


圖 23-3 清除歷史流量排行記錄

23.1 即時流量分析

步驟1. 於【監控報告】>【流量排行】>【即時流量分析】頁面中，會顯示經 MHG-2000 進行傳輸的來源位址、網路服務之即時流量。（如圖 23-4）

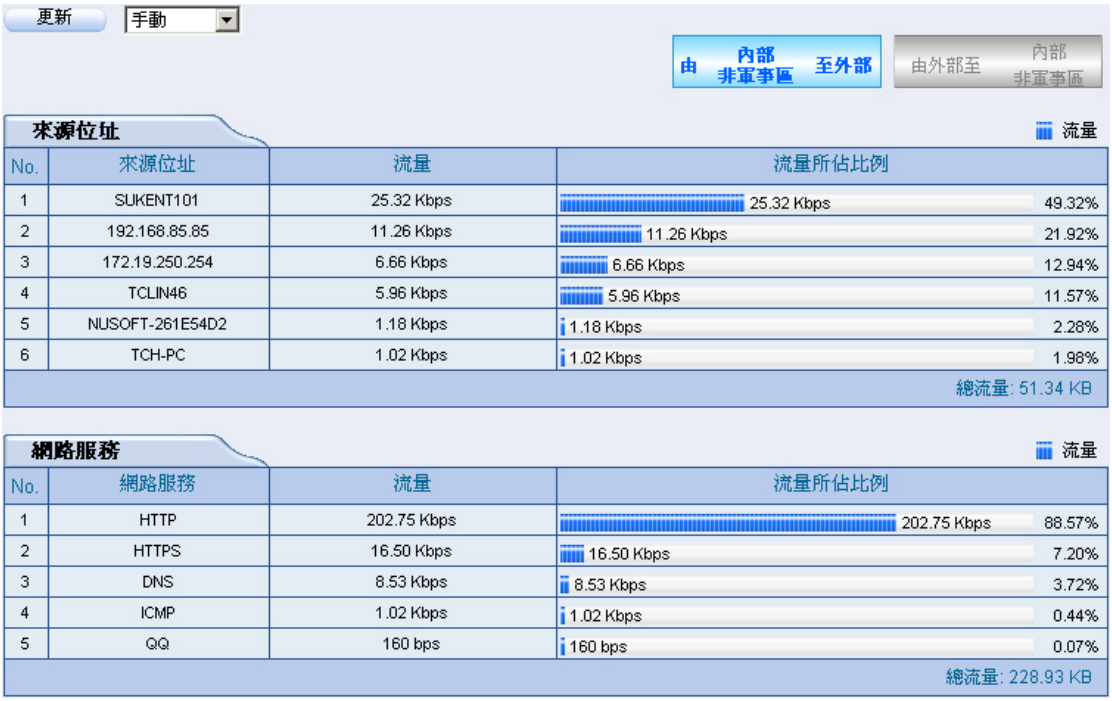


圖 23-4 即時流量排行榜

23.2 今日排行榜

步驟1. 於【監控報告】>【流量排行】>【今日排行榜】頁面中，會顯示當天特定時段內，經 MHG-2000 進行傳輸的來源位址、目的位址、網路服務之累積流量。（如圖 23-5）

- 可使用滑鼠拖曳畫面上方的滑動鈕來設定統計時間，左邊滑動鈕為起始時間，右邊滑動鈕為終止時間。調整時間區間後，MHG-2000 將會自動統計區間內的流量，來源位址、目的位址與網路服務排行榜也會隨著時間點改變而同步調整。（如圖 23-6）
- 在來源位址排行榜點擊【來源位址】連結，會跳出視窗顯示傳輸資料時，該來源位址連線的目的位址、透過的網路服務。（如圖 23-7）
- 在目的位址排行榜點擊【目的位址】連結，會跳出視窗顯示傳輸資料時，連線該目的位址的來源位址、透過的網路服務。（如圖 23-8）
- 在網路服務排行榜點擊【網路服務】連結，會跳出視窗顯示傳輸資料時，透過該網路服務連線的來源位址、目的位址。（如圖 23-9）

由 內部 非軍事區 至外部
由外部至 內部 非軍事區
18:47 18:57
00:00
18:57
您可以拖曳 游標 / 游標間紅色區塊 來選擇欲統計的時間
來源位址
下載流量
上傳流量
1 / 4 移至
No. 來源位址 下載流量 / 上傳流量 流量所佔比例
1 V12 4.86 MB / 180.80 KB 5.02 MB 69.03%
2 SUKENT101 577.79 KB / 124.01 KB 701.80 KB 9.43%
3 RAYEARTH111 424.71 KB / 104.83 KB 529.52 KB 7.11%
4 DD 455.87 KB / 11.94 KB 467.79 KB 6.28%
5 192.168.85.85 285.81 KB / 84.94 KB 370.73 KB 4.98%
6 172.19.250.254 41.32 KB / 14.22 KB 55.54 KB 0.75%
7 NUSOFT-WIN 7.40 KB / 21.66 KB 29.04 KB 0.39%
8 NUSOFT-RD31 18.74 KB / 5.00 KB 23.71 KB 0.32%
9 172.19.100.91 17.72 KB / 4.44 KB 22.13 KB 0.30%
10 172.19.100.170 14.87 KB / 0 B 14.87 KB 0.20%
時間: 18:47 - 18:57 總流量: 7.28 MB 平均流量: 99.27 KBits/Sec
1 / 4 移至
目的位址
下載流量
上傳流量
1 / 14 移至
No. 目的位址 下載流量 / 上傳流量 流量所佔比例
1 i175.photobucket.com 4.19 MB / 94.38 KB 4.29 MB 58.88%
2 mail.formay.com 577.59 KB / 123.98 KB 701.54 KB 9.42%
3 image.tca.org.tw 450.55 KB / 11.49 KB 462.01 KB 6.21%
4 www.eurobricks.com 205.35 KB / 30.22 KB 235.57 KB 3.16%
5 lh3.ggpht.com 204.87 KB / 30.59 KB 235.44 KB 3.16%
6 www.google.com.tw 164.22 KB / 16.21 KB 180.44 KB 2.42%
7 www.brickshelf.com 144.49 KB / 9.95 KB 154.41 KB 2.07%
8 images-na.ssl-images-amaz... 91.12 KB / 5.17 KB 96.28 KB 1.29%
9 www.google.com.tw 82.79 KB / 9.91 KB 92.67 KB 1.24%
10 www.gamer.com.tw 79.28 KB / 5.38 KB 84.66 KB 1.14%
時間: 18:47 - 18:57 總流量: 7.28 MB 平均流量: 99.27 KBits/Sec
1 / 14 移至
網路服務
下載流量
上傳流量
1 / 5 移至
No. 網路服務 下載流量 / 上傳流量 流量所佔比例
1 HTTP 6.20 MB / 416.67 KB 6.62 MB 90.82%
2 HTTPS 382.77 KB / 123.22 KB 505.99 KB 6.80%
3 DNS 94.67 KB / 24.86 KB 119.51 KB 1.61%
4 MSN 13.25 KB / 5.34 KB 18.59 KB 0.25%
5 ICMP 15.26 KB / 0 B 15.26 KB 0.20%
6 BT 3.85 KB / 270 B 4.10 KB 0.06%
7 SSH 1.54 KB / 1.79 KB 3.30 KB 0.04%
8 POP3 1.66 KB / 845 B 2.48 KB 0.03%
9 CALLBOOK 1.85 KB / 624 B 2.45 KB 0.03%
10 TCP:2703 924 B / 760 B 1.66 KB 0.02%
時間: 18:47 - 18:57 總流量: 7.28 MB 平均流量: 99.27 KBits/Sec
1 / 5 移至

圖 23-5 今日排行榜

圖 23-6 指定時間區間的今日排行榜

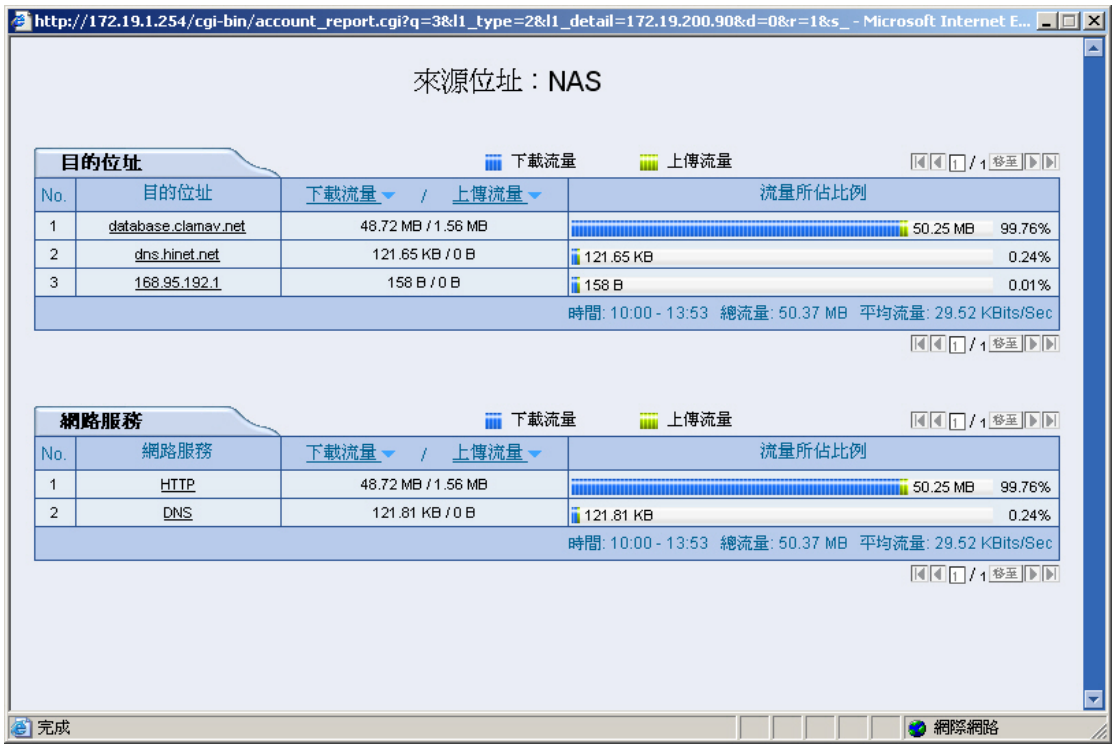


圖 23-7 傳送資料時來源位址連線的目的位址、透過的網路服務

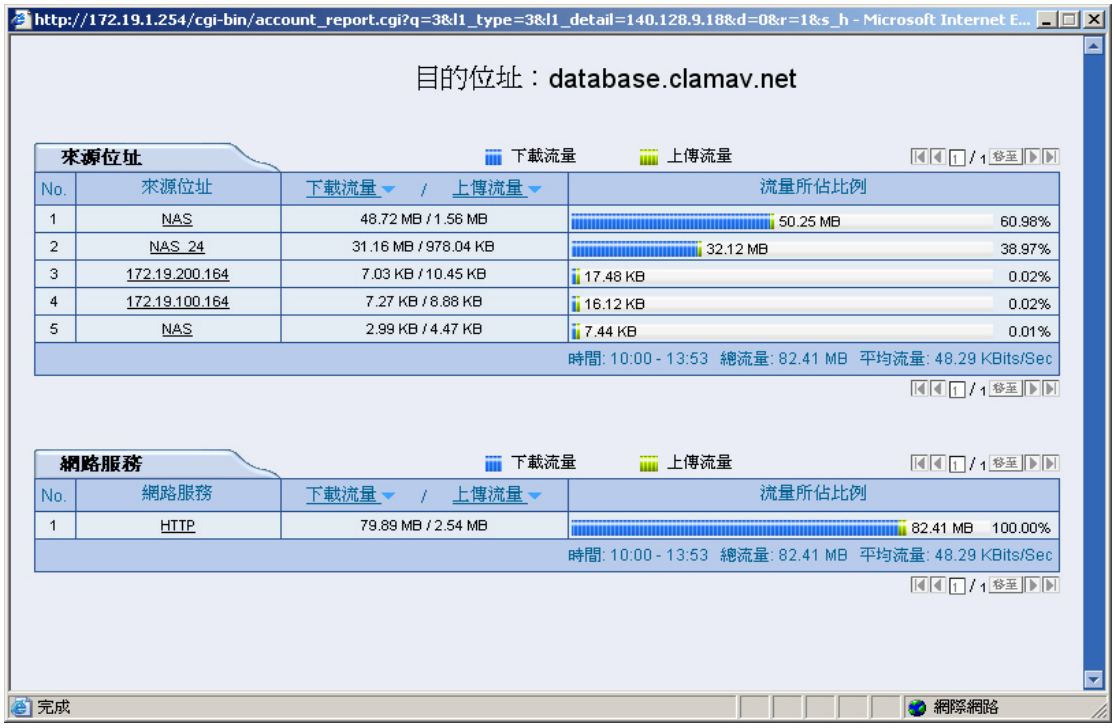


圖 23-8 傳送資料時連線目的位址的來源位址、透過的網路服務

圖 23-9 傳送資料時透過特定網路服務連線的來源位址、目的位址

23.3 歷史排行榜

步驟1. 於【監控報告】>【流量排行】>【歷史排行榜】頁面中，可顯示指定時間範圍內，經 MHG-2000 進行傳輸的日期、來源位址、目的位址、網路服務之累積流量。（如圖 23-10）

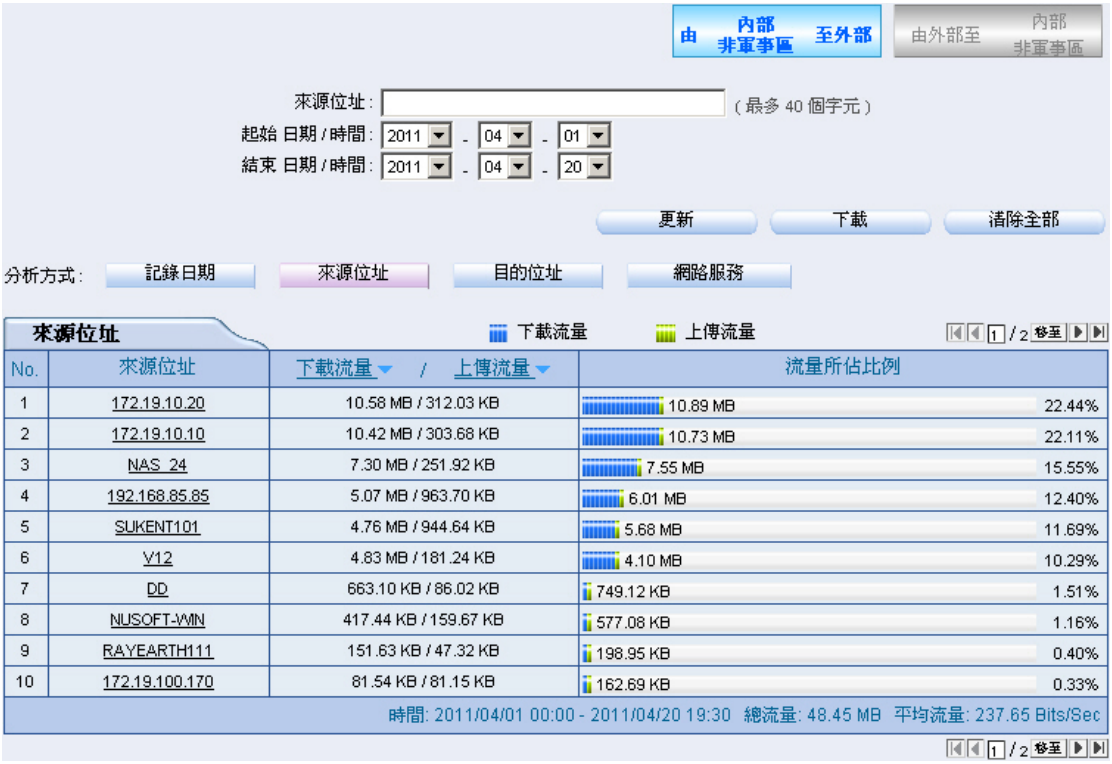


圖 23-10 歷史排行榜

第24章　流量圖表

用於統計 MHG-2000 外部網路介面或是所設定的管制條例之封包與資料傳輸流量，讓系統管理員了解網路流量狀況。

- 【外部網路 / 虛擬外部網路】: 經過外部網路介面下載/上傳的資料量、接收/傳送的封包量統計資料。
- 【管制條例】: 經過管制條例下載/上傳的資料量、接收/傳送的封包量統計資料。

【流量圖表】功能概述：

流量統計圖表 說明如下：

- 縱座標：網路流量。
- 橫座標：時間。

管制條例方向 / 來源網路 / 目的網路 / 服務名稱 / 動作 說明如下：

- 條列進行流量統計的管制條例規則。

時間 說明如下：

- 可分別檢視以分、時、日、週、月、年為時間單位的流量統計。

說明：

1. 當檢視時間選擇為：

- 【分】: 流量統計圖表會每分鐘更新一次。
- 【時】: 流量統計圖表會每小時更新一次。
- 【日】; 流量統計圖表會每日更新一次。
- 【週】: 流量統計圖表會每週更新一次。
- 【月】: 流量統計圖表會每月更新一次。
- 【年】: 流量統計圖表會每年更新一次。

Bits/sec Bytes/sec 使用率 累計（全部） 說明如下：

- 系統管理員可由此變換統計圖的流量計算標準。
  - Bits/sec：每秒鐘傳送的資料位元。
  - Bytes/sec：每秒鐘傳送的資料位元組。
  - 使用率：流量佔 MHG-2000 外部網路介面設定的最大下載/上傳頻寬之比例。
  - 累計（全部）: 單位時間內所累加的資料傳輸量。

24.1 外部網路

步驟1. 在【監控報告】>【流量圖表】>【外部網路】頁面中，找到欲檢視的外部網路介面名稱，對應至右方【時間單位】欄：**（如圖 24-1, 圖 24-2）**

- 點選【分】，可檢視以每分鐘（Minute）為單位的流量統計圖表。
- 點選【時】，可檢視以每小時（Hour）為單位的流量統計圖表。
- 點選【日】，可檢視以每日（Day）為單位的流量統計圖表。
- 點選【週】，可檢視以每週（Week）為單位的流量統計圖表。
- 點選【月】，可檢視以每月（Month）為單位的流量統計圖表。
- 點選【年】，可檢視以每年（Year）為單位的流量統計圖表。

外部網路	時間
WAN1	分 時 日 週 月 年
WAN2	分 時 日 週 月 年
All WAN	分 時 日 週 月 年

圖 24-1 外部網路流量統計頁面

圖 24-2 外部網路流量統計圖

說明：

1. 當設定【網路介面】>【介面位址】為外部網路介面時，其對應的外部網路流量統計機制也會隨之啟用。
2. 可檢視指定時間開始記錄的流量統計圖。

24.2 虛擬外部網路

步驟1. 在【監控報告】>【流量圖表】>【虛擬外部網路】頁面中，找到欲檢視的虛擬外部網路介面名稱，對應至右方【時間單位】欄：**（如圖 24-3, 圖 24-4）**

- 點選【分】，可檢視以每分鐘（Minute）為單位的流量統計圖表。
- 點選【時】，可檢視以每小時（Hour）為單位的流量統計圖表。
- 點選【日】，可檢視以每日（Day）為單位的流量統計圖表。
- 點選【週】，可檢視以每週（Week）為單位的流量統計圖表。
- 點選【月】，可檢視以每月（Month）為單位的流量統計圖表。
- 點選【年】，可檢視以每年（Year）為單位的流量統計圖表。

名稱	時間單位
Virtual_WAN1	分 時 日 週 月 年

圖 24-3 虛擬外部網路流量統計頁面

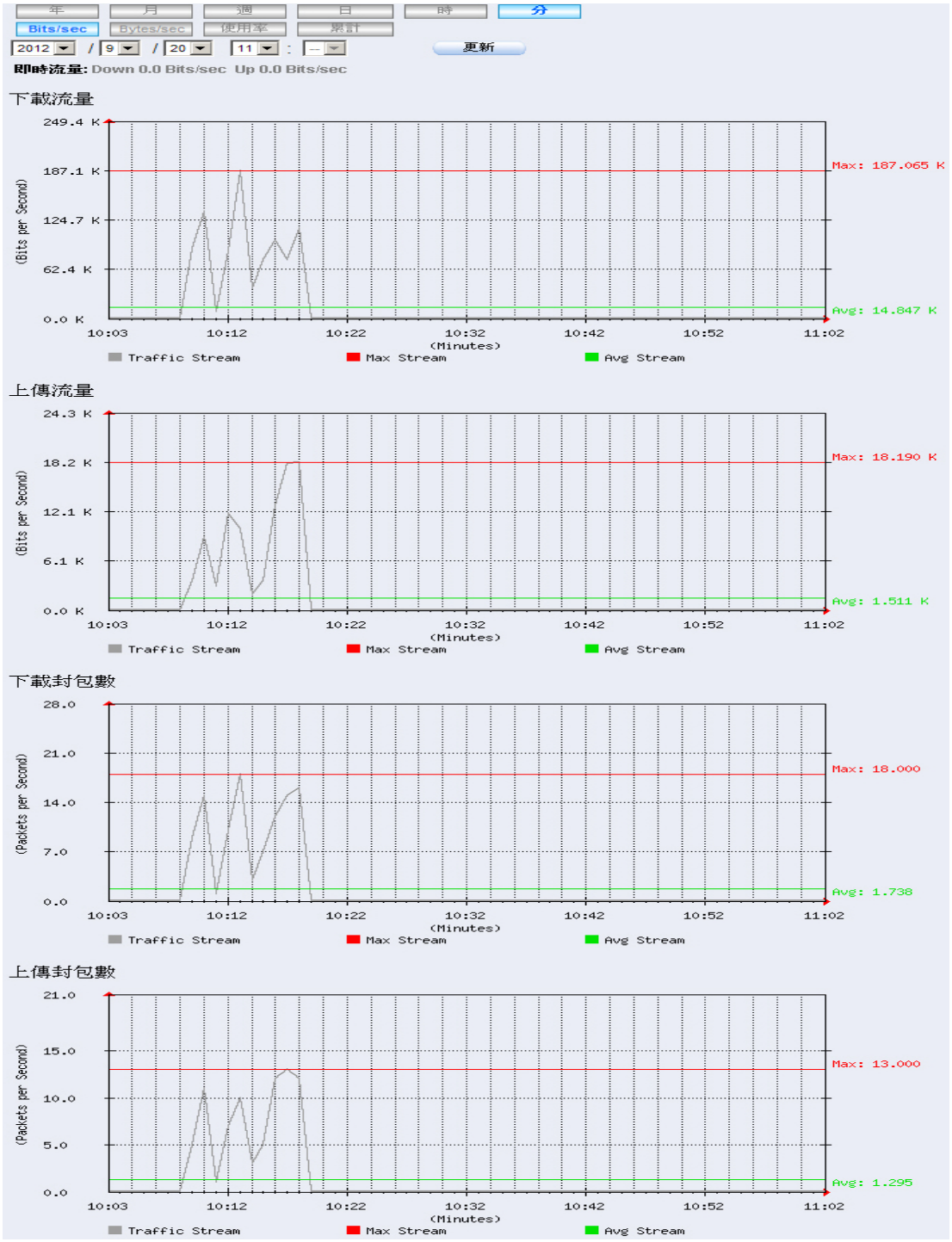


圖 24-4 虛擬外部網路流量統計圖

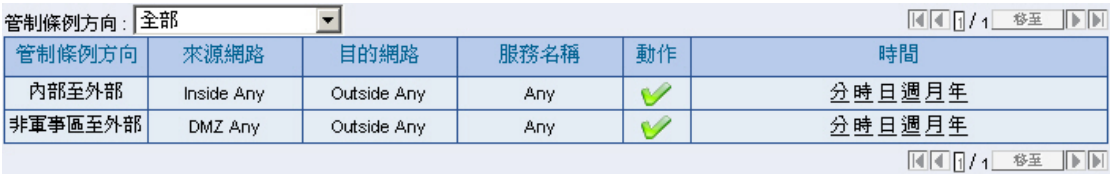
說明：

1. 當設定【網路介面】>【虛擬外部網路】介面時，其對應的虛擬外部網路流量統計機制也會隨之啟用。
2. 可檢視指定時間開始記錄的流量統計圖。

24.3 管制條例

步驟1. 當【管制條例】有開啟【流量圖表】功能時，在【監控報告】>【流量圖表】>【管制條例】頁面中，找到欲檢視的【管制條例】，對應至右方【時間】欄：（如圖 24-5, 圖 24-6）

- 點選【分】，可檢視以每分鐘（Minute）為單位的流量統計圖表。
- 點選【時】，可檢視以每小時（Hour）為單位的流量統計圖表。
- 點選【日】，可檢視以每日（Day）為單位的流量統計圖表。
- 點選【週】，可檢視以每週（Week）為單位的流量統計圖表。
- 點選【月】，可檢視以每月（Month）為單位的流量統計圖表。
- 點選【年】，可檢視以每年（Year）為單位的流量統計圖表。



管制條例方向	來源網路	目的網路	服務名稱	動作	時間
內部至外部	Inside Any	Outside Any	Any	✔	分 時 日 週 月 年
非軍事區至外部	DMZ Any	Outside Any	Any	✔	分 時 日 週 月 年

1 / 1 移至

圖 24-5 管制條例流量統計頁面

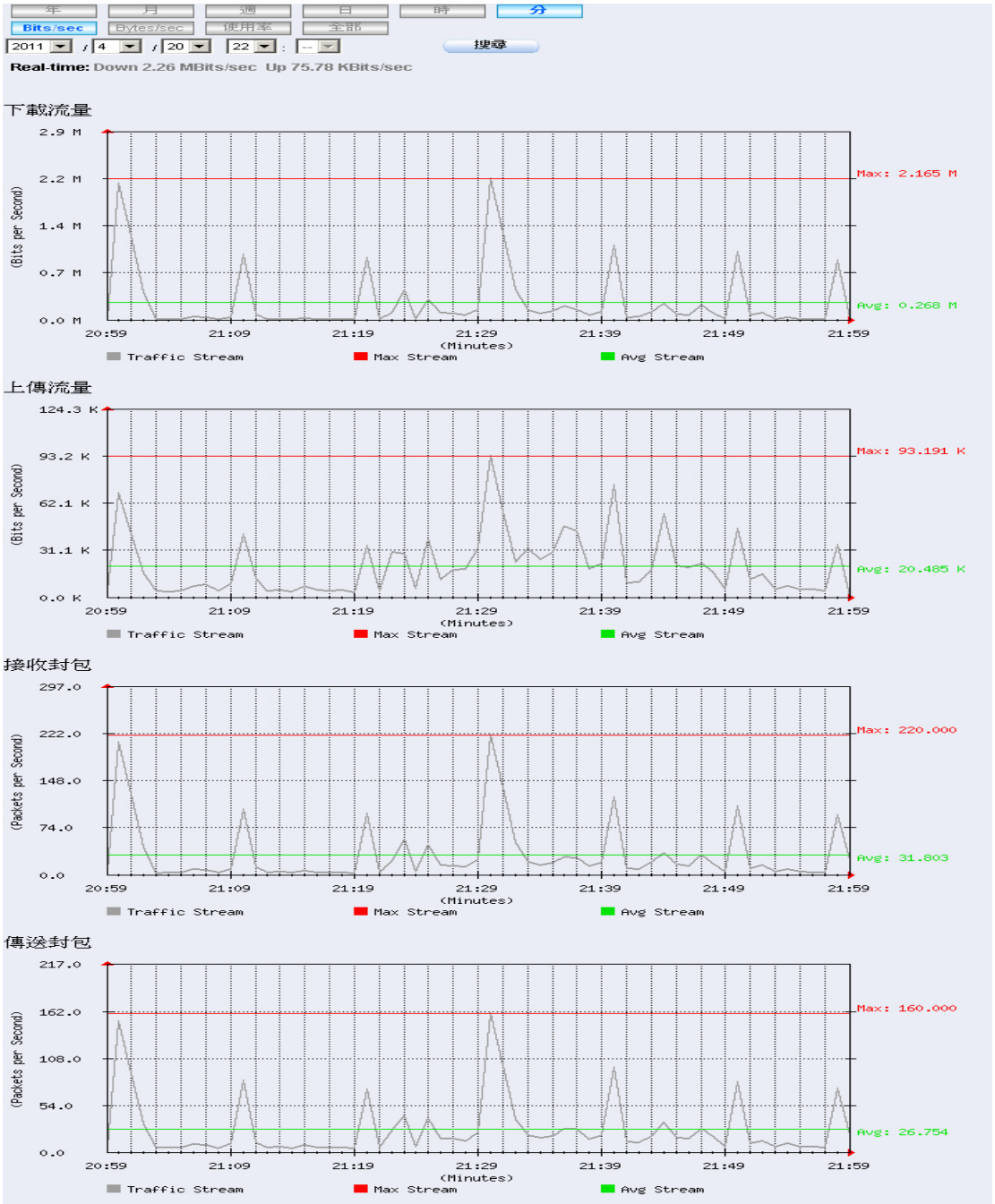


圖 24-6 管制條例流量統計圖

說明：

1. 若欲進行管制條例流量統計，系統管理員須於【管制條例】啟動【流量圖表】功能。
2. 管制條例流量統計的【管制條例方向】可分為：內部至外部、外部至內部、外部至非軍事區、內部至非軍事區、非軍事區至外部、非軍事區至內部、內部至內部、非軍事區至非軍事區。
3. 可檢視指定時間開始記錄的流量統計圖。

第25章　網路偵測

使用者可由系統主動發送封包（Ping 和 Traceroute），得知目前連線的資料傳輸品質和狀態。

25.1 Ping

步驟1. 在【監控報告】>【網路偵測】>【Ping】頁面中，可直接由 MHG-2000 用 Ping 指令，發送封包到特定位址，以確認連線的資料傳輸狀況：（如圖 25-1）

- 輸入指定的【目標 IP 或網域名稱】、【封包大小】(預設為 32 Bytes)、【回應次數】(預設為 4)、【等待時間】(預設為 1 秒)。
- 選填指定的來源【介面位址】。
- 按下【確定】鈕，進行網路偵測。（如圖 25-2）

圖 25-1Ping 偵測設定

圖 25-2Ping 偵測結果

說明：

1. 【介面位址】若選擇 VPN-WAN1, VPN-WAN2 或其他 VPN 連線介面，必須填入 VPN 連線溝通的本地端 MHG-2000 內部網路介面 IP 位址，【目標 IP 或網域名稱】則要填入遠端內網可透過 VPN 收送封包的 IP 位址。

- 當本地端的 192.168.189.x/24 網段透過 WAN1 和遠端的 192.168.169.x/24 網段，建起 VPN 連線時，可以下列方式，測試彼此封包傳輸的情形：**（如圖 25-3）**

圖 25-3 透過 VPN 連線的 Ping 偵測結果

25.2 Traceroute

步驟1. 在【監控報告】>【網路偵測】>【Traceroute】頁面中，可直接由 MHG-2000 用 Traceroute 指令，發送封包到特定位址，以確認連線的資料傳輸狀況：（如圖 25-4）

- 輸入指定的【目標 IP 或網域名稱】、【封包大小】(預設為 40 Bytes)、【最大存活時間】(預設為 30 節點)、【等待時間】(預設為 2 秒)。
- 選擇指定的【測試介面】發送封包。
- 按下【確定】鈕，進行網路偵測。（如圖 25-5）

圖 25-4Traceroute 偵測設定

圖 25-5Traceroute 偵測結果

第26章　遠端喚醒

使用者可由系統主動發送封包，來啟動內部網路允許透過網路卡開機的特定電腦，並搭配 VNC、Terminal Service 或 PC Anywhere 等軟體，執行遠端遙控的動作。

26.1 遠端喚醒功能使用範例

26.1.1 遠端啟動欲遙控的內部電腦

步驟1. 可被遠端啟動遙控的內部網路電腦，其網卡MAC為00:0C:76:B7:96:3B。

步驟2. 在【監控報告】>【遠端喚醒】>【設定】頁面中，做下列設定：

- 輸入指定的【名稱】。
- 【MAC 位址】輸入 00:0C:76:B7:96:3B。
- 按下【確定】鈕，完成設定。（如圖 26-1）

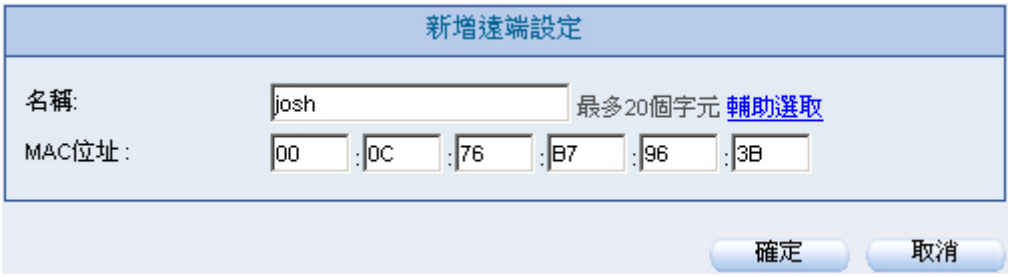


圖 26-1 遠端喚醒設定頁面

步驟3. 按下【喚醒】鈕，執行遠端啟動電腦的動作。（如圖 26-2）

圖 26-2 遠端啟動電腦

第27章　系統狀態

系統管理員可隨時得知目前 MHG-2000 的網路介面狀態、系統效能、認證狀態、ARP 表、連線狀態、DHCP 用戶表、主機資訊等各項資訊。

- 【介面狀態】：顯示目前 MHG-2000 的所有網路介面狀態。
- 【系統效能】：顯示目前 MHG-2000 的 CPU、記憶體的使用率。
- 【認證狀態】：記錄 MHG-2000 之認證機制使用情況。
- 【ARP 表】：記錄透過或與 MHG-2000 建立連線的設備之 IP、MAC 位址對應資訊。
- 【連線狀態】：記錄目前所有透過 MHG-2000 管制條例傳輸封包的連線。
- 【DHCP 用戶表】：記錄 MHG-2000 內建 DHCP 伺服器配發 IP 的狀況。
- 【主機資訊】：記錄通過 MHG-2000 的連線 IP 和其對應 NetBIOS、DNS 名稱資訊。

【ARP 表】功能概述：

搜尋 說明如下：

- 可依照網際協定、目前 IP 位址、MAC 位址和介面等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【系統狀態】>【ARP 表】的【搜尋】頁面中，做下列設定：
    - 選擇指定【網際協定】、【介面】。
    - 按下【搜尋】鈕。（如圖 27-1）

圖 27-1 搜尋特定記錄

【連線狀態】功能概述：

搜尋 說明如下：

- 可依照管制條例方向、排序、網際協定、來源位址、目的位址和埠號等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【系統狀態】>【連線狀態】的【搜尋】頁面中，做下列設定：
    - 選擇指定【管制條例方向】、【排序】、【網際協定】。
    - 按下【搜尋】鈕。（如圖 27-2）

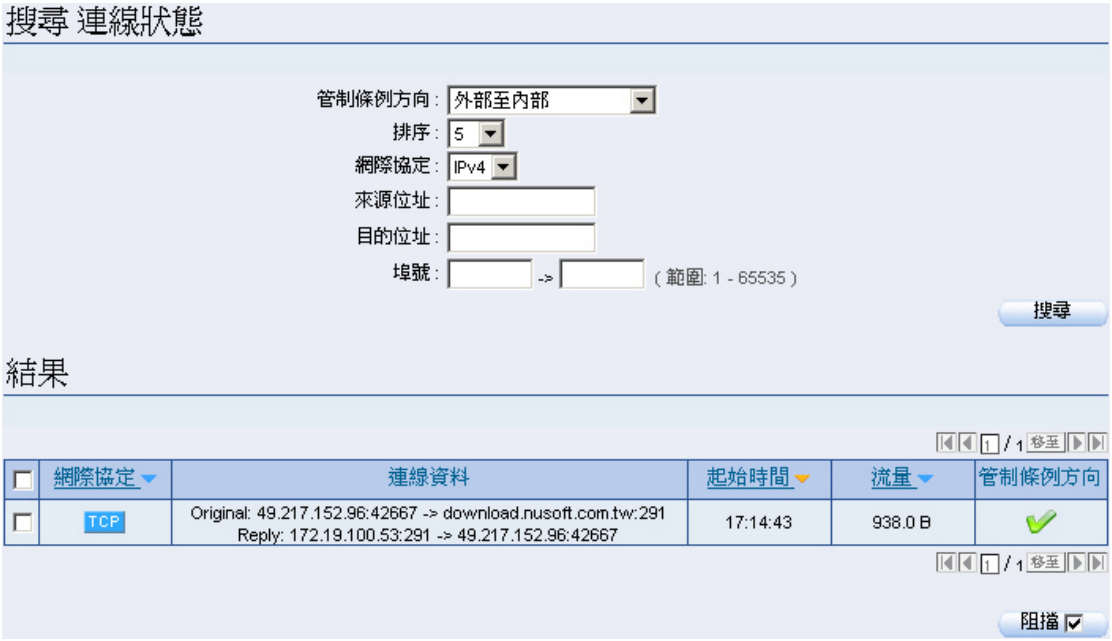


圖 27-2 搜尋特定記錄

【DHCP 用戶表】功能概述：

搜尋 說明如下：

- 可依照網際協定、IP 位址和 MAC 位址等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【系統狀態】>【DHCP 用戶表】的【搜尋】頁面中，做下列設定：
    - 選擇指定【網際協定】。
    - 按下【搜尋】鈕。（如圖 27-3）

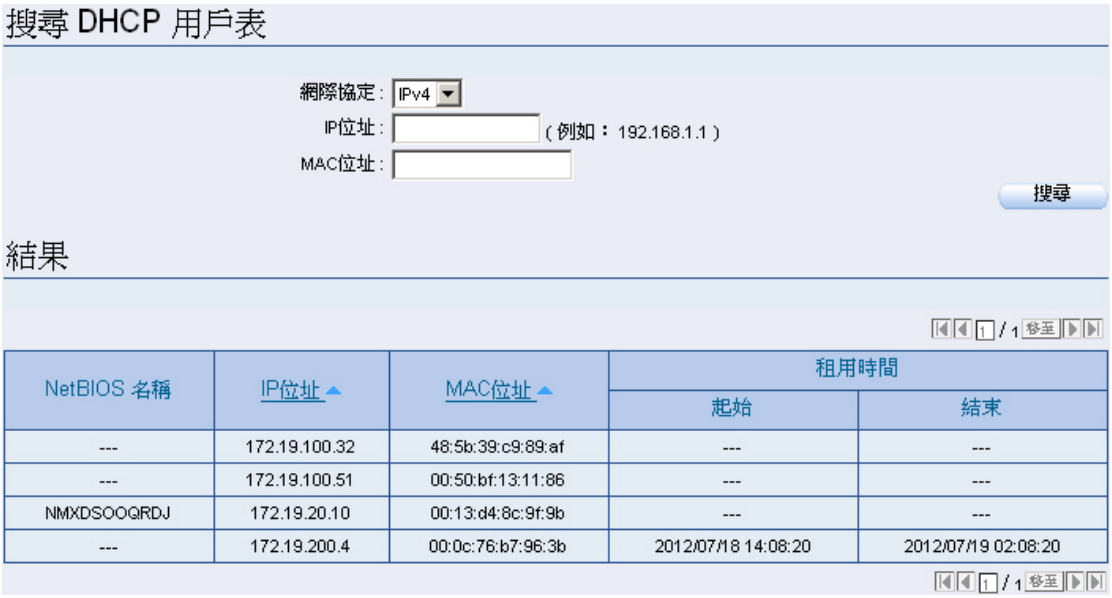


圖 27-3 搜尋特定記錄

【主機資訊】功能概述：

搜尋 說明如下：

- 可依照主機類型、IP 位址和名稱等關鍵字或特徵，來尋找儲存在 MHG-2000 內所有符合條件之記錄。
  - 在【監控報告】>【系統狀態】>【主機資訊】的【搜尋】頁面中，做下列設定：
    - 選擇指定【主機類型】。
    - 按下【搜尋】鈕。（如圖 27-4）

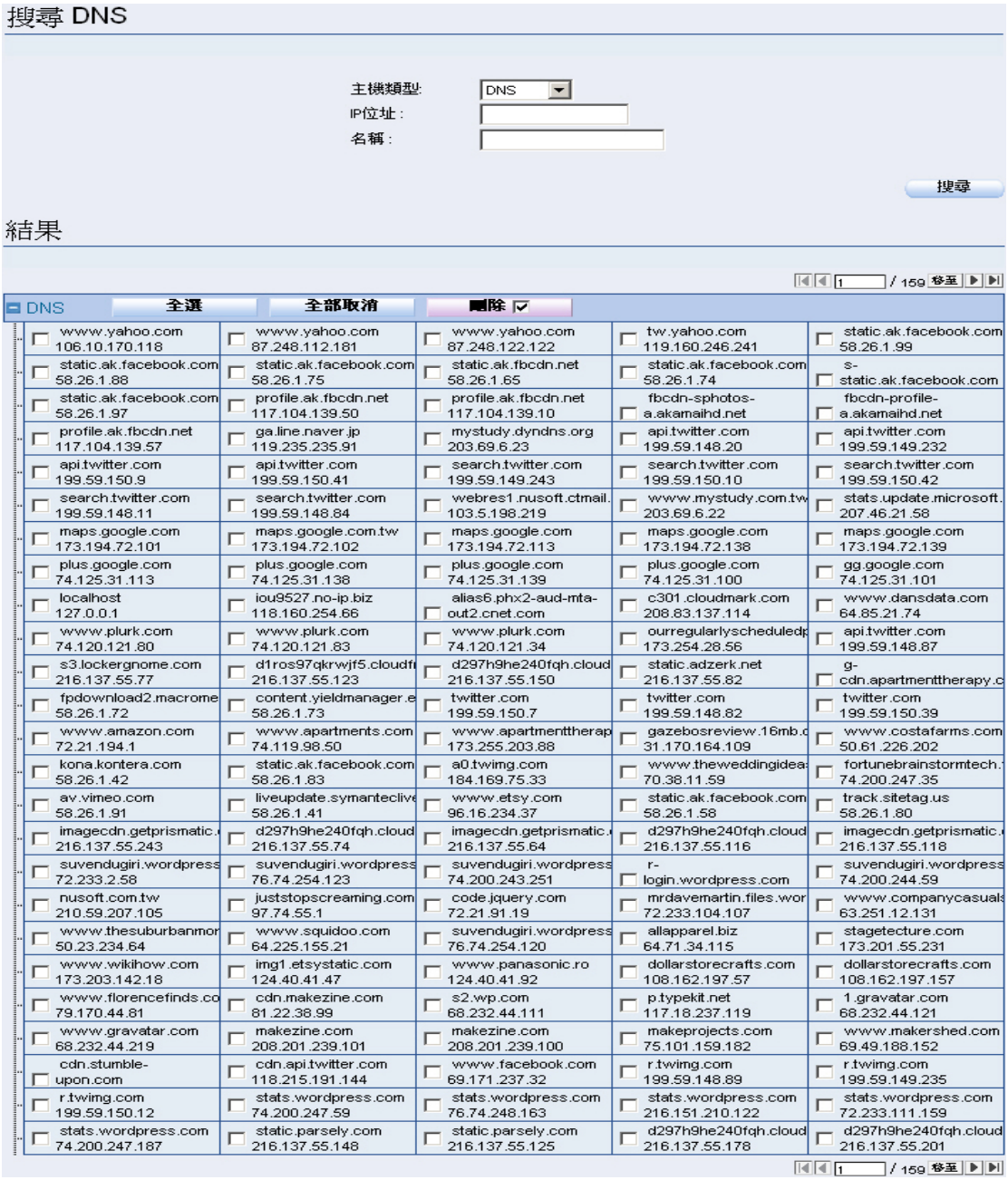


圖 27-4 搜尋特定記錄

27.1 介面狀態

步驟1. 在【監控報告】>【系統狀態】>【介面狀態】頁面中，會顯示目前 MHG-2000 各網路介面運作之相關訊息：（如圖 27-5）

系統連線數目 : 7617　　系統開機歷時 : 0 天 21 時 48 分 36 秒

介面編號	1	2	3	4	5	6	7
介面定義	LAN1	WAN1	WAN2	WAN3	DMZ1	WAN4	DMZ2
模式	NAT	固定IP	撥號連線	撥號連線	透通路由模式	固定IP	透通橋接模式
外部網路連線狀態							
連線速率	1000Mb/s	100Mb/s	100Mb/s	100Mb/s	100Mb/s		
雙工模式	全雙工	全雙工	全雙工	全雙工	全雙工		
網路頻寬（上傳/下載）Kbps		4096 / 4096	10240 / 2048	4096 / 2048		204800 / 204800	
下載流量比例		90%	10%	0%			
上傳流量比例		98%	2%	0%			
連線歷時			4:01:27	21:46:27			
MAC位址	00:90:0B:14:B1:46	00:90:0B:14:B1:4B	00:90:0B:14:B1:4A	00:90:0B:14:B1:49	00:90:0B:14:B1:48	00:90:0B:14:B1:47	
IPv4位址	172.19.1.254	59.124.36.162	114.32.109.246	114.37.82.95		172.39.1.1	
子網路遮罩	255.255.0.0	255.255.255.240	255.255.255.255	255.255.255.255		255.255.0.0	
IPv4預設閘道		59.124.36.161	168.95.98.254	168.95.98.254		172.39.1.254	
IPv6位址	2001:0DB8:0:F101::1	2001:0DB8:1FF:F101::2					
首碼長度	64	64					
IPv6 預設閘道		2001:0DB8:1FF:F101::1					
DNS伺服器 1		168.95.1.1	168.95.1.1	168.95.1.1		168.95.1.1	
DNS伺服器 2		168.95.192.1	168.95.192.1	168.95.192.1		168.95.192.1	
接收封包數（成功 / 錯誤）	3011470,0	22209204,0	2636762,0	84527,0	17517723,0	0,0	0,0
傳送封包數（成功 / 錯誤）	3470591,0	21343726,0	2056879,0	72681,0	18370979,0	0,0	0,0
Ping	✔	✔	✔	✔	✔	✔	✘
HTTP	✔	✔	✔	✔	✔	✔	✘
HTTPS	✔	✔	✔	✔	✔	✔	✘
Telnet	✔	✘	✘	✘	✘	✘	✘
SSH	✘	✘	✘	✘	✘	✘	✘

圖 27-5 介面狀態

說明：

1. 【系統開機歷時】：MHG-2000 開機歷時。
2. 【系統連線數目】：顯示目前通過 MHG-2000 建立的連線數。
3. 【模式】：為該網路介面的連線模式。
4. 【外部網路連線狀態】：顯示該外部網路介面的連線狀態。
5. 【網路頻寬（上傳/下載）Kbps】：顯示該外部網路介面所能使用的最大下載 / 上傳頻寬（為系統管理員在【網路介面】>【介面位址】頁面中，設定的外部網路介面頻寬）。
6. 【下載流量比例】：MHG-2000 依照各外部網路介面的流量，所分配的下載比例。
7. 【上傳流量比例】：MHG-2000 依照各外部網路介面的流量，所分配的上傳比例。
8. 【連線歷時】：當外部網路介面的連線模式為撥號連線 / 動態 IP 位址時，會於此欄位顯

示其連線歷時。

9. 【MAC 位址】：該網路介面之 MAC Address。

10. 【IPv4 位址 / 子網路遮罩】：為該網路介面之 IPv4 位址與網路遮罩設定。

11. 【IPv4 預設閘道】：顯示該外部網路介面之 IPv4 通訊閘道位址。

12. 【IPv6 位址 / 首碼長度】：為該網路介面之 IPv6 位址與首碼長度設定。

13. 【IPv6 預設閘道】：顯示該外部網路介面之 IPv6 通訊閘道位址。

14. 【DNS 伺服器 1】：外部網路介面可用來解析網域名稱的主要 DNS 伺服器。

15. 【DNS 伺服器 2】：外部網路介面可用來解析網域名稱的次要 DNS 伺服器。

16. 【接收封包數（成功/錯誤）】：顯示該介面所接收之正常、錯誤封包數。

17. 【傳送封包數（成功/錯誤）】：顯示該介面所傳送之正常、錯誤封包數。

18. 【Ping/Tracert / HTTP / HTTPS / Telnet / SSH】：顯示使用者能否從該網路介面 Ping/Tracert 到 MHG-2000；或是透過 HTTP、HTTPS、Telent、SSH 協定登入其 UI。

27.2 系統效能

步驟1. 在【監控報告】>【系統狀態】>【系統效能】頁面中，可顯示目前或指定日期的 MHG-2000 系統 CPU、記憶體使用狀況之相關訊息：（如圖 27-6）

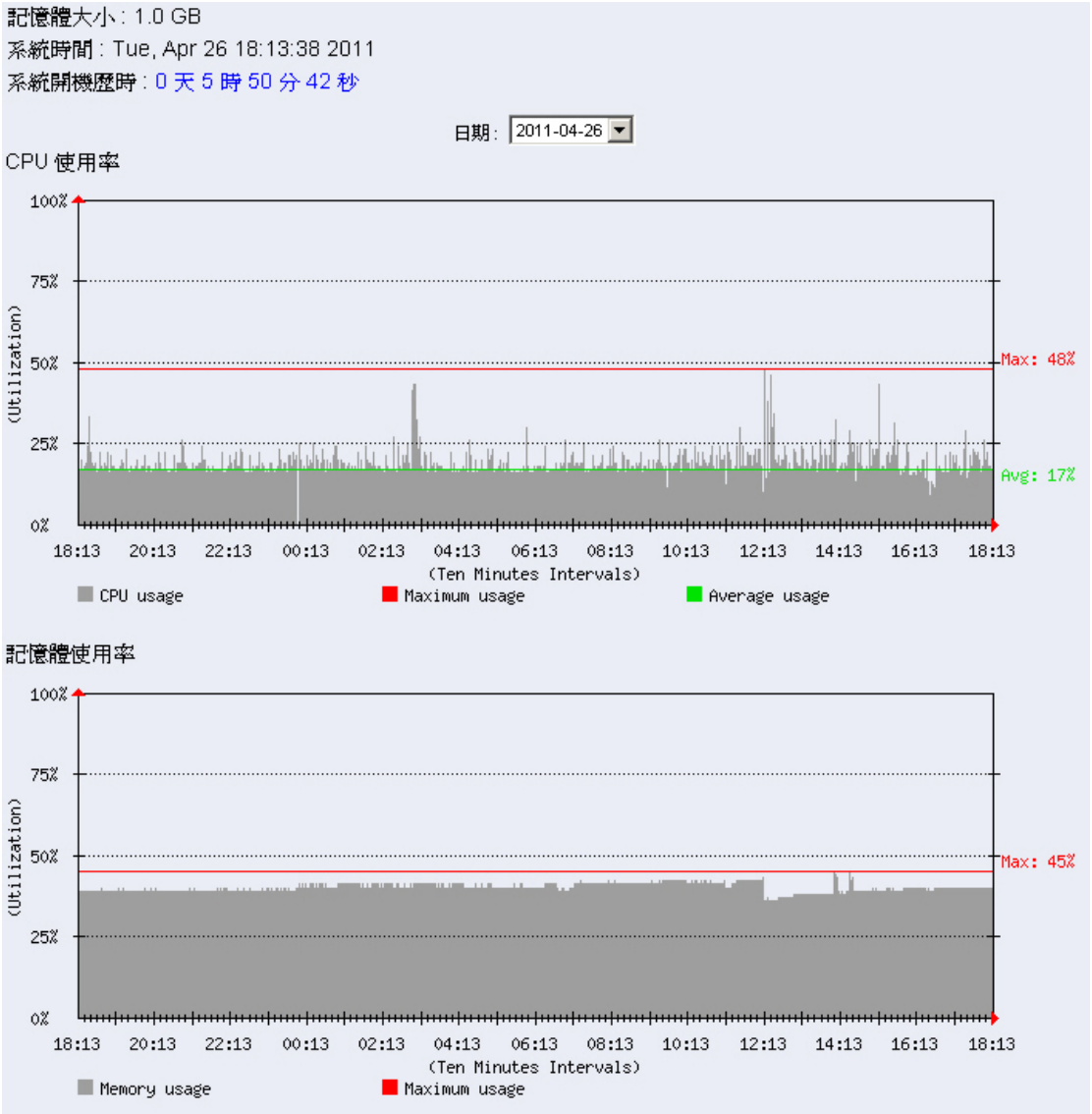


圖 27-6 系統資源使用狀態

27.3 認證狀態

步驟1. 在【監控報告】>【系統狀態】>【認證狀態】頁面中，會顯示目前 MHG-2000 認證機制之相關訊息：（如圖 27-7）

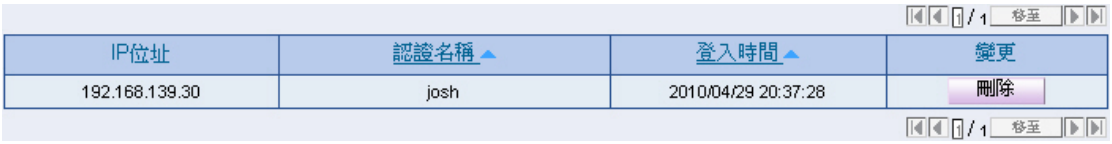


圖 27-7 認證狀態

說明：

1. 【IP 位址】：認證使用者 IP 位址。
2. 【認證名稱】：認證使用者採用的認證帳號。
3. 【登入時間】：使用者進行認證的起始時間。(年/月/日 時/分/秒)。

27.4 ARP 表

步驟1. 在【監控報告】>【系統狀態】>【ARP 表】頁面中，可顯示在 IPv4、IPv6 網際協定下，目前透過或與 MHG-2000 建立連線之設備的 NetBIOS 名稱、IP 位址、MAC 位址和所屬網路介面之相關訊息：（如圖 27-8）

圖 27-8ARP 表

說明：

1. 【NetBIOS 名稱】：該設備之網路識別名稱。
2. 【目前 IP 位址】：該設備之網路 IP 位址。
3. 【MAC 位址】：該設備之網路卡識別號碼。
4. 【介面】：該設備所屬網路介面。
5. MHG-2000【靜態】ARP 表功能和提供的【ARP 防偽程式】，必須同時搭配使用，可分別綁定 MHG-2000 和用戶端彼此的 IP 及 MAC 位址對應，避免內部代回封包導致的網路異常情形。
6. 從 MHG-2000 下載【ARP 防偽程式】後：（如圖 27-9）
   - 可立即執行，使其生效。（如圖 27-10）
   - 將其複製到開機磁碟的 \Documents and Settings\All Users\開始功能表\程式集\啟動 目錄下，於每次開機時自動執行。（如圖 27-11）

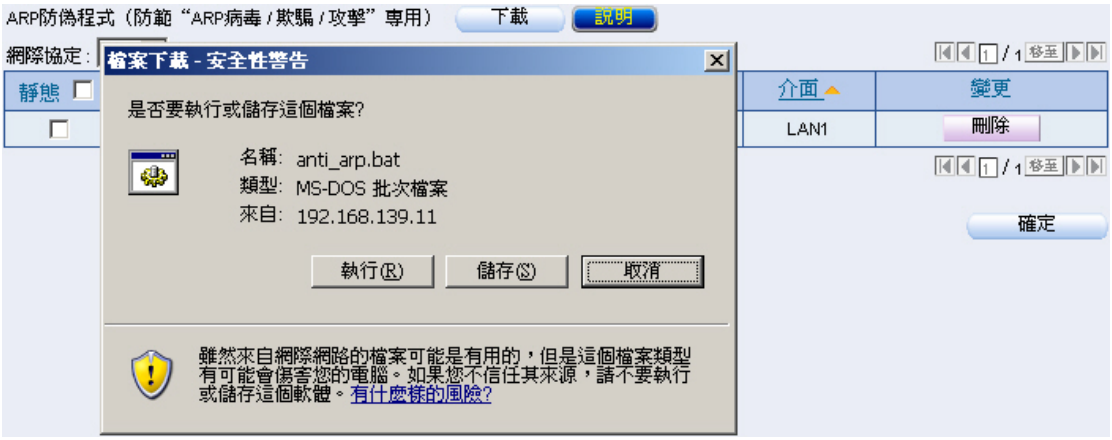


圖 27-9 下載 ARP 防偽程式

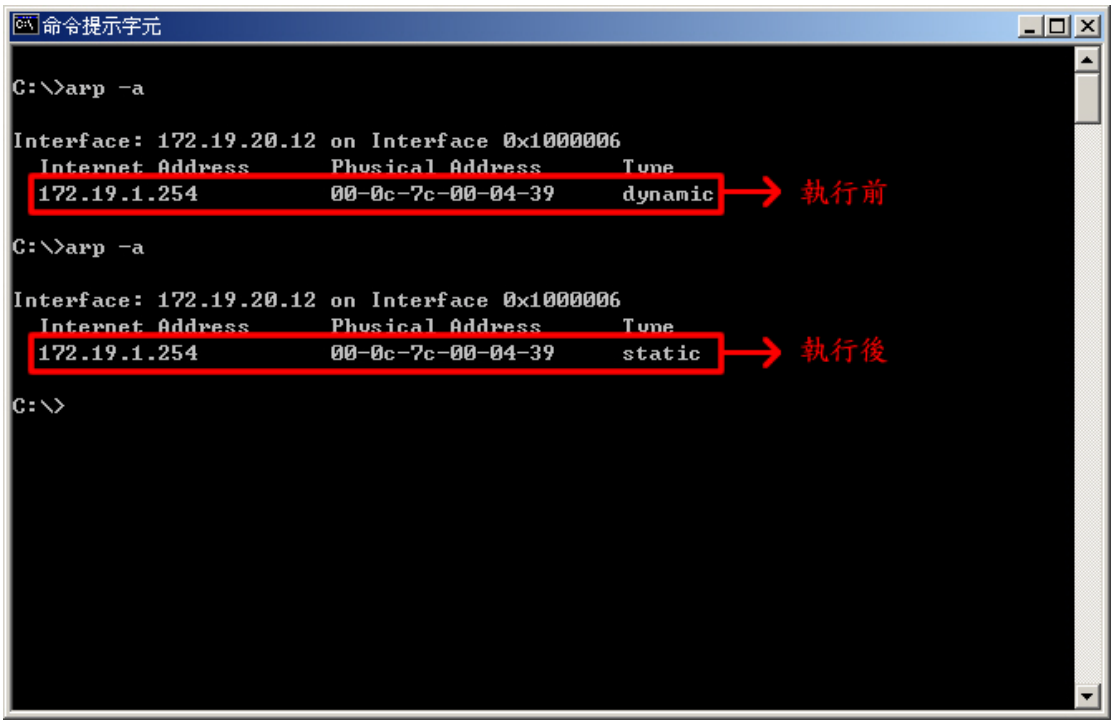


圖 27-10ARP 防偽程式執行結果

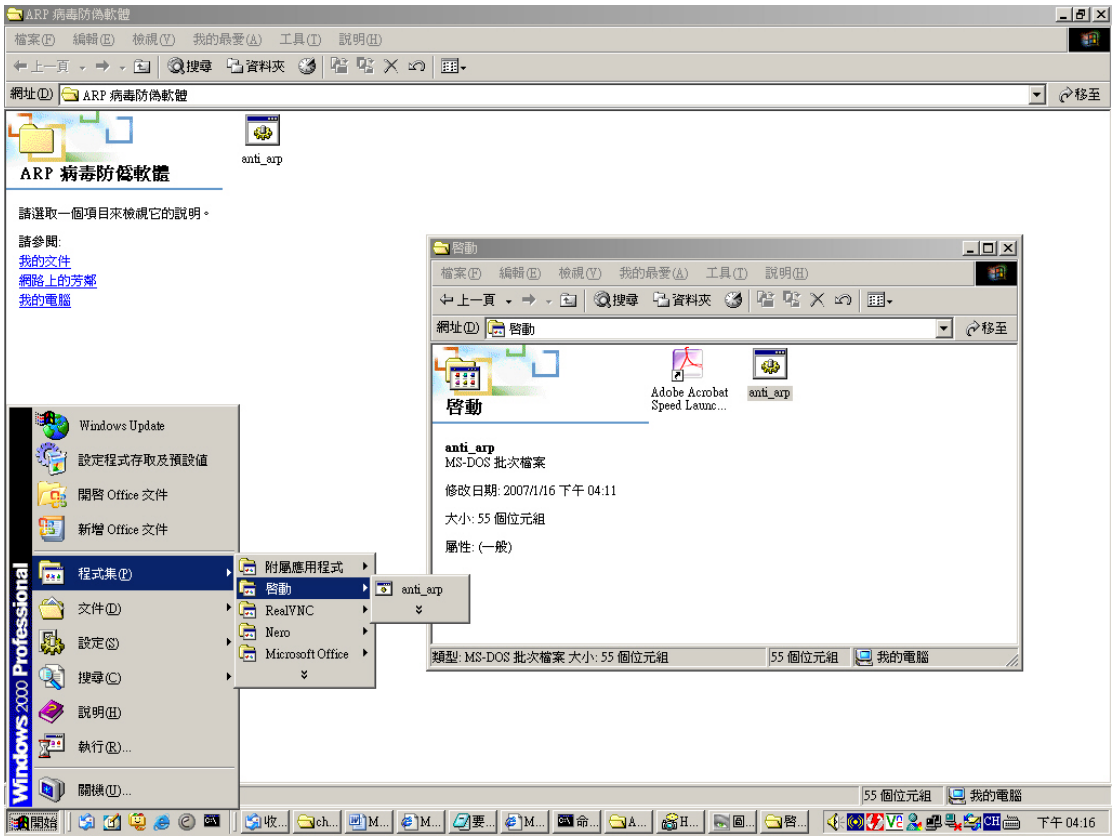


圖 27-11 開機自動執行 ARP 防偽程式

27.5 連線狀態

步驟1. 在【監控報告】>【系統狀態】>【連線狀態】頁面中，可顯示在 IPv4、IPv6 網際協定下，目前透過 MHG-2000 管制條例傳輸封包的連線：（如圖 27-12）

- 點選【來源位址】連結，可顯示其存取網路資源時，透過之埠號和所使用之流量。（如圖 27-13）

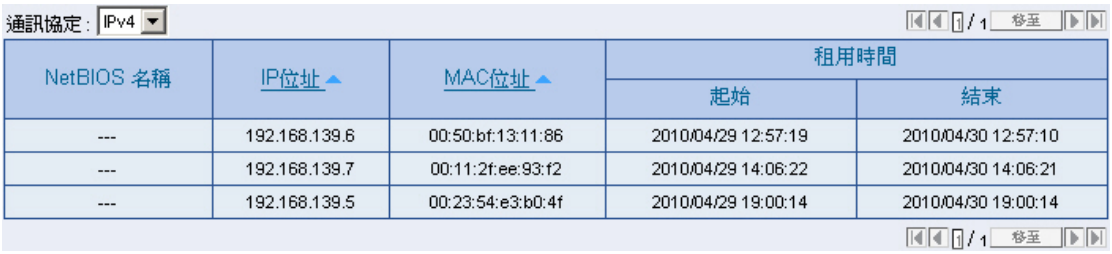
圖 27-12 系統連線狀態

通訊協定	連線資料	起始時間	流量	管制條例方向
TCP	Original: 192.168.139.118:5105 -> 74.125.153.19:443 Reply: 74.125.153.19:443 -> 114.37.89.247:5105	21:03:24	10.5 KB	2
TCP	Original: 192.168.139.118:5104 -> 60.199.252.160:80 Reply: 60.199.252.160:80 -> 114.37.89.247:5104	21:03:18	8.2 KB	2
TCP	Original: 192.168.139.118:5103 -> 72.14.203.100:80 Reply: 72.14.203.100:80 -> 114.37.89.247:5103	21:03:18	1.9 KB	2
TCP	Original: 192.168.139.118:5101 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5101	21:03:17	3.1 KB	2
TCP	Original: 192.168.139.118:5099 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5099	21:03:17	2.4 KB	2
TCP	Original: 192.168.139.118:5100 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5100	21:03:17	2.4 KB	2
TCP	Original: 192.168.139.118:5102 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5102	21:03:17	7.4 KB	2
TCP	Original: 192.168.139.118:5098 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5098	21:03:16	2.3 KB	2
TCP	Original: 192.168.139.118:5097 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5097	21:03:16	5.8 KB	2
TCP	Original: 192.168.139.118:5096 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5096	21:03:16	5.0 KB	2
TCP	Original: 192.168.139.118:5092 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5092	21:03:16	10.5 KB	2
TCP	Original: 192.168.139.118:5095 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5095	21:03:16	2.3 KB	2
TCP	Original: 192.168.139.118:5093 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5093	21:03:16	20.1 KB	2
TCP	Original: 192.168.139.118:5094 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5094	21:03:16	5.1 KB	2
TCP	Original: 192.168.139.118:5091 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5091	21:03:16	20.0 KB	2
TCP	Original: 192.168.139.118:5089 -> 74.125.153.104:80 Reply: 74.125.153.104:80 -> 114.37.89.247:5089	21:03:14	69.3 KB	2
TCP	Original: 192.168.139.118:5090 -> 60.199.252.179:80 Reply: 60.199.252.179:80 -> 114.37.89.247:5090	21:03:14	4.5 KB	2
TCP	Original: 192.168.139.118:5088 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5088	21:03:13	20.2 KB	2
TCP	Original: 192.168.139.118:5085 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5085	21:03:13	14.9 KB	2
TCP	Original: 192.168.139.118:5087 -> 60.199.252.155:80 Reply: 60.199.252.155:80 -> 114.37.89.247:5087	21:03:13	266.9 KB	2

圖 27-13 系統連線過濾頁面

27.6 DHCP 用戶表

步驟1. 在【監控報告】>【系統狀態】>【DHCP 用戶表】頁面中，記錄在 IPv4、IPv6 網際協定下，MHG-2000 內建的 DHCP 伺服器配發 IP 之情況：（如圖 27-14）


通訊協定： IPv4 1 / 1 移至

NetBIOS 名稱	IP位址	MAC位址	租用時間	
			起始	結束
---	192.168.139.6	00:50:bf:13:11:86	2010/04/29 12:57:19	2010/04/30 12:57:10
---	192.168.139.7	00:11:2f:ee:93:f2	2010/04/29 14:06:22	2010/04/30 14:06:21
---	192.168.139.5	00:23:54:e3:b0:4f	2010/04/29 19:00:14	2010/04/30 19:00:14

1 / 1 移至

圖 27-14 DHCP 用戶表

說明：

1. 【NetBIOS 名稱】：接受 MHG-2000 配發 IP 的設備之網路識別名稱。
2. 【IP 位址】：MHG-2000 所配發給該設備之動態 IP 位址。
3. 【MAC 位址】：該動態 IP 位址所對應之 MAC 位址。
4. 【租用時間】：該動態 IP 位址之有效時間(起始 / 結束時間)（年/月/日/時/分/秒）。

27.7 主機資訊

步驟1. 在【監控報告】>【系統狀態】>【主機資訊】頁面中，可顯示在 IPv4 網際協定下，通過 MHG-2000 的連線 IP 位址和其對應 NetBIOS、DNS 名稱資訊。**（如圖 27-15, 圖 27-16）**

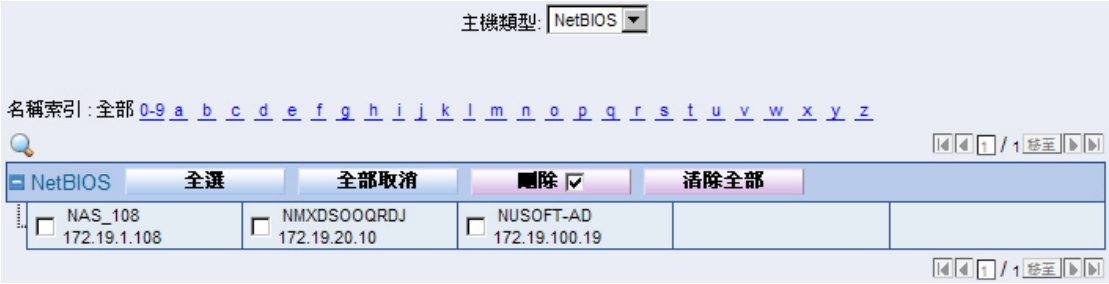


圖 27-15NetBIOS 主機列表

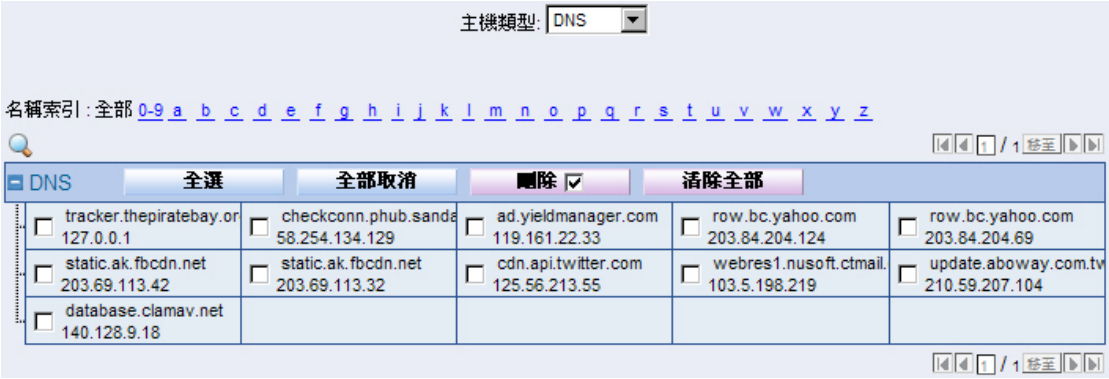


圖 27-16 DNS 主機列表