禾翔資訊股份有限公司

多功能防火牆設備 HSecurity+

V2.1.5 使用手冊

WWW.HERHSIANG.COM

目　　錄

第零章 安裝與訊息

HSecurity+硬體外部介面說明 (圖 0-1)：

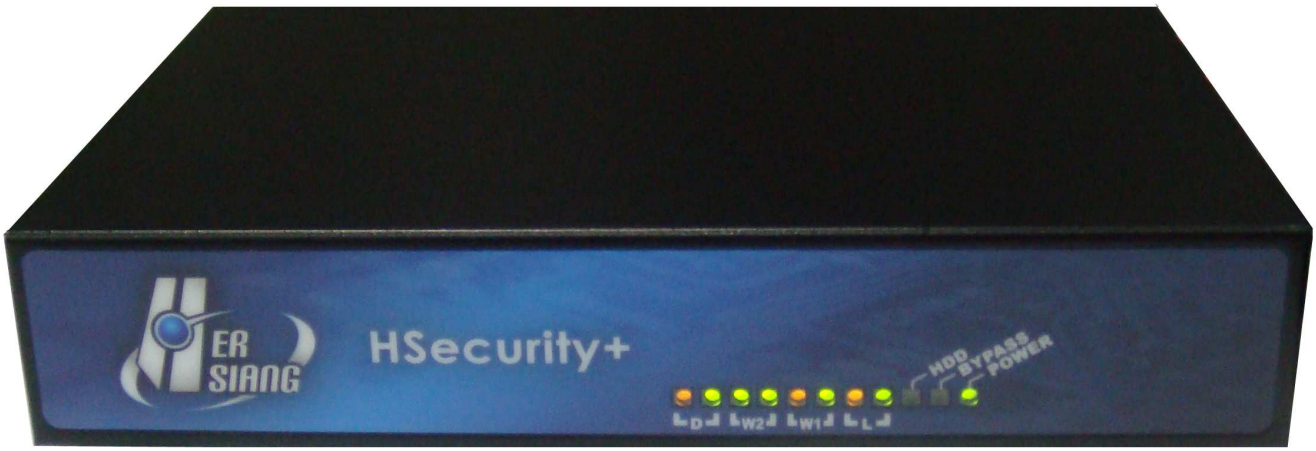

圖 0-1 HSecurity+接孔、指示燈說明

- Power LED：電源顯示，主機的電源供應正常，它會恆亮。
- HDD LED：當電源開啟後，LED 燈會頻繁地閃爍，表示系統正在開機狀態，約 2 分鐘後系統開機程式結束，當 LED 停止頻繁地閃爍，進入不規則的閃爍狀態，表示系統已開機成功。
- LAN ：內部網路介面，將企業內部的網路連結在此網路。
- WAN 1/2：外部網路介面 1 / 2，與外部路由器連結。
- DMZ ：非軍事區網路介面，將企業內的伺服器連結在此網路。

0-1、建議的安裝設定圖

建議的安裝設定圖如(圖 0-2)：

圖 0-2 建議的網路安裝設定圖

- 內部埠【LAN 】= 192.168.1.1
- 外部埠 1【WAN 1】= 211.22.22.22 (Gateway 211.22.22.254，Mask 255.255.255.0)
- 外部埠 2【WAN 2】= PPPoE (PPPoE 帳號及密碼)
- 非軍事區埠【DMZ，NAT 模式】=172.16.1.1

0-2、軟體安裝設定

內部網路設定

步驟1. 首先將管理員的電腦和 HSecurity+的 LAN 介面接到同一個 Hub 或 Switch，再使用瀏覽器 (IE 或 FireFox) 進入 HSecurity+ 的管理介面。

HSecurity+ LAN 的 IP 地址預設值為 http://192.168.1.1，所以管理員電腦的 IP 位址必須是 192.168.1.2 至 192.168.1.254 其中之一，子網路遮罩為 255.255.255.0。

步驟2. 瀏覽器會詢問使用者名稱及密碼，輸入管理員名稱與密碼。(圖 0-3)

- 使用者名稱：admin
- 密碼：admin
- 點選【確定】

圖 0-3 鍵入使用者名稱與密碼

步驟3. 預設的管理介面是英文，到 [Configuration >> Language] 將操作畫面改成 Traditional Chinese，按下『Save』後系統會自動更換成中文環境。(圖 0-4)

圖 0-4 選擇操作語系

步驟4. 設定新的內部網路介面位址，如果新的網路環境的 IP 網段不是預設的 192.168.1.0/24，要先更換 HSecurity+ 的 LAN IP 位址，例如，將內部網路介面位址改為 172.16.16.254/24，系統會重新啟動內部網路卡位址。

此時，管理員必須更改電腦端的 IP 位址為：172.16.16.2 至 172.16.16.254 中的任何一個 IP 位址，管理員的電腦或許需要重新開機，新的 IP 位址才能生效。再以新的 IP 位址 (172.16.16.254) 重複『步驟 2』，進入管理介面。

步驟5. 進入 HSecurity+的畫面後，在左方的主功能選項中，點選【網路介面及路由】中的【網路介面】，再點選【內部網路】功能選項。（圖 0-5）

IP 地址：預設值為 192.168.1.1，可以改成任何 IP 位址，IP 改好之後，再以新的 IP 位址進入管理介面。

圖 0-5 輸入內部網路 IP 位址與子網路遮罩

- 網路遮罩：預設值為 255.255.255.0
- 上傳速度：單位為 Kbps ，如果是 100M 的網路可以設成 102400 Kbps，如果是 1Gbps，可以設成 1024000 Kbps。
- 下載速度：單位為 Kbps ，如果是 100M 的網路可以設成 102400 Kbps，如果是 1Gbps，可以設成 1024000 Kbps。
- MAC 位址：可以依照狀況更改。
- 按下『儲存』按鍵後，設定的數值就會生效。

步驟6. 選擇是否啟動 ARP 防偽(圖 0-6)

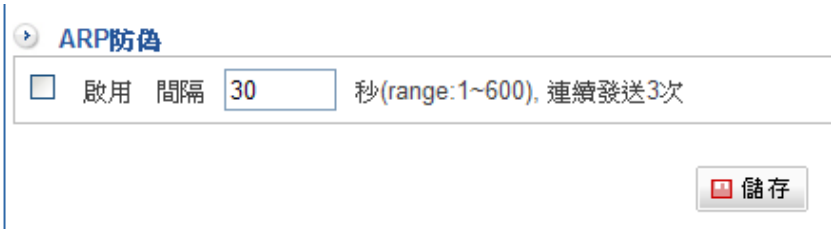

圖 0-6 啟用 APR 防偽攻擊

- 按下『儲存』按鍵後，設定的數值就會生效。

外部網路設定

步驟1. 進入 HSecurity+ 的畫面後，在左方的主功能選項中，點選【網路介面及路由】中的【網路介面】，再點選【外部網路_1】功能選項。（圖 0-6）

圖 0-6 外部網路介面設定

- 介面名稱-eth1：輸入一個可供辨識外部網路名稱，可以是任何中英文文字，例如『中華電信』、『中華光纖』。
- 連線模式：系統支援 3 種連線模式

  1.Static：固定 IP 位址。

  2.DHCP：自動從 ISP 取得 IP 位址

  3.PPPoE：PPPoE 連線。
- IP 地址：依照不同的連線模式設定，只有在『Static』模式下才需要自訂 IP 位元址，在 DHCP 及 PPPoE 模式下都會由電信業者主動配發，不需要設定。
- 網路遮罩：預設值為 255.255.255.0，在 DHCP 及 PPPoE 模式下都會由電信業者主動配發，不需要設定。
- 預設閘道：依照不同的連線模式設定，只有在『Static』模式下才需要設定預設閘道的 IP 位址，在 DHCP 及 PPPoE 模式下都會由電信業者主動配發，不需要設定。
- MAC 位址：可以依照狀況更改。
- 上傳速度：依照電信業者給的線路速度設定，系統預設值 64Kbps、128Kbps、256Kbps、512Kbps、1Mbps、2Mbps、3Mbps、10Mbps、100Mbps，管理者也可選擇自訂，單位為 Kbps。
- 下載速度：依照電信業者給的線路速度設定，系統預設值 64Kbps、128Kbps、256Kbps、512Kbps、1Mbps、2Mbps、3Mbps、10Mbps、

100Mbps，管理者也可選擇自訂，單位為 Kbps。

- 負載分配模式：『自動分配』依照設定的上、下傳速度，自動分配負載。『手動分配』依照管理者的需求，分配流量。亦可使用來源 IP 分配、目的分配。
- 按下『儲存』按鍵後，設定的數值就會生效。

步驟2. 線路偵測設定（圖 0-7）

- 可採 DNS、ICMP 或不偵測 3 種模式，設備依照測試的數值，判斷線路斷線與否，如果選擇的是 DNS、ICMP 都需要填入測試目標的 IP 位址，必須要確認測試目標 IP 位址會回應 DNS 或是 ICMP。
- 設定啟用的管理服務：計有 PING、HTTP 與 HTTPS 三種模式，如果希望更改預設的埠號，則需到 共同設定 中更改。

圖 0-7 線路偵測設定方式

步驟3. 防火牆防護設定

- 防護項目計有 SYN、ICMP、UDP 和 PortScan。（圖 0-8）

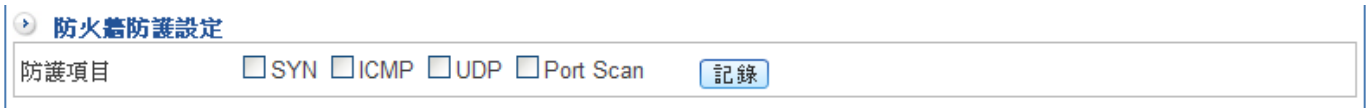

圖 0-8 防火牆防護項目

- 並可瀏覽防護記錄，點選旁邊『紀錄』的按鈕，就會列出這個網路介面遭受駭客攻擊的時間、方法等攻防紀錄。（圖 0-9）

圖 0-9 防火牆防護紀錄

步驟4. 共同設定：外部網路_1：（圖 0-10）

- DNS Server1：線路的 DNS 伺服器 IP 位址，預設是 168.95.1.1。
- DNS Server2：線路的 DNS 伺服器 IP 位址，預設是 168.95.192.1。
- HTTP：HTTP 管理的埠號，預設是 80。
- HTTPS：HTTPS 管理的埠號，預設是 443。
- 偵測間隔時間：偵測線路的間隔時間，預設是 3 秒
- 管理介面閒置多久自動斷線：當管理者沒有操作 WEB 介面，超過多少時間，管理介面會自動關閉，預設是 60 分。
- 按下『儲存』按鍵後，設定的數值就會生效。

圖 0-10 鍵入共同設定資料

步驟5. 當將內部網路與外部網路設定完成時，即表示安裝成功。最後將內部所有電腦的 IP 位址須設定為 HSecurity+內部網路介面的同一個網域與預設閘道設定為 HSecurity+內部網路介面，或將內部的電腦設為自動取得 IP，內部網路可馬上連結至網際網路存取資料，

系統預設的管制動作是『內部到外部全開放』，只要外部網路一通，所有人都可以上網，如欲使用 HSecurity+的管制功能，請在【管制條例】和【管制目標】功能中設定。

0-3、首頁訊息

登入 HSecurity+ 的畫面後，系統會提供豐富的訊息，讓管理者清楚，目前設備的運作狀況。

系統時間及伺服器系統資源

顯示目前設備的時間及時區，甚至是開機時間，同時也顯示設備目前的 CPU、RAM、Flash 等使用量。(圖 0-11)

系統時間		
伺服器日期 / 時間	2012-03-15	10:37:04
現在時區	Asia/Taipei	
伺服器開機時間	1 days,2 hours,10 minutes	

伺服器系統資源		
CPU 使用率/系統平均負載	18.2%	0.00 0.03 0.01
記憶體 (使用量/全部) MB	21%	1,030.4
Flash (使用量/全部) MB	17%	182

圖 0-11 系統時間及資源

HSecurity+ 的版本及開啟的服務如下圖，  ：代表服務正常，  ：代表服務每有啟用或無法順利運作。（圖 0-12）

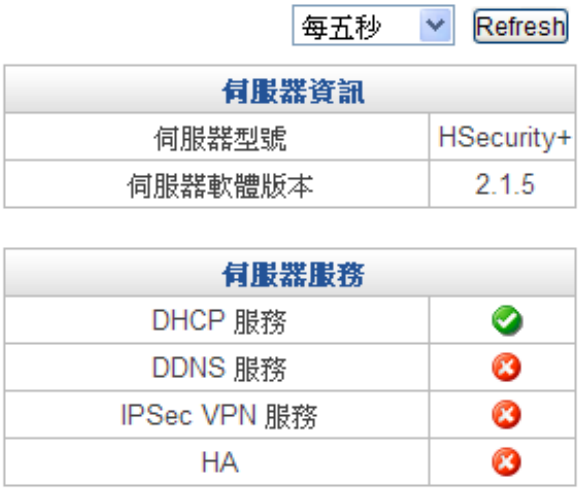

圖 0-12 系統服務狀態

管理者登入名稱、IP 位址及同時間有多少人登入等訊息，也可以設定多久時間將首頁的訊息自動更新一次。可自動設定系統更新的時間，每五秒、十秒、二十秒、三十秒自動更新一次。（圖 0-13）

圖 0-13 管理員登入狀況

網路介面

HSecurity+ 的詳細網路介面訊息：（圖 0-14）

- 【實際介面】：系統實際抓到的網路介面名稱。
- 【連線狀態】：網路是否暢通，  ：代表線路暢通，  ：代表線路斷線。
- 【線路】：實體網路介面是否有接上，  ：代表沒接線，  ：代表連線。。
- 【IP 位址】：系統綁定的 IP 位址。
- 【總封包量】：每個網路介面傳送、接收的封包量。
- 【總傳輸量】：每個網路介面傳送、接收的流量，以 Bytes 為單位。

網路介面 » More					
名稱		LAN	WAN1	WAN2	DMZ
實際介面		eth0	eth1	eth2	eth3
連線狀態					
線路					
IP 位址		192.168.1.1	192.168.168.155	OFF	OFF
總封包量	Tx	10,720	7,380	0	0
	Rx	8,179	11,338	0	0
總傳輸量 (byte)	Tx	8.63M	862K	0	0
	Rx	1.09M	7.75M	0	0

圖 0-14 系統服務狀態

第一章　系統設定

系統設定的名詞解釋

系統設定，是指 HSecurity+運作時必須的基本設定，在本單元中則有時間設定、管理員、備份和升級、套件管理、語系、訊息通知與資料匯出及掛載。

【時間設定】名詞解釋

時區與時間

可自行設定系統的時區及時間，將 HSecurity+的系統時間與時區設定成當地的時間或是外部時間伺服器的時間同步化。

網路時間校定

將 HSecurity+系統的時區及時間與網際網路上的時間伺服器同步化。

1-1、時間設定

設定時間與日期

步驟1. 手動設定時區及時間

自行設定時區與時間，輸入時區、時間與日期，再按下儲存。（圖 1-1）

步驟2. 網路時間校正

勾選【網路時間校定】，選定採用獨立公開伺服器或者自訂時間伺服器，系統會每 30 分鐘跟時間伺服器校正一次，並將校正過的資料顯示在【時區與時間】中。

立即更新：如果需要馬上校正時間，可以按下『立即更新』按鈕，系統會立刻跟設定的時間伺服器校正資料。

時間記錄：按鈕會顯示系統跟時間伺服器的校正資料，所有的資料會保留 3 天。

圖 1-1 系統時間設定

1-2、管理員

【管理員】名詞解釋

HSecurity+是全功能的 多功能防火牆系列，它包含 管制條例、個人流量分析紀錄等機密等級的資料，如何避免同一個人的管理弊病呢 ？自定義的管理者介面就是最好的答案。

設想一下幾個運作的情況

1.某位管理者只能管理 VPN 的操作，例如 VPN 通道的建立，管制等，至於其他功能就不方便讓他知道太多。

2.稽核人員可以進入 多功能防火牆 中詢紀錄下來的資訊。

按照傳統的管理介面，要達成上述的功能幾乎不可能，但是藉由" 自定義的管理者介面" 就可以輕鬆達到。

管理者帳號及權限

admin 為 HSecurity+預設之系統主管理員名稱，無法刪除，其他管理員名稱則可刪除與變更。

註 1：HSecurity+預設之系統管理員**帳號：admin　　密碼：admin**。

註 2：預設之系統主管理員，可新增或修改其他管理員為主管理員或次管理員，亦可由其他主管理員更改其權限為次管理員。系統管理員無論如何配置，HSecurity+一定會強制保留一個主管理員的設定。

權限

主管理員權限為【讀/寫】，它可以新增和刪除次管理員。

【Read】：具有瀏覽功能，沒有寫入的權限，管理者可自訂瀏覽的功能項目。

【Write】：具有寫入、瀏覽功能，管理者可自訂讀寫的功能項目。

【All Privileges】：具有寫入、瀏覽功能，不能自訂讀寫功能選項。

系統設定

為了方便管理者管理多據點(分公司)設備，可自行設定主機名稱、登入標題、首頁標題、瀏覽器標題與 LOGO 圖示，讓網管人員可以在第一時間立即掌握。

清除記憶體

系統會依設定時間來檢查設備記憶體使用率狀況，當使用率超過比率時會自動清除已關閉的程式佔用記憶體空間。

Pass-through Protocol

開啟此功能後，所有經過 HSecurity+傳輸的 SIP 或者 H-323 封包，都會被處理後再送出。

恢復出廠設定值

清除所有設備裡面資料與設定，回到最初原始設備狀態。管理者可自行設定是否要保留網路介面設定與格式化硬碟。

管理者的 IP 位址

限定特定的 IP 位址才能進入管理系統。

紀錄清除

HSecurity+硬碟容量空間有限，管理者可自行清除特定服務紀錄保留的時間。目前可自行設定清除的項目計有系統設定(時間更新紀錄、訊息通知記錄)、網路介面及路由(PPPOE 撥接紀錄)、管制條例(LAN 的管制封包追蹤紀錄、DMZ 的管制封包追蹤紀錄、WAN 的管制封包追蹤紀錄)、管理目標(防火牆功能防護紀錄、上網認證記錄)、網路服務(DDNS 更新紀錄)、、VPN(IPSec Tunnel 紀錄、PPTP 伺服器紀錄、PPTP Client 紀錄)、日誌(日誌紀錄)。

SMTP 伺服器設定

可以針對特定的網域寄送清單郵件。

1-2-1、帳號管理

Read、(閱讀)帳號管理權限

步驟1. 在【管理員】設定視窗中，點選螢幕下方【新增】功能按鈕。

步驟2. 在【新增次管理員】視窗中，鍵入以下資料：（圖 1-2）

- 【帳號】：read、【密碼】：1013。
- 【密碼檢測】：系統會自動幫您判別密碼強度，要想讓您使用的密碼更安全可以利用下面幾種方式：

  1.使用字母和數字

  2.使用特殊字元(但是冒號與逗號禁止使用)

  3.混合使用大小寫
- 【密碼確認】：系統需要您再次輸入設定的密碼，避免您欲設定的密碼與輸入的字元有誤。
- 【註解】：次管理者方便辨識及記憶的描述。
- 【權限】：設定 read 的權限。
- 勾選【自訂化選單】功能，可自行設定此管理者能使用功能的權限有哪些？

步驟3. 點選【新增】鈕以登錄使用者。

圖 1-2 新增 Read 次管理員

步驟4. 重新登入管理介面，以 read 帳號、密碼登入。(圖 1-3)

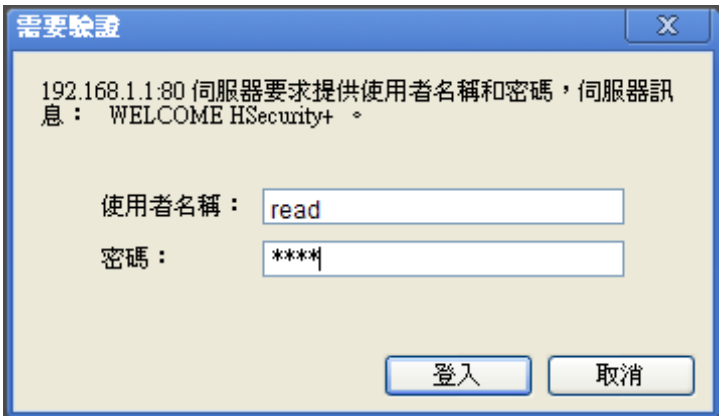

圖 1-3 以 read 帳號、密碼登入

步驟5. 以 Read、(閱讀)權限登入後，只能瀏覽裡面設定檔資料，也就是沒有【新增】、【修改】、【刪除】的按鈕，無法針對條例或功能做設定。(圖 1-4)

圖 1-4 權限 read 瀏覽畫面

註：Read 次管理者具有閱讀權限，但是並沒有內容紀錄閱讀的權限

Write、(寫入)帳號管理權限

步驟1. 在【管理員】設定視窗中，點選螢幕下方【新增】功能按鈕。

步驟2. 在【新增次管理員】視窗中，鍵入以下資料：（圖 1-5）

- 【帳號】：write。
- 【密碼】：pw1013。
- 【密碼檢測】：系統會為您檢測密碼安全強度，可混合英文字母與數目字搭配，或使用特殊字元(如@，但逗號與冒號不能使用)。
- 【密碼確認】：pw1013。
- 【註解】：次管理者方便辨識及記憶的描述。
- 【權限】：設定 write 的權限。

步驟3. 點選【新增】鈕以登錄使用者。

圖 1-5 新增 Write 次管理員

步驟4. 重新登入管理介面，以 write 帳號、密碼登入。 **(圖 1-6)**

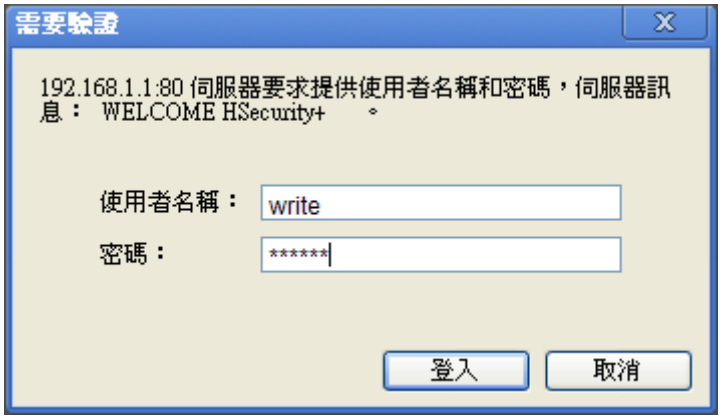

圖 1-6 以 write 帳號、密碼登入

步驟5. 以 Write、(寫入)權限登入後，可以設定條例與管制功能。**(圖 1-7)**

圖 1-7 權限 write 瀏覽畫面

All Privileges、(寫入)帳號管理權限

步驟1. 在【管理員】設定視窗中，點選螢幕下方【新增】功能按鈕。

步驟2. 在【新增次管理員】視窗中，鍵入以下資料：（圖 1-8）

- 【帳號】：All。
- 【密碼】：@it168。
- 【密碼檢測】：系統會為您檢測密碼安全強度，可混合英文字母與數目字搭配，或使用特殊字元(如@，但逗號與冒號不能使用)。
- 【密碼確認】：@it168。
- 【註解】：讀寫，次管理者方便辨識及記憶的描述。
- 【權限】：設定 All Privileges 的權限。
- 勾選【自訂化選單】會自動開啟所有管控功能，無法自訂。

圖 1-8 新增 All Privileges 次管理員

步驟3. 重新登入管理介面，以 All 帳號、密碼登入。(圖 1-9)

圖 1-9 以 All 帳號、密碼登入

步驟4. 以 All(寫入)權限登入後，管理權限與 admin 相同。(圖 1-10)

圖 1-10 All 管理權限

1-2-2、系統設定

HSecurity+防火牆登入時名稱設定

HSecurity+的登入及 WEB 管理介面，都可以依照輸入的資料，改成管理者想要或是方便記憶的樣式。

範例：在【一般設定】視窗中，鍵入下列資料：（圖 1-11）

- 登入標題：HERHSIANG_FW。
- 首頁標題：禾翔資訊股份有限公司
- 瀏覽器標題：HSecurity+

圖 1-11 系統設定

2

重新登入管理介面時會出現登入標題已經被改成《HERHSIANG_FW》。（圖 1-12）

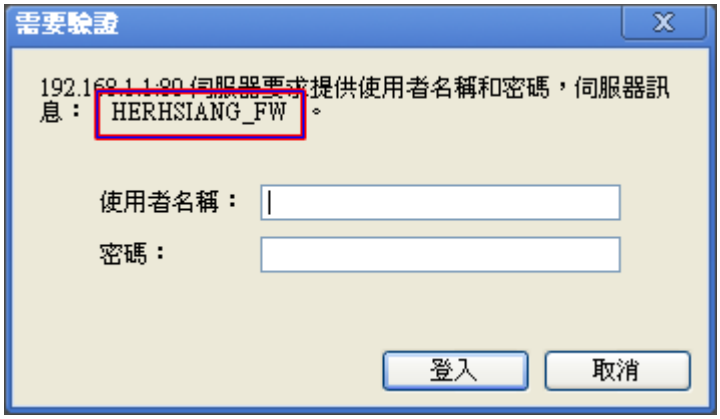

圖 1-12 登入標題顯示頁面

首頁標題已經被改成《禾翔資訊股份有限公司》。（圖 1-13）

圖 1-13 首頁標題顯示頁面

瀏覽器標題已經被改成《HSecurity+》。（圖 1-14）

圖 1-14 瀏覽器標題顯示頁面

更新 LOGO

上傳解析度為 154x54 pix 的 gif 圖檔，HSecurity+會自動將這個圖形放在設備的左上角。（圖 1-15）

圖 1-15 LOGO 顯示畫面

清除記憶體&Protocol Pass-Through

在 v7.10 版本之前，Herhsiang UTM 設備是每隔 60 分鐘，達到 90%才做記憶體空間釋放動作，現在開放讓管理者自行設定，最小值為 10 分鐘，比率最小需達 70%。

在使用網路電話時，若發生網路電話與多功能防火牆不合導致網路電話無法使用時，啟用 SIP/H323 protocol pass-through 可修正此問題。（圖 1-16）

圖 1-16 清除記體體設定畫面

註：H323 與 SIP 的差異比較表

通訊協定	H323	SIP
發展時間	較早	較晚
開發動機	節省電話費	彌補 H.323、MGCP 缺點
技術差異性	H.323 為較老舊的網路電話協定，雖然已升級到第六版,但仍舊建構在舊有的技術之上	SIP 為最新的 VoIP 通訊協定，開發起因為改善舊有技術的瓶頸和缺點
廠商進入門檻	低	較高
語音話質	較差	有品質控管機制來確保話質，較優
對公司員有網路的影響	會將網路速度減慢 50%，且對網路頻寬要求較多	可支援網路環境下各種不同 IP 型態，頻寬要求較小
系統當機時	所有安裝客戶均無法相互通話	客戶通話完全不受影響，一樣繼續保持暢通
容量限制	約僅能支援 300~500 個客戶	無容量限制，可以無上限地擴充
相容性	較難與以後微軟所推的 SIP 新協定相通	可以和 H.323、MGCP 協定相通，無被排擠的窘境

恢復出廠設定值和重新啟動系統

按下恢復出廠設定值旁的「確定恢復」按鈕，UTM 防火牆 UR-9 系列會清掉所有的設定值，並將 LAN IP 位址改為 192.168.1.1。

管理者可自行決定執行恢復出廠設定值時，是否保留網路介面設定與格式化硬碟當勾選保留網路介面設定，按下「確定恢復」鍵，則系統會保留目前網路介面資料，方便管理者遠端作業時可以利用原來的 IP 資訊登入系統。

按下重新啟動系統旁的「確定恢復」按鈕，系統會自動重新開機。(圖 1-20)

圖 1-17 恢復出廠預設值與重新啟動系統畫面

註：當勾選保留網路介面設定，在按「確定恢復」鍵，則系統在 reset 時候會保留目前網路介面設定資料。

1-2-3、管理者的 IP 位址

HSecurity+ 可以限制從網際網路進來管理介面的 IP 位址，預設是不限定來源，如果在【管理者的 IP 位址】中輸入特定的 IP 位址或範圍，對於不是屬於設定範圍內的連線要求，HSecurity+會通通拒絕，從內部網路來的連線則不受這個限制。

管理者的來源 IP 限制，預設是套用在外部網路介面上，從內部網路來的連線則不受這個限制，當【內部網路】、【非軍事區網路】的選項啟用時，來源 IP 的限制一樣會套用在這 2 個介面上。

進入到【管理員】之【管理者的 IP 位址】介面時，設定一個外部 IP 與網路遮罩。

- 設定註解為【MIS_HOME】。(圖 1-18)
- IP 與網路遮罩：設為 58.211.211.211/255.255.255.255(/32)。
- 按下「新增」鍵。

圖 1-18 新增外部 IP 管理者位址

- 完成設定，此時從外部連到管理介面只能透過 58.211.211.211 IP 位址。(圖 1-19)

圖 1-19 完成外部 IP 管理者 IP 位址設定

但是如果要限制只能有部分內部人員可以登入管理位址時，只要在新增加內部管理者的 IP 為址在套用來源網路設定值即可。

- 新增一筆內部管理者 IP 位址，註解輸入【MIS_IP】。(圖 1-20)
- 輸入【IP 與網路遮罩】：192.168.1.22/255.255.255.0(/32)。
- 按下「新增」鍵。

圖 1-20 設定內部管理者 IP 位址

- 完成設定。(圖 1-21)

圖 1-21 完成內部管理者 IP 位址設定

- 勾選「內部網路」，再套用來援網路設定值即可完成內部管理登入介面設定。(圖 1-22)

圖 1-22 套用來源網路設定值

註：當外部網路_1、外部網路_2 介面的 Http、Https 服務都關掉時，會導致無法從外面連進 HSecurity+的管理介面。

1-2-4、紀錄清除

為了節省 HSecurity+硬碟容量的空間，管理者可自行清除特定服務並設併內容紀錄的保存時間。

目前提供清除紀錄服務選項計有

系統設定(時間更新紀錄、訊息通知記錄)

網路介面及路由(PPPOE 撥接紀錄)

管制條例(LAN 的管制封包追蹤紀錄、DMZ 的管制封包追蹤紀錄、WAN 的管制封包追蹤紀錄)

管理目標(防火牆功能防護紀錄、上網認證記錄)

網路服務(DDNS 更新紀錄、異常 IP 分析記錄)

VPN(IPSec Tunnel 紀錄、PPTP 伺服器紀錄、PPTP Client 紀錄)、

日誌(日誌記錄)

內容記錄保存時間，可針對訊息通知記錄、防火牆防護紀錄、系統日誌紀錄，保存時間最長可達三年時間。(圖 1-23)


系統設定 > 管理員
帳號管理
系統設定
管理者的IP位址
記錄清除
SMTP 伺服器設定
記錄清除
全選
系統設定
時間更新記錄
訊息通知記錄
網路介面及路由
PPPOE 撥接記錄
管制條例
LAN 的管制封包追踪記錄
DMZ 的管制封包追踪記錄
WAN 的管制封包追踪記錄
管理目標
防火牆功能防護記錄
上網認證記錄
網路服務
DDNS 更新記錄
VPN
IPSec Tunnel 記錄
PPTP 伺服器記錄
PPTP Client 記錄
日誌
日誌記錄
清除
內容記錄保留時間設定
訊息通知記錄保留
12
個月
變更
防火牆防護記錄保留
12
個月
變更
系統日誌記錄保留
12
個月
變更

圖 1-23 紀錄清除畫面

1-2-5、SMTP 伺服器設定

Herhsiang UTM 為了讓管理者能更順手管控設備，提供多種人性化簡易工具，例如通知信件、放行信件...等，而 SMTP 伺服器設定功能就是方便網管人員操作運用的起始者。（圖 1-24）

- 寄件者：用戶名稱以登入 SMTP 伺服器；例如 mis@herhsiang.com
- 伺服器：SMTP 伺服器主機；例如 mail.herhsiang.com 或 58.211.211.211
- 帳號：使用者郵件帳號名稱，可以輸入帳號或是完整 email，例如 mis 或是 mis@herhsiang.com.tw
- 密碼：輸入使用者郵件帳號密碼，例如 123456
- 需要驗證：若你的伺服器需要認證，請勾選此格。
- TLS：依照郵件帳號登入的方式，選擇是否要啟動 TLS。TLS 是利用密鑰演算法在網際網路上提供端點身份認證與通訊保密
- 郵件寄送網域：選擇此封通知信函欲寄送的網域位址，例如：herhsiang.com.tw
- 資料設定完成，點選新增鈕。

圖 1-24 設定 SMTP 伺服器設定畫面

註 1：『郵件寄送網域』使用郵件放行與垃圾郵件清單時，若收件者的網域符合這項設定，會以這組設定寄送。若沒有符合的設定，會使用第一組設定寄送。

步驟1. 設定完成後，按下新增即完成建立。（圖 1-25）

圖 1-25 完成 SMTP 伺服器設定畫面

如果擔心設定資料有誤，無法順利收取到信件。Herhsiang 提供 SMTP 測試郵件功能，讓管理者在完成設定之後可以馬上進行驗證，以確認設定資料無誤。

步驟1. 按下測試鍵，輸入收件人郵件位址，例如 jean@sharetch.com.tw ，輸入完按下確定鈕。（圖 1-26）

步驟2. 寄件者信箱會收到一封主旨名稱為 This is a SMTP TestMail 的信件，代表您 SMTP 伺服器設定資料正確無誤。（圖 1-27）

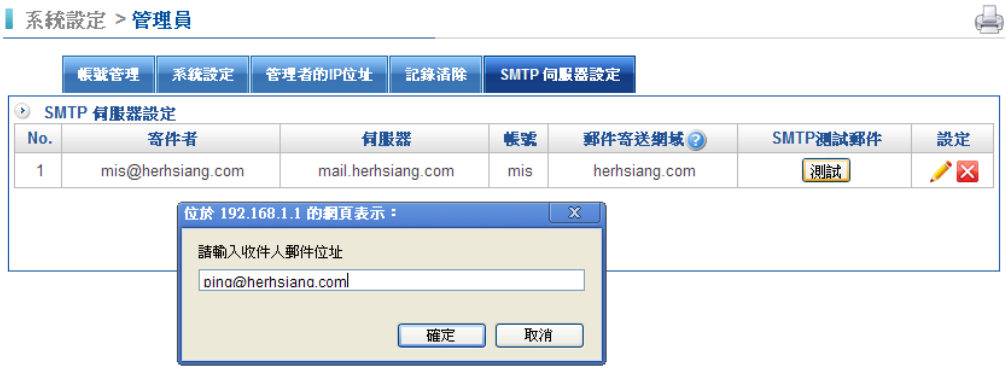

圖 1-26 測試 SMTP 伺服器

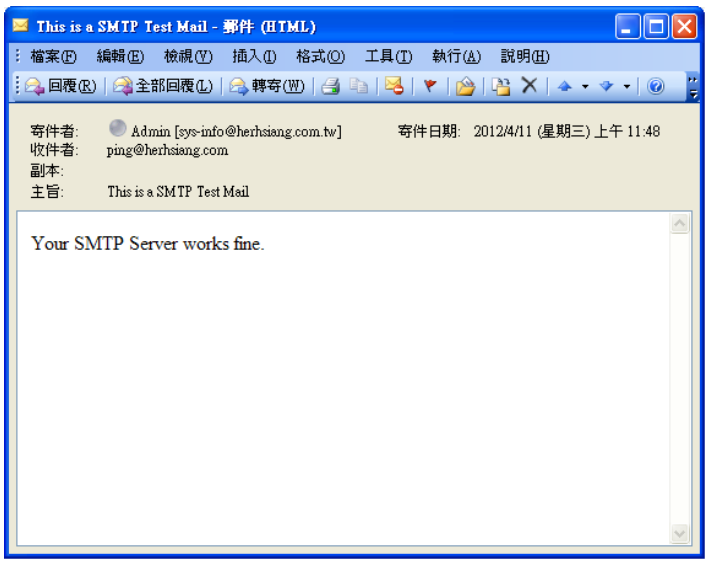

圖 1-27 SMTP 測試信件

1-3、備份和升級

【系統備份】名詞解釋：

系統備份

系統管理員可在此備份或匯入系統設定檔。

HSecurity+ 可以將所有的設定檔匯出，操作步驟如下。

軟體升級

從螢幕上【目前軟體版本】資訊中，獲知目前軟體使用版本的號碼。再經由瀏覽器到 Internet 取得最新軟體版本，並將更新軟體下載儲存至管理 HSecurity+多功能防火牆列之電腦硬碟中。

自動備份

管理者可依日期、時間備份設定檔，當有意外狀況發生時可快速還原至特定時間。

1-3-1、系統備份

系統備份

【系統備份】功能中，按下【備份】鍵，就可將目前系統之設定檔匯出。（圖 1-26）

圖 1-26 系統備份設定視窗

系統還原

輸入系統還原檔案路徑，選擇以前備份出來的備份檔，按下【更新】鍵，即可完成系統更新還原動作。（圖 1-27）

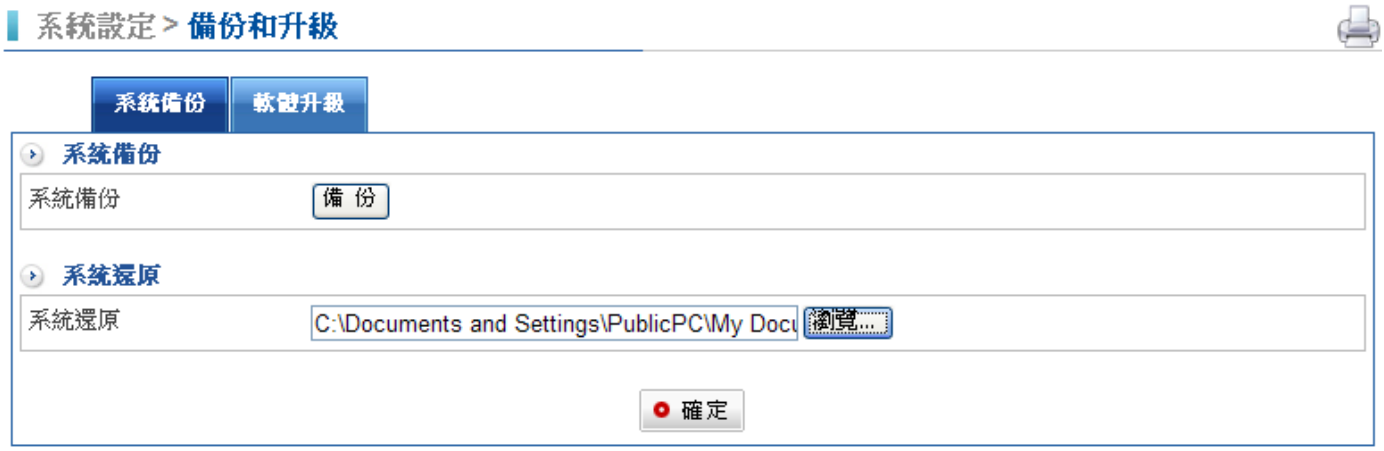

圖 1-27 系統還原設定視窗

1-3-2、軟體升級

軟體升級

到 www.herhsiang.com 的網站中下載 HSecurity+最新的韌體，再到【備份和升級】之【軟體升級】功能中，可依下列步驟更新韌體：

步驟1. 由螢幕上【首頁】資訊中，獲知目前韌體使用版本，再經由瀏覽器到 Internet 取得最新韌體版本，並將韌體下載至管理 HSecurity+的管理者電腦硬碟中。

步驟2. 點選【瀏覽】，於【選擇檔案】視窗中，選擇最新的韌體版本檔案名稱。

步驟3. 點選螢幕右下方【升級】功能按鈕，執行軟體自動更新升級。（圖 1-28）

圖 1-28 HSecurity+軟體更新

升級紀錄

有進行過更新動作後，軟體升級頁面會多出一個【升級紀錄】欄位，所有的歷史升級紀錄都會顯示在這個欄位中。

註：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、斷線或是離開網頁，這可能會造成 HSecurity+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）

1-4、語系

設定語言

HSecurity+ 支援 3 種語言版本，英文、繁體中文、簡體中文等。透過下列步驟可以選擇適當的語系，一旦選擇完畢，系統會立刻更新為選擇的語系。

【系統設定】之【語系】功能中，選擇欲使用之語言介面。按下【確定】鍵，就完成了。（圖 1-29）

圖 1-29 語言版本 WebUI 設定視窗

1-5、訊息通知

防火牆最怕的就是當斷線的時候，管理者是最後一位知道；或者是網路遭到攻擊卻不知道。為了讓管理者可以在第一時間掌控設備、網路訊息，HSecurity+提供訊息通知功能，不管是外部線路斷線、DDNS 更新失敗、SLB 主機偵測斷線、HA 狀態切換、防火牆攻擊防護(SYN,ICMP,UDP,PortScan)、系統操作日誌、管理者使用帳號,登入錯誤事件、上網認證,登入錯誤事件、軟體更新通知與自動備份系統設定檔，都可即時掌握。(圖 1-30)

圖 1-30 訊息通知

1-5-1、訊息通知

「訊息通知」，管理者只需選定 SMTP 伺服器設定中之寄件者帳號，並輸入收件者之完整 Email 帳號。

範例：在【訊息通知】視窗中，鍵入下列資料：（圖 1-31）

- 寄件者帳號：選定我們在『管理員』-『SMTP 伺服器設定』中所設定寄件者帳號，例如：mis@herhsiang.com。如果選擇自動方式，代表系統將偵測收件者的網域並選擇相對應網域的 SMTP 伺服器帳號寄出通知信，若無對應設定將以 SMTP 伺服器設定的第一筆帳號寄出，沒設定則不寄出。
- 收件者：輸入收件者帳號，多筆建立以隔行區隔。

圖 1-31 設定訊息通知項目

- 勾選需傳達的訊息事項，並可設定該事項信件主旨名稱。（圖 1-32）

選擇	項目	信件主旨
☐	1. 外部線路斷線	WAN disconnect
☐	2. DDNS更新失敗	DDNS fail
☐	3. SLB主機偵測斷線	SLB disconnect
☐	4. HA狀態切換	HA switch
☐	5. 防火牆攻擊防護 (SYN, ICMP, UDP, PortScan)	Firewall protection
☐	6. 系統操作日誌	Admin log
☐	7. 管理者使用帳號,登入錯誤事件	Admin login fail
☐	8. SSL-VPN,上網認證,登入錯誤事件	Auth login fail
☐	9. 軟體更新通知	Software upgrade
☐	10. 自動備份系統設定檔	Auto Backup

儲存

圖 1-32 設定訊息通知項目

第二章 網路介面及路由

網路介面包括了 HSecurity+系統的內部網路和外部網路和非軍事區等設定值，在【網路介面】中，系統管理員可定義企業網路架構之內部網路、外部網路和非軍事區的 IP 位址、子網路遮罩、閘道位址等介面設定。

【網路介面】名詞解釋：

內部網路設定

系統管理員可在此設定 HSecurity+的內部網路之網段範圍。

MAC 位址

可依架設環境所需，適時設定 HSecurity+網路介面的 MAC 位址。

Speed and Duplex Mode 設定 說明如下：

可藉由此項功能設定 WAN Port 與其他設備連接時的傳輸速率和模式，目前系統提供有六種方式，分別為 Auto、10baseT/Half、10baseT/Full、100baseT/Half、100baseT/Full、1000baseT/Full。

MTU

MTU 為 Maximum Transmission Unit 的縮寫, 一般預設值為 1,500。但是在不同的網路環境中，應該是有不同的數值。以下列出各種 Maximum MTU

EtherNet Used：1,500（一般的預設值）
EtherNet Actually：1,496（因為 1,500 比較方便記憶）
PPPoE（撥接 ADSL 用的）：1,492
Dial-up（Modem 用的）：576

ARP 防偽

ARP 的攻擊是駭客行為的一種，它的目的是混淆內部網路上網行為，藉以攔截網路封包或是讓內部網路無法正常上網。

遭受此攻擊時會讓 PC 的閘道器 MAC 位址換成攻擊者或是其他不相關的位址，又因為 ARP 攻擊是用廣播的方式，管理者不容易偵測出攻擊者的 IP 及位置，造成管理上的困擾。

HSecurity+藉由固定週期主動更新 MAC 位址的技術，跟內部網路的 PC 溝通更新閘道器的 MAC 位址，避免被 ARP 攻擊者換掉。

介面名稱-eth1 / 2

外部網路_1/2 名稱，讓管理者辨識線路。

連線模式

顯示目前外部網路介面連線模式，可分為 Static、DHCP、PPPOE 等 3 種連線型態。

- Static 固定模式(固接式或 ADSL 專線使用者)
- DHCP 模式 (纜線數據機使用者)
- PPPoE 模式（ADSL 撥接使用者）

上傳速度＆下載速度

系統管理員必須在此設定該外部網路介面的正確頻寬，以作為 HSecurity+頻寬管理運作的依據。

負載分配模式

自動分配：HSecurity+依照外部網路下載和上傳頻寬使用情形，會自動調整對外線路的負載分配。

手動分配：由管理者決定對外線路的負載分配比例。

依來源 IP 分配： HSecurity+依照使用者設定的來源 IP 來分配對外網路連線。

依目的 IP 分配：判別內部用戶是透過 HSecurity+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。

線路偵測方式

測試外部網路是斷、連線的狀態，測試之方法，分為下列三種：

- DNS：以查詢網功能變數名稱稱 的方式來測試是否斷、連線。
- ICMP：以 ICMP 測試，所設定的 IP 之方式來測試是否斷、連線。
- NONE：線路不偵測，永遠是連線狀態。

啟用的管理服務

- Ping ：使用者可 Ping 到該網路介面之 IP 位址，以確認 HSecurity+的網路介面是否存活。
- HTTP ：勾選時，使用者可從該網路介面之 IP 位址，透過 HTTP 協定進入 HSecurity+的管理介面(預設是停用)。
- HTTPS：勾選時，使用者可從該網路介面之 IP 位址，透過 HTTPS 協定進入 HSecurity+的管理介面。

防火牆防護設定

Herhsiang HSecurity+目前提供 SYN、ICMP、UDP 與 Port Scan 等防護。

偵測間隔時間

系統管理者可輸入系統每隔多少間隔時間做檢測，單位以秒為計算。

管理介面閒置多久自動斷線

系統管理員在外部網路介面為 PPPoE 設定（ADSL 撥接使用者）連線模式時，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）。

非軍事區網路介面位址

系統管理員可在此設定 HSecurity+的非軍事區之網段或運作模式。

非軍事區有 2 種模式：

- NAT：在此模式中，非軍事區為一獨立虛擬網段，該虛擬網段可由系統管理員設定。（但不可和內部網路介面為同一網段）
- BRI：在此模式中，外部網路_1 與 DMZ Port 處於橋接（bridge）模式。

下列表格為標準虛擬 IP 位址範圍，不可使用外部真實 IP 位址。

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

IPv6 設定 說明如下：

為次世代網際網路協定（Internet Protocol Next Generation），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：

00100001110110101001000011010011000000000101000000101111001110110 0

0000101010101000000000111111111111111000101000100111000101101 0，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
  0010000111011010:1001000011010011:0000000001010000:0010111100111011:0000001010101010:0000000011111111:1111111000101000:10011100

  01011010 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 目的位元址時，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 對映位址：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。**

2-1、網路介面

HSecurity+ 的網路介面，都在這裡設定，這個部份是要讓 HSecurity+ 正常運作必須要設定的第一個項目。

2-1-1、內部網路

更改內部網路介面位址

步驟1. 在【網路介面】之【內部網路】功能中，鍵入以下資料：（圖 2-1）

- 輸入內部網路 IP 位址為【192.168.1.254】。
- 輸入網路遮罩為【255.255.255.0】。
- 輸入上傳、下載速度為【102400】，單位為 Kbps。
- 選擇 Speed and Duplex Mode 模式。
- 設定 MTU 數值，並按下【儲存】鍵

步驟2. 勾選是否啟動 ARP 防偽，為了避免遭受 ARP 攻擊，管理者可設定間隔時間，讓系統自動更新目前使用者 IP 與 MAC 位址，並免遭受竄改。

圖 2-1 內部網路介面位址 Web UI 設定畫面

註：HSecurity+的預設內部網路位址為 192.168.1.1，系統管理員在更動內部網路位址後，必須使 PC 重新取得跟內部網路同網段的 IP 位址，這樣才可以變更後的內部網路位址進入管理介面。

【Multiple Subnet】：內部網路可支援多個區段的網路位址。

可讓內部網路設定多個網段位址，並可經由不同的外部位址與網際網路建立連線。

例如：公司的專線申請到多個真實 IP 位址 168.85.88.0/24，公司內部也分為許多的部門，研發部、客服部、業務部、採購部、會計室等，為了方便管理可將各部門以不同 IP 網段來區分。設定方式如下：

客服部網段 192.168.2.1/24(Internal Gateway) ←→ 123.85.88.252(External)

業務部網段 192.168.3.1/24(Internal Gateway) ←→ 123.85.88.251(External)

採購部網段 192.168.4.1/24(Internal Gateway) ←→ 123.85.88.250(External)

會計室網段 192.168.5.1/24(Internal Gateway) ←→ 123.85.88.249(External)

在 Multiple Subnet 設定完成後每個部門就會從不同的外部 IP 位址出去，以業務部的範例，192.168.3.1/24 的電腦，會使用 123.85.88.251 的 ip 位址 NAT 出去。（圖 2-2）

圖 2-2 Multiple Subnet 的設定

如果想讓內部某個 IP 位址使用特定的外部 IP 位址，則只要在 subnet 中輸入 255.255.255.255 ，代表只有這個 內部 IP 位址使用選定的外部 IP 位址。

以下圖為範例，192.168.168.123 的 IP 位址，會使用 123.85.88.253 的外部 IP 為 NAT 的位址。（圖 2-3）

圖 2-3 一對一 Multiple Subnet 的設定

註 1：記得在內部網路介面上設定 Multiple Subnet，可以切出許多 vlan。

註 2：Multiple Subnet 的 Routing 模式只在 Static 連線模式下才能使用。

2-1-2、外部網路_1

外部網路_1：範例一、設定外部網路介面位址為 Static

步驟1. 於【網路介面】功能中，點選【外部網路_1】選單。

步驟2. 設定連線模式為 Static（固接或 ADSL 專線使用者）（圖 2-4）

- 在介面名稱-eth1 中輸入任何文字，管理者可以辨識這個線路。
- 鍵入 ISP 所提供的【IP 位址】【網路遮罩】【預設閘道】。
- 鍵入【上傳速度】及【下載速度】，可以用下拉式選單選擇預設的速度，或是自行輸入速度，自行輸入時的單位為 Kbps。(※ 依照 ISP 提供的速度)
- 勾選負載分配模式為【自動分配】、【手動分配】、【依來源 IP 分配】、【依目的 IP 分配】的選項。針對某些特定服務，當連線建立完成後，不合適切換 WAN 的線路，則需要選以來源 IP 位址分配 WAN 的線路。
- ：代表斷線，：代表連線。

圖 2-4 外部網路介面位元址連線方式為 Sttaic 模式

線路偵測方式

設定線路偵測設定方式（有 DNS、ICMP 和 NONE 三種方式）（圖 2-5）

- DNS：用 DNS 查詢的方式，確認線路斷線或是連線，輸入被偵測伺服器 IP 位址，必須確認設定的 IP 位址會回應 DNS 封包要求。
- ICMP：用 ICMP 查詢的方式，確認線路斷線或是連線，輸入被偵測的 IP 位址，必須確認設定的 IP 位址會回應 ICMP 封包要求。
- 不偵測：如果確認線路不會斷線，可以選它。
- 啟用管理的服務，包含 Ping、Http、Https。

圖 2-5 線路偵測方式

防火牆防護設定

外部 IP 位址要不要接受防火牆的保護，HSecurity+ 目前提供 SYN 攻擊、ICMP 攻擊、UDP 攻擊及 PortScan 等 4 種攻擊防護。（圖 2-6）

圖 2-6 防火牆防護設定

記錄：管理者可以點選【紀錄】按鈕，查看這個 IP 位址的遭受駭客攻擊的方式、時間等攻防紀錄。

共同設定

共同設定是指外部網路_1 跟外部網路_2 會共同使用的參數部份，設定資料如下：（圖 2-7）

- 鍵入【DNS Server1】為【168.95.1.1】或是 該線路 ISP 提供的 DNS 伺服器 IP 位址。
- 鍵入【DNS Server2】為【168.95.192.1】或是 該線路 ISP 提供的 DNS 伺服器 IP 位址。
- 設定外部網路 HTTP 與 HTTPS 管理埠號，HTTP 預設埠號是 80，HTTPS 預設埠號是 443。
- 設定偵測間隔時間，預設是 3 秒測試一次，測試連線為 HSecurity+偵測該外部網路是否斷線或是連線的依據。在測試連線中所設定之測試 DNS 伺服器或 IP 位址皆必須永久運作，否則會造成 HSecurity+的判斷錯誤。
- 管理介面閒置多久自動斷線，預設是 60 分鐘，管理者進入管理介面，超過這個設定時間，就需要重新登入。

圖 2-7 完成共同設定

註：當在外部網路介面中勾選 Ping 時，使用者將可從外部網路 Ping 的到 HSecurity+與進入 HSecurity+的外部介面。這有可能會影響到網路的安全性，建議系統管理員在確定所有設定皆無虞之後，能將 Ping 的選項取消。

2-1-3、外部網路_2

外部網路_2：範例二、設定外部網路介面位址為 DHCP

步驟1. 於【網路介面】功能中，點選【外部網路_2】選單鈕。

步驟2. 設定連線模式為 DHCP 自動取得 IP 位址，它會自動從 DHCP 伺服器取得 IP 資訊。（圖 2-8）

- 在介面名稱-eth2 中輸入任何文字，管理者可以辨識這個線路。
- 鍵入【上傳速度】及【下載速度】，可以用下拉式選單選擇預設的速度，或是自行輸入速度，自行輸入時的單位為 Kbps。(※ 依照 ISP 提供的速度)
- 系統會自動取得 IP 位址、網路遮罩、預設閘道。
- 負載分配模式只可手動設定，當外部網路_1 設為自動分配時，它無法選擇，只有外部網路_1 設為手動分配時，它才可以選擇分配比例。
- ：代表斷線，：代表連線。

圖 2-8 外部網路介面位元址連線方式為 DHCP 模式

步驟3. 設定線路偵測設定方式（有 DNS、ICMP 和 NONE 三種方式）（圖 2-9）

- DNS：用 DNS 查詢的方式，確認線路斷線或是連線，輸入被偵測伺服器 IP 位址。
- ICMP：用 ICMP 查詢的方式，確認線路斷線或是連線，輸入被偵測的 IP 位址。
- 啟用管理的服務，包含 Ping、Http、Https。

圖 2-9 線路偵測設定

步驟4. 設定 SYN 攻擊、ICMP 攻擊與 UDP 攻擊設定值：（圖 2-10）

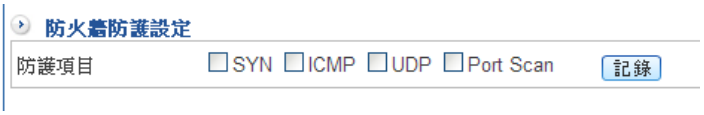

圖 2-10 防火牆防護設定

記錄：管理者可以點選【紀錄】按鈕，查看這個 IP 位址的遭受駭客攻擊的方式、時間等攻防紀錄。

註：在外部網路_2 中，指定 IP 位元址的連線方式並不需要設定 DNS 伺服器，因為它是屬於跟外部網路_1 共同設定值。

範例三：設定外部網路介面位址為 PPPoE

步驟1. 於【網路介面】功能中，點選【外部網路_2】的選單鈕。

步驟2. 設定連線模式為 PPPoE（ADSL 撥接使用者）（圖 2-11）

- 在介面名稱-eth2 中輸入任何文字，管理者可以辨識這個線路。
- 選擇【PPPoE】連線模式。
- 輸入【帳號】，申請帳戶之名稱。
- 輸入【密碼】，申請帳戶之密碼。
- 鍵入【上傳速度】及【下載速度】，可以用下拉式選單選擇預設的速度，或是自行輸入速度，自行輸入時的單位為 Kbps。(※ 依照 ISP 提供的速度)
- 負載分配模式只可手動設定，當外部網路_1 設為自動分配時，它無法選擇，只有外部網路_1 設為手動分配時，它才可以選擇分配比例。
- ：代表斷線，：代表連線。

圖 2-11 外部網路介面位元址連線方式為 PPOoE 模式

步驟3. 設定線路偵測設定方式（有 DNS、ICMP 和不偵測三種方式）（圖 2-12）

- DNS：用 DNS 查詢的方式，確認線路斷線或是連線，輸入被偵測伺服器 IP 位址。
- ICMP：用 ICMP 查詢的方式，確認線路斷線或是連線，輸入被偵測的 IP 位址。
- 啟用管理的服務，包含 Ping、Http、Https。

圖 2-12 完成線路偵測方式

步驟4. 設定防火牆防護設定（圖 2-13）

- 防護項目計有 SYN、ICMP、UDP、Port Scan 四種防護方式。
- 點選「記錄」鍵可細看防護記錄。

圖 2-13 完成防火牆防護設定方式

記錄：管理者可以點選【紀錄】按鈕，查看這個 IP 位址的遭受駭客攻擊的方式、時間等攻防紀錄。

2-1-4、非軍事區

範例一、設定非軍事區介面位元址（NAT 模式）

步驟1. 選取【網路介面】中的【非軍事區】。

步驟2. 選擇非軍事區運作模式為 NAT 模式。（圖 2-14）

- 選取【非軍事區介面位址】為【NAT】。
- 設定【IP 位址】與【網路遮罩】。
- 設定【上傳速度】、【下載速度】。
- 如果需要更改 MAC 位元址，在 MAC 位址欄填入新的 MAC 位址就可以。

步驟3. 勾選是否啟動 ARP 防偽。

步驟4. 按下【儲存】。

圖 2-14 非軍事區域網路 NAT 模式 Web UI 設定畫面

範例二、設定非軍事區介面位元址（Transparent Bridge 模式）

DMZ Bridge 模式是將 WAN1 跟 DMZ 設成橋接模式，所有 DMZ 下的 IP 位址跟 WAN 介面使用相同的 IP 區段及閘道器位址，此時 WAN 1 必須設為 STATIC 模式。

步驟1. 選取【網路介面】中的【非軍事區】。

步驟2. 選擇非軍事區運作模式為透通路由模式：（圖 2-15）

- 選取【啟用】模式為【Transparent Bridging】。
- 設定【上傳速度】、【下載速度】。
- 如果需要更改 MAC 位元址，在 MAC 位址欄填入新的 MAC 位址就可以。
- 按下【儲存】鈕，啟用這個模式，HSecurity+多功能防火牆會將設備重新開機，套用新的模式。

圖 2-15 非軍事區域網路橋接模式 Web UI 設定畫面

範例三、設定非軍事區介面位元址（Transparent Routing 模式）

DMZ Transparent Routing 模式是將 WAN1 跟 DMZ 設成路由模式，所有 DMZ 下的 IP 位址跟 WAN 介面使用相同的 IP 區段，此時 WAN 介面 必須設為 STATIC 模式。

步驟1. 選取【介面位址】中的【非軍事區域網路】。

步驟2. 選擇非軍事區運作模式為路由模式：

- 選取【非軍事區域介面位址】為【Transparent Routing】。
- 設定【上傳速度】、【下載速度】。
- 如果需要更改 MAC 位元址，在 MAC 位址欄填入新的 MAC 位址就可以。
- 設定路由要用的 IP 位址。
- 按下【儲存】鈕，啟用這個模式，UTM 防火牆 UR-9 系列 會將設備重新開機，套用新的模式。

註：在 DMZ 切換運作模式時，都需要重新開機。

2-2、路由設定

串接於 HSecurity+下用來互連兩不同網段之 Router，能使彼此區域網路透過 HSecurity+連上網際網路。

範例：網路架構圖 (圖 2-16)

甲公司 ：WAN 1、WAN 2 和 ATU-R 連接，連上網際網路，LAN 網段為 192.168.1.1/24，串接於 LAN 之 Router1（Lan1 :192.168.1.39，wan：10.10.10.1，支援 RIPv2）。

乙公司：Router2（wan：10.10.10.2，支援 RIPv2），其 LAN 網段為 192.168.20.1/24。

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

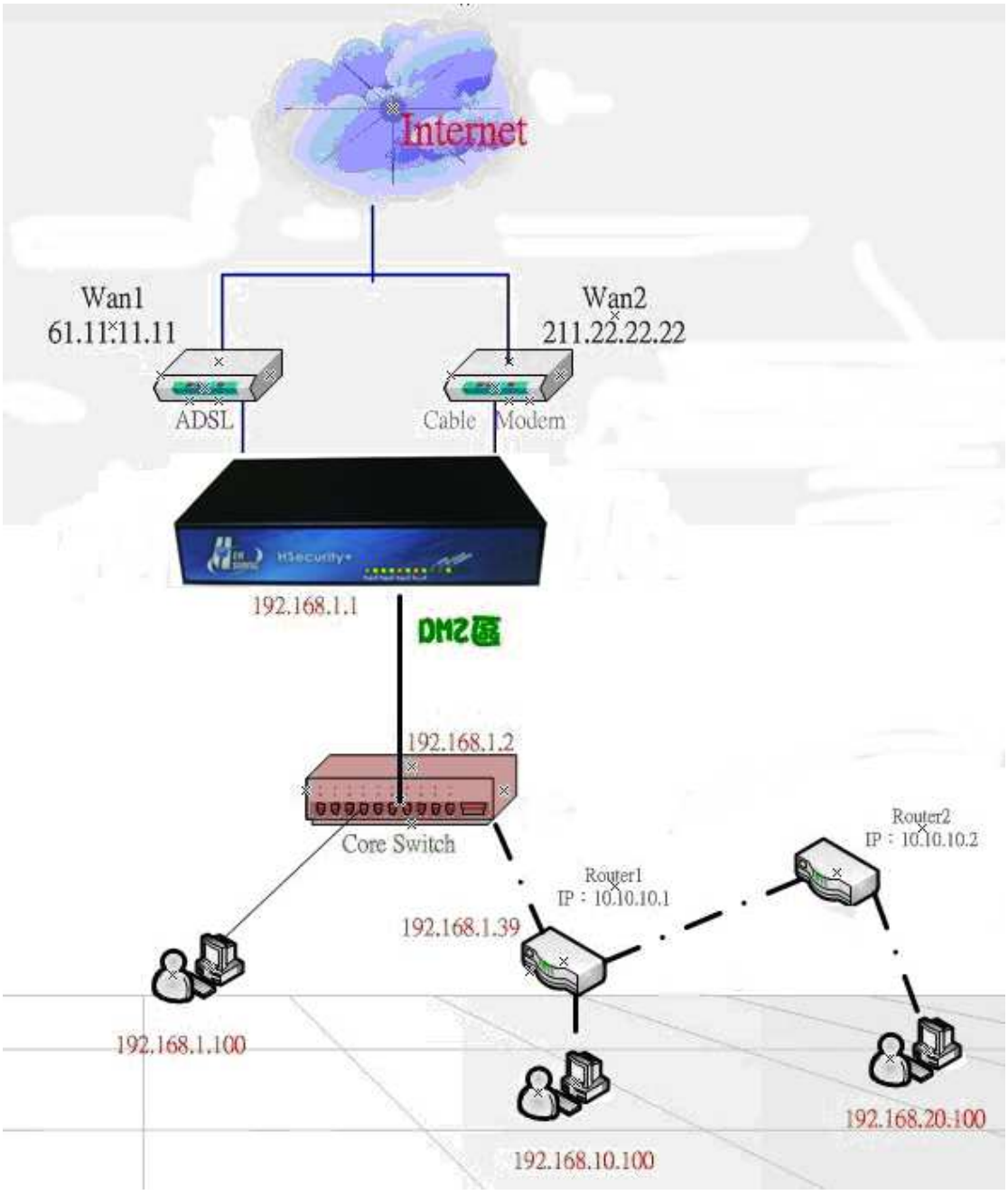

圖 2-16 指定路由表運用環境

步驟1. 於【路由設定】之【路由表】功能中新增下列設定：（圖 2-17）

- 【目的位元址】輸入 192.168.99.0。
- 【子網路遮罩】輸入 255.255.255.0。
- 【閘道位址】輸入 192.168.1.253。
- 按下【新增】鈕。

圖 2-17 新增指定路由表

步驟2. 新增完成，此時 192.168.99.0/24 和 192.168.1.0/24 網段下之電腦可互相連通，且皆可由 HSecurity+轉換成真實 IP 連上網際網路。

範例：動態路由網路 (圖 2-18)

UTM 防火牆支援 RIP 協定，以 RIP V2 協定，將內外的路由網段，自動學習。

步驟1. 於【路由設定】之【動態路由】功能中選擇要套用的網路介面，啟用的介面將會自動交換學習到的網路區段。

步驟2. 設定路由更新週期。

步驟3. 路由逾時時間設定。

圖 2-18 動態路由

第三章 管 制 條 例

預設的管制行為是內對外全開放，當外部網路通了，內部就可以全部上網際網路。

每一個封包在通過 HSecurity+時，需要逐條檢查是否符合管制條例，當封包的條件符合某條管制條例時，就會按該管制條例的設定來通過 HSecurity+，而不會再向下檢查其他的管制條例。

如封包無法符合任何管制條例時，該封包就會被放行，如果不想放行這類型的封包，可以在最後一條加上全部禁止的條例。

管制條例的參數包含『基本設定』、『管制行為設定』2 大區塊。

1.基本設定：管制條例名稱、來源網路(IP 位址、MAC 位元址) 、目的網路(IP 位元址)與動作。

2.管制行為設定：通訊協定、通訊埠或群組、應用程式管理、頻寬管理、時間表、URL 管制、上網認證、使用的外部網路、每個來源 IP 能使用的最大連線數、郵件掃毒/垃圾信過濾、禁止使用 SKYPE、WEB、FTP 掃毒、IDP、封包追蹤、流量分析與流量配額/天。

並不是每一個管制方向都有上述所有的管制目標物，外到內或是外到 DMZ 只可以管制通訊埠、頻寬表、時間。內到 DMZ 之間多了一項應用程式的管理。

註：所有經過 HSecurity+管制的應用程式、頻寬、時間表、URL 管制....等，都必須要有管制條例許可才能通過。

【管制條例】名詞解釋：

管制條例名稱：

為該管制條例所管制的名稱，可以輸入任何中英文字。

來源網路位址（來源網路）& 目的網路位元址（目的網路）：

來源網路位址（來源網路）與 目的網路位元址（目的網路）是以 HSecurity+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元址，除了從『管制目標』中選擇外，也可以直接輸入使用者 IP 位址與 MAC 位址。

為了方便管理者對來源網路與目的網路的辨識，Herhsiang 針對不同來源位址以不同顏色區別，來源網路為單一位址以黑色字體呈現、來源為網路群組以藍色字體表現，如來源網路是 Multiple Subnet 則以綠色字體呈現，讓管理者可以快速、方便管控。

動作：

主要動作有兩種，分別為拒絕與允許，當設為允許動作時，任何滿足『基本設定』、『管制行為設定』的封包就會被放行，設為拒絕則此封包會被丟棄。當啟動 LAN 對 WAN 管制或 DMZ 對 WAN 管制時，系統會詢問管理者是要以 NAT 或 ROUTE 進行動作連線。

通訊協定：

可單獨管制 UDP 或 TCP 埠號，或全部管控。

通訊埠或群組：

系統管理員可以在【服務表】的【服務群組】選項中，新增服務群組名稱，將要提供的服務包含進去。

有了服務群組的功能，管理員在制訂管制條例時可以簡化許多流程。例如，有 10 個不同 IP 位址可以對伺服器存取 5 個不同的服務，如 HTTP、FTP、SMTP、POP3 和 TELNET，如果不使用服務群組的功能，總共需制定 10x5=50 條管制條例，但使用服務群組名稱套用在服務選項上，則只需一條管制條例即可達到 50 條管制條例的功能。

應用程式管制：

可管制 P2P、即時通訊軟體、WEB 應用、娛樂軟體、其他軟體的連線。

頻寬管理：

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用）。

時間表：

設定該條管制條例的生效時間。

URL 管制：

管制通過該條管制條例的 URL 網址過濾。

上網認證：

被管制的 IP 位址使用 WEB 服務時，需不需要輸入帳號、密碼，藉以取得上網路的權利。

使用的外部網路：

指定封包進出 HSecurity+時，所經由的路徑（WAN1、WAN2 或全部）。

每個來源 IP 能使用的最大連線數：

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，則超過的連線數的連線要求會被丟棄。

禁止使用 Skype：

限定來源目標透過管制條例禁止使用 SKYPE。

封包追蹤：

記錄通過該條管制條例的所有封包，可以在管制條例中這個條例的封包通聯記錄。

流量配額/天：

HSecurity+的主要靈魂是管制條例，目前支援每一個管制條例的流量限額，一旦超過管理者的使用額度，這個條例的服務就會被禁止使用。在管制條例的顯示限制的上下傳限額及剩下的數量。

圖示說明：

圖 示	名 稱	說　明
	頻寬管理	頻寬管理功能已開啟。
	時間排程	啟動時間表，在設定時間範圍內自動執行條例。
	URL 管制	URL 管制功能已開啟。
	外部網路管制	使用哪一條外部網路線路。
	最大頻寬限制	限制每來源 IP 位址最大頻寬量或連線數。
	上網認證	該條例使用者需要通過上網認證。
	流量配額	每日最多上傳、下載頻寬量。
	允許	NAT 運作模式，允許符合該管制條例的封包進出。
	拒絕	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。
	啟動	啟動該管制條例的運作。
	修改	修改該管制條例的內容。
	刪除	刪除該管制條例。
	紀錄	開啟新視窗，顯示這個管制條例下的封包通聯記錄。

如何運用管制條例

HSecurity+依據不同來源介面過濾封包，將管制條例設定功能區分為下列六項（在 DMZ 設成 Bridge 模式下只有 5 項），以便利系統管理員，針對來自不同介面的封包執行管制動作。

（一）【LAN 對 WAN 管制】：來源網路位址是在內部網路區，目的網路位元址是在外部網路區。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。

（二）【LAN 對 DMZ 管制】：來源網路區是內部網路區，目的網路區是在非軍事區。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。

（三）【DMZ 對 LAN 管制】：來源網路區是非軍事區，目的網路區是在內部網路區。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，DMZ 設成 Bridge 模式下，沒有這個管制。

（四）【WAN 對 LAN 管制】：來源網路位址是在外部網路區，目的網路位元址是在內部網路區（如 IP 對映、虛擬伺服器）。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。

（五）【WAN 對 DMZ 管制】：來源網路區是外部網路區，目的網路區是在非軍事區（如 IP 對映、虛擬伺服器）。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。

以範例來說明管制條例如何運作，在範例中，總共假設了 6 種管制條例應用環境，如下表說明。

編號	適用範圍	範例環境
範例 1	LAN 至 WAN	建立可監控內部使用者上網之管制條例。（以應用程式管理、頻寬管理、時間表為例）
範例 2	LAN 至 WAN	禁止使用者存取特定之網路資訊。（以特定外部網路 IP 和 URL 管制為例）
範例 3	WAN 至 LAN	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）
範例 4	WAN 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、每日下載時間和最多同步下載連線數。
範例 5	WAN 至 DMZ DMZ 至 WAN LAN 至 DMZ	在非軍事區為橋接的模式下，架設一 Mail Server，允許內部和外部網路使用者，透過其收發 E-mail。

3-1、範例一：管理內部上網

目的

內部某一個特定 IP 位址或是群組，開放他們在指定的時間內（時間表的應用），限定的頻寬下（頻寬表的應用）使用 P2P 協定下載時。對於這使用者使用非 P2P 協定，則沒有任何限制。

步驟大綱

先將要管理的 P2P 協定、管制的時間及頻寬表在管理目標中設定完畢，再到 LAN to WAN 的管制中建立一條新的管制條例。

步驟1. 於【管理目標】之【應用程式管理】功能中，輸入該管制條例名稱，並勾選是否啟動【啟用紀錄】。

步驟2. 選取要管理的應用程式：（圖 3-1）

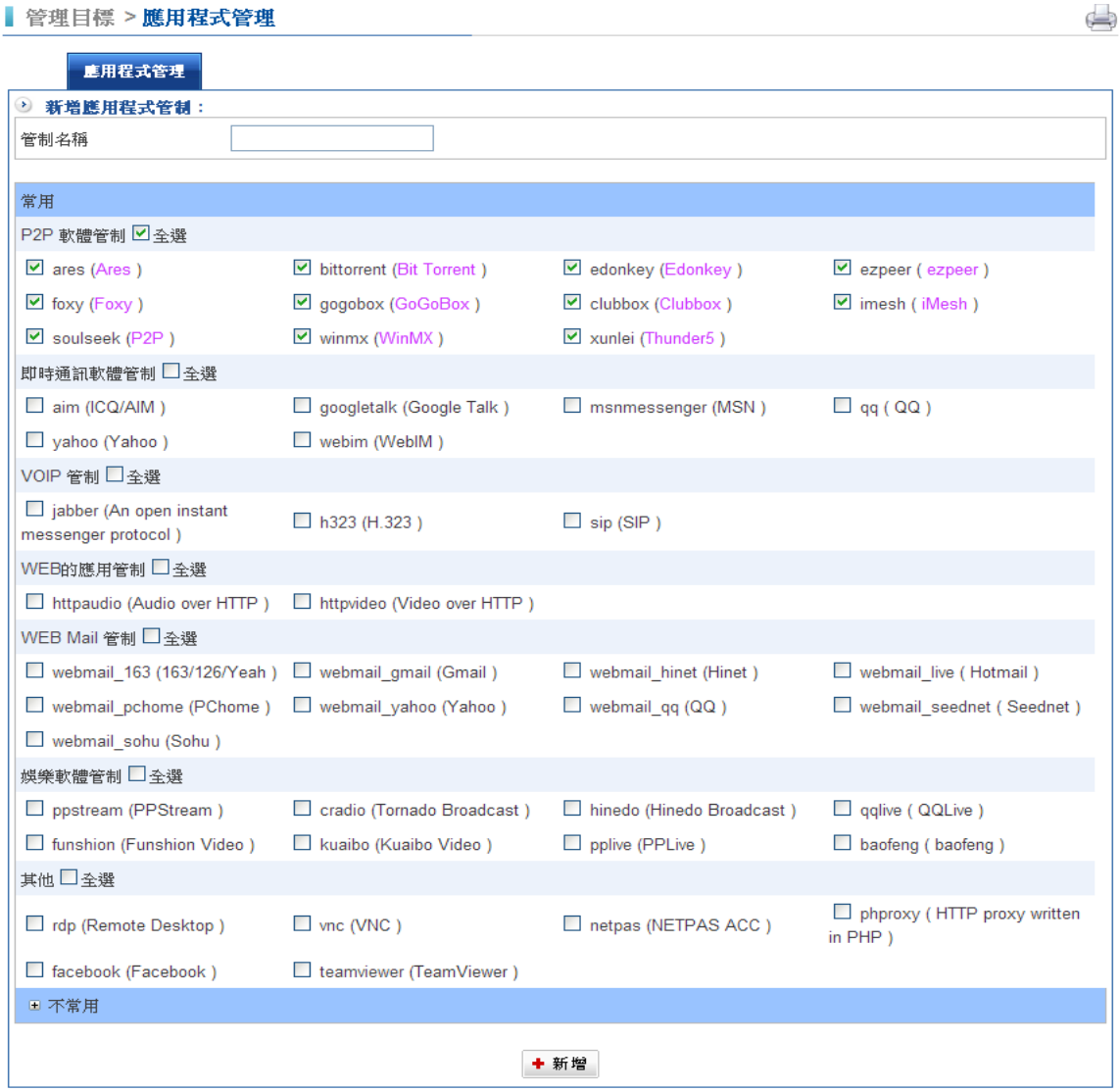

圖 3-1 設定應用程式管制

步驟3. 按下『新增』按鈕後，系統就會將這筆資料建立，並且顯示出來。（圖 3-2）

圖 3-2 應用程式管制列表

步驟4. 於【管理目標】之【頻寬管理】功能中，新增一筆頻寬管理管制條例：（圖 3-3），HSecurity+ 可以管理對 WAN、LAN 介面的上傳及下載頻寬。

圖 3-3 設定頻寬管制

步驟5. 按下『新增』按鈕後，系統就會將這筆資料建立，並且顯示出來。（圖 3-4）

圖 3-4 完成頻寬管制設定

步驟6. 於【管理目標】之【時間表】功能中，完成一筆時間表管制：（圖 3-5）

圖 3-5 建立時間表管制

步驟7. 於【管制條例】之【LAN 對 WAN 管制】功能中，新增一條管制條例。

步驟8. 基本設定區：選擇要管制的內部 IP 位址（來源網路）或是自行填入 IP、MAC 位元址，在目的網路中可以選擇（Outside_Any）或是自行填入 IP、MAC 位址，動作上選擇（允許）。（圖 3-6）

圖 3-6 基本設定

步驟9. 管制行為區：將剛剛在管理目標中建立的 3 個管理目標（P2P 軟體、頻寬表、時間表）分別選入，並按下『新增』按鈕。（圖 3-7）

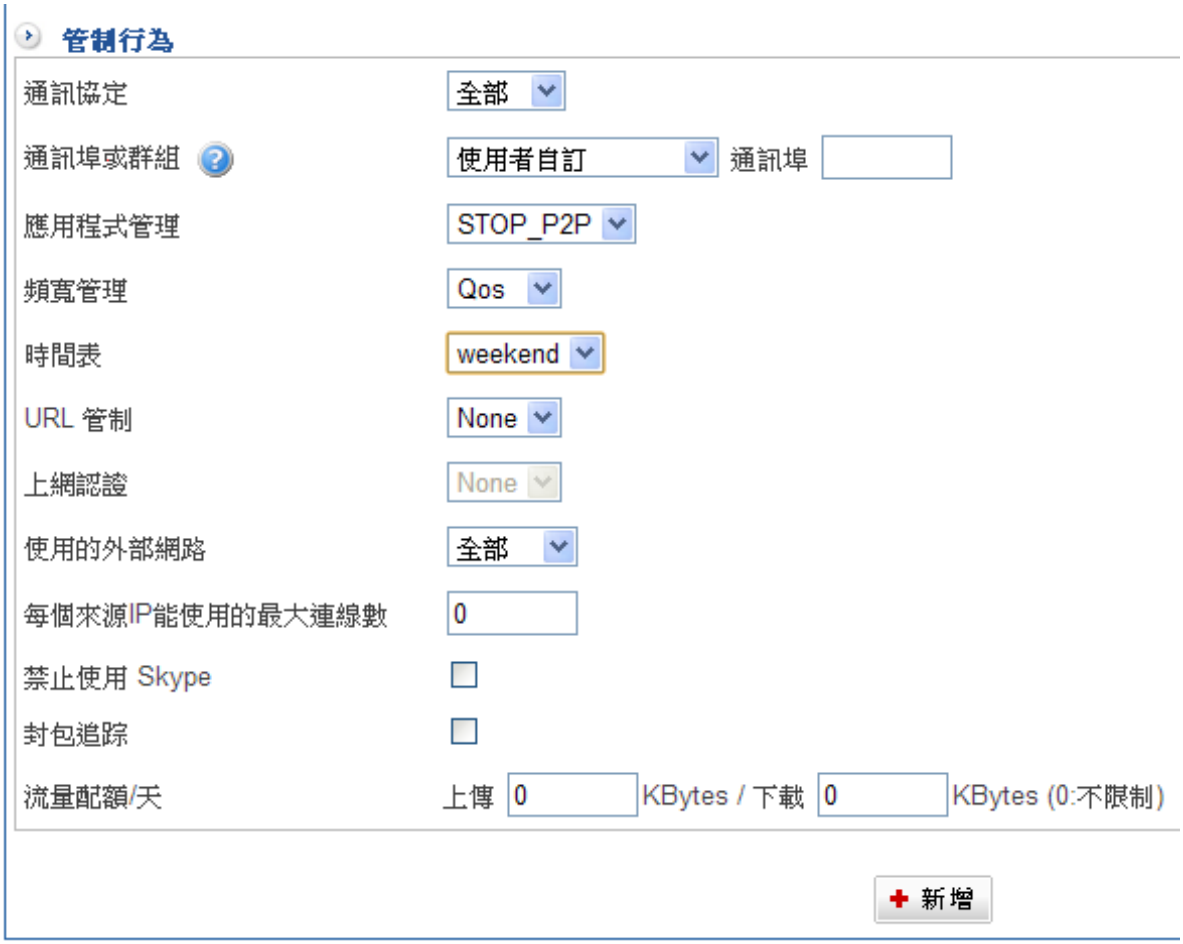

圖 3-7 設定 LAN 對 WAN 管制條例設定

步驟10. 完成內部使用者(LAN)對外部網路(WAN)之應用程式管理、頻寬管理、時間表管制行為設定。（圖 3-8）

圖 3-8 完成內對外上網管制行為

3-2、範例二：禁止上特定網站

目的

內部某一個特定 IP 位址或是群組，不可以上某些網站（www.sample.com）或是只允許上這一些網站。

步驟大綱

步驟1. 先將要管理的網站或外部 IP 位址在管理目標中設定完畢，再到 LAN to WAN 的管制中建立一條新的管制條例並套用這個 URL。

步驟2. 於【URL 管理】之【黑白名單設定】功能中，按下『新增』按鈕，並輸入名稱及要管制的網站，每一個網站都是獨立一行，URL 的輸入數量不限。（圖 3-9）

圖 3-9 設定 URL 管制

步驟3. 於【URL 設定】中設定群組，輸入群組名稱及名單選擇。（圖 3-10）

圖 3-10 設定 URL 群組名稱

步驟4. 於【位址表】之【外部 IP 位址表】與【外部網路群組】功能中，新增外部 IP 位址或群組。（圖 3-11）

圖 3-11 設定欲阻擋的外部 IP

註：系統管理員可利用位址表內的群組功能，將自訂的位址表群組化，這可使在設定管制條例時能更方便。

步驟5. 在【管制條例】的【LAN 至 WAN 管制】功能中，新增規則：

步驟6. 基本設定區：選擇要管制的內部 IP 位址（來源網路）或是自行填入 IP、MAC 位元址，在目的網路中可以選擇剛剛制定的外部 IP 位址或是群組，也可以自行填入 IP、MAC 位址。

步驟7. 動作上選擇（允許），代表允許用戶瀏覽 URL 設定的網址，選擇（拒絕），代表拒絕用戶瀏覽 URL 設定的網址。（圖 3-12）

圖 3-12 基本設定區

步驟8. 管制行為區：將剛剛在管理目標中建立的管理目標（URL 管制）選入，並按下『新增』按鈕。（圖 3-13）

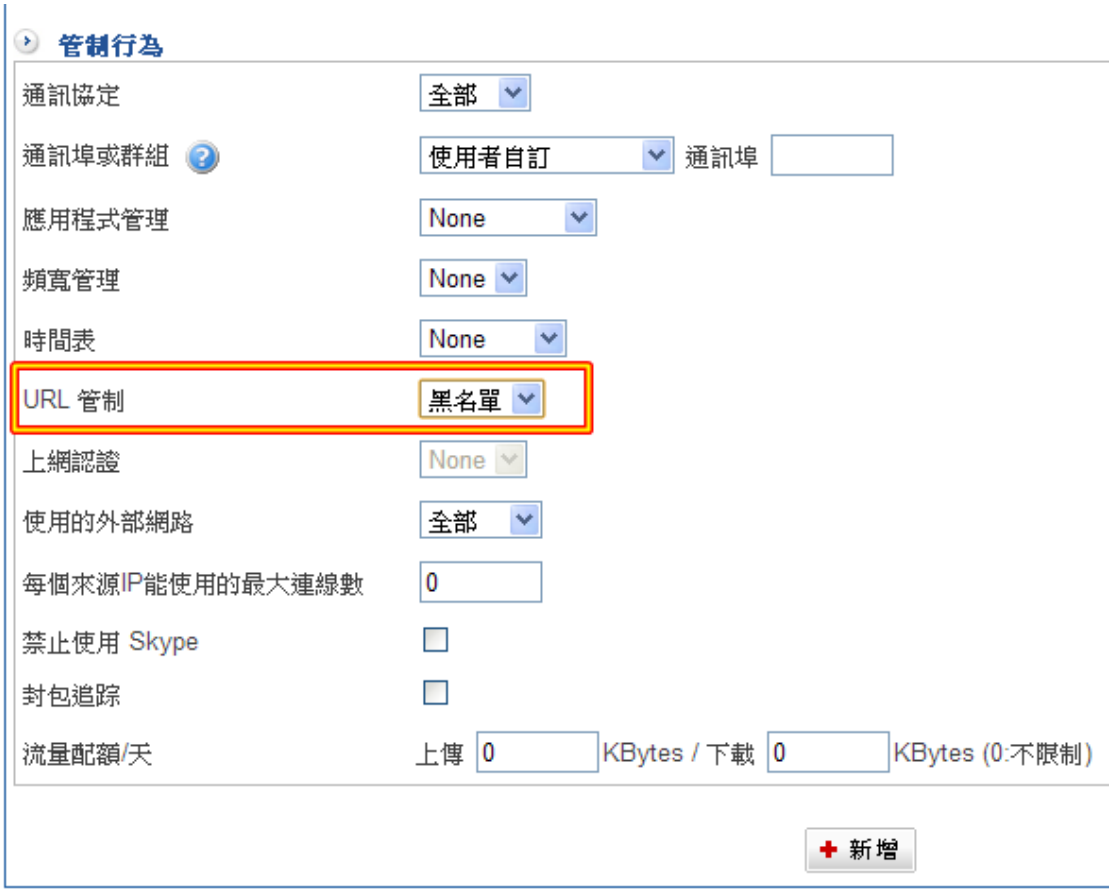

圖 3-13 設定具阻擋功能之管制條例

步驟9. 完成管制使用者存取特定網路資源之管制條例設定。（圖 3-14）

圖 3-14 管制使用者存取特定網路資源之管制條例設定完成

註：URL 管制不一定要搭配外部 IP 位址或是群組。

3-3、範例三：WAN 對 LAN 的管制

目的

將外部 IP 位址的特定埠號對應到內部某一個特定 IP 位址的相同或是不同埠號。

步驟大綱

先在虛擬伺服器上選一個外部 IP 位址，並將要轉到內部網路的埠號及 IP 位址設定好，再到管制條例的外對內中增加一條允許的條例即可。

步驟1. 在虛擬伺服器中選擇一個可以使用的 IP 位址。

步驟2. 於對外【虛擬伺服器】功能中，新增下列設定：

- 外部通訊埠選定 TCP 21。
- 對應到內部的 IP 位址：192.168.2
- 按下【新增】鈕。（圖 3-15）

圖 3-15 設定虛擬伺服器

步驟3. 於【管制條例】之【WAN 對 LAN 管制】功能中，新增下列設定：（圖 3-16）

- 按下【新增】鈕。
- 輸入管制條例名稱【外對內管制】。
- 來源網路設定為【Outside_Any】。
- 【目的網路】選擇 Virtual Server。
- 通訊埠或群組設定為【ALL】，ALL 代表所有在虛擬服器上設定的埠對應，以這個案例是，TCP 21。
- 啟動封包追蹤，若有需要也可以開啟 NAT 功能。
- 啟動防護攻擊設定。

圖 3-16 設定外部遙控內部電腦之管制條例

步驟4. 完成由外部遠端電腦操控內部網路電腦之管制條例設定。（圖 3-17）

圖 3-17 完成外部遙控內部電腦之管制條例設定

註：在服務中顯示【ALL】並不是指所有的通訊埠，而是定義在虛擬伺服器中的所有通訊埠。

3-4、範例四：WAN 對 DMZ 的管制

目的

將外部 IP 位址的特定埠號對應到 DMZ 區的某一個特定 IP 位址的相同或是不同埠號，並限制外部使用者下載的頻寬和最多同步下載連線數。

步驟大綱

步驟1. 先在虛擬伺服器上選一個外部 IP 位址，並將要轉到 DMZ 區的埠號及 IP 位址設定好，再到管制條例的外對 DMZ 中增加一條允許的條例即可。

步驟2. 於【非軍事區】架設一 FTP 伺服器，其 I P 為 172.172.1.2。（非軍事區的介面位元址設為 1172.172.1.1/24 ）

步驟3. 於【虛擬伺服器】選定外部網路位址，可藉由輔助遠取快速選取（圖 3-18 ）

圖 3-18 設定虛擬伺服器對外 IP 位址

步驟4. 於對外【虛擬伺服器】功能中，新增下列設定：

- 外部通訊埠選定 FTP(21 埠)。
- 虛擬伺服器 IP 位址設定為 172.172.1.2。
- 按下【新增】鈕。（圖 3-19 ）

圖 3-19 設定虛擬伺服器 IP 位址

步驟5. 於【頻寬表】功能中，新增下列設定：（圖 3-20）

圖 3-20 設定頻寬表

步驟6. 於【管制條例】之【WAN 對 DMZ 管制】功能中，新增下列設定：

- 鍵入管制條例名稱【外部至非軍事區管制】。
- 來源網路設定為【Outside_Any】。
- 【目的網路】選擇 Virtual Server (192.168.168.155)。
- 通訊埠或群組設定為【FTP】。
- 設定頻寬管理管制行為。
- 按下【新增】鈕。（圖 3-21）

圖 3-21 新增管制條例

完成限制外部使用者存取非軍事區網路伺服器服務及佔用網路資源之管制條例設定。（圖 3-22）

圖 3-22 管制條例設定完成

3-5、範例五：WAN 對 DMZ Bridge 的管制

目的

在非軍事區為橋接的模式下，架設 Mail Server，允許內部和外部網路使用者，透過其收發 E-mail。

步驟大綱

選一個外部 IP 位址，將 IP 要設定到 DMZ 區的郵件伺服器上，管制條例的外對 DMZ 中增加一條允許的條例即可。

步驟1. 於【非軍事區】新增郵件伺服器 IP，其對外網路 IP 位址為 111.22.33.44。（圖 3-23）

圖 3-23 Mail 伺服器外部網路 IP 位址設定

步驟2. 於【管理目標】之【服務表 > 服務群組】功能中，自訂 SMTP(25)、POP3(110)、、HTTPS(443)、IMAP(143)...等相關通訊埠：（圖 3-24）

圖 3-24 設定含有 POP3、SMTP 與 HTTP...等的服務群組

步驟3. 於【管制條例】之【WAN 對 DMZ 管制】功能中，新增下列設定：

- 鍵入管制條例名稱【Mail SV 管制】。
- 來源網路設定為【Outside_Any】。
- 【目的網路】選擇 Mail Server (或直接在 IP 位址欄位輸入 111.22.33.44)。
- 通訊埠或群組設定為【Mail_port】(包含所有已對應過的服務)。
- 按下【新增】鈕。（圖 3-25）

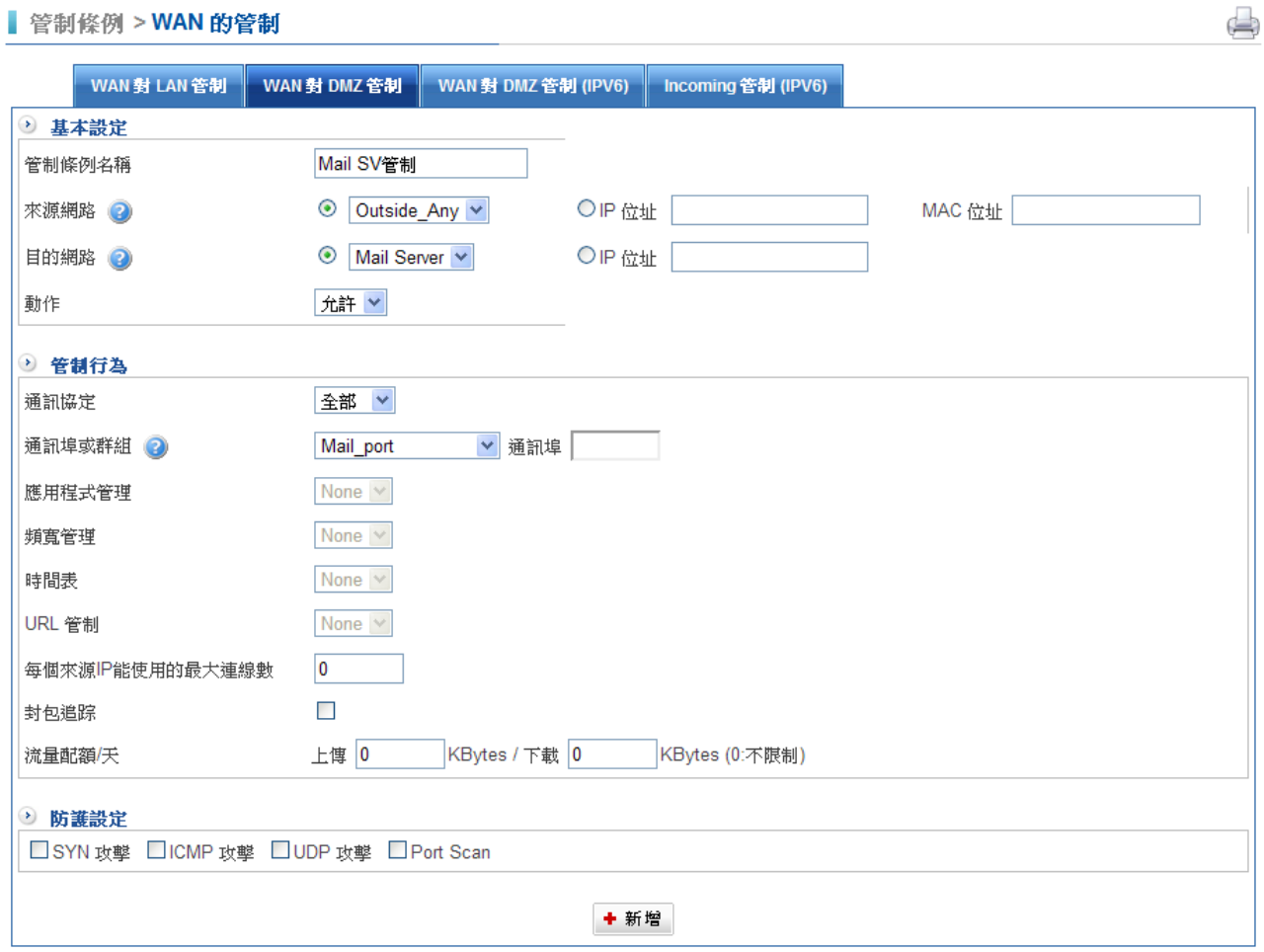

圖 3-25 設定外部至非軍事區存取電子郵件服務之管制條例

步驟4. 完成外部至非軍事區存取電子郵件服務之管制條例。（圖 3-26）

圖 3-26 完成外部至非軍事區存取電子郵件服務之管制條例設定

第四章 管理目標

4-1、位址表

HSecurity+在此單元中提供系統管理員，定義內部 IP 位址表、內部網路群組、非軍事區 IP 位址表、非軍事區群組、外部 IP 位址表、外部網路群組的介面位址。

【位址表】記錄的 IP 位址可能是一個主機 IP 位址，也可能是一個網域多個 IP 位址，系統管理員可以自行設定一個易辨識的名字代表此一 IP 位址或區段。

基本上位址表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式。

註：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網路或目的網路。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】名詞解釋：

電腦名稱

系統管理員自訂一個易辨識的名字代表所設定之 IP 位址。

IP 位址

設定單一特定 IP 位址。

MAC 位址

將特定單一主機之網卡 MAC Address 與其 IP 對映，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。

DHCP IP 狀態

開啟此功能時，LAN 或 DMZ 下以自動透過 HERHSIANG HSecurity+內建的 DHCP 伺服器取得 IP 之 PC，就會被配發在位址表內指定之 IP 給相對映的 MAC Address。

4-1-1、內部 IP 位址

進入位址表後會出現內部 IP 位址列表，它把管理者設定的位址表條列出來。（圖 4-1）

圖 4-1 內部 IP 位址表

輔助選取：如果管理者不知道使用者 MAC 位址，可藉由輔助選取功能，快速列出目前 HSecurity+ 蒐集到的電腦名稱、IP 位址與 MAC 位址關係。

實體位置：如果內部有 SNMP 交換器或是協同防禦交換器，這裡會顯示這個 IP 實際的位置。

Port Lock：內部有協同防禦交換器，除了顯示這個 IP 實際的位置外，管理者還可以將這個 IP 跟 MAC 鎖在這個 PORT 上面，一但互鎖後，如果使用者將這部電腦換網路孔，則網路不會通。

進階：可以將這個位址表的內容匯入匯出。

管理者也可以在這個畫面直接修改電腦名稱、IP 位址及 MAC 位址，按儲存後就完成修改。（圖 4-2）

圖 4-2 內部 IP 位址表輔助選取

位址表新增方式有兩種方式：僅以 IP 位址方式設定、IP 與 MAC 號碼綁定方式設定

一：以 IP 位址方式設定

步驟1. 於【新增電腦名稱及 IP 位址】中新增下列設定：

- 【電腦名稱】輸入 Ping。
- 【IP 位址】輸入 192.168.1.202。
- 【設定方式】選擇僅設定 IP 位址 (圖 4-3)

圖 4-3 以 IP 方式設定位址表

二：以 IP 和 MAC 編號方式設定

步驟2. 於【新增電腦名稱及 IP 位址】中新增下列設定：

- 【電腦名稱】輸入 Ping-1。
- 【IP 位址】輸入 192.168.1.2。
- 【Mac】輸入 00:13:D3:CD:24:11。
- 取得 MAC：如果此部電腦有透過設備上網過，按下『取得 MAC』，設備會自動填入 MAC 位址。
- Get static IP address from DHCP Server. ☐：如果電腦是用 DHCP 取得 IP 位址，啟用這個功能，每次都會取得固定 IP 位址。
- 按下【新增】鈕。（圖 4-4）

圖 4-4 新增內部 IP 位址表

步驟3. 完成單筆 IP 位址表設定。（圖 4-5）

圖 4-5 完成內部 IP 位址表

內部網路群組新增

HSecurity+內部網路群組增加方式有五種：從位址表選擇成員、從範圍選擇成員、從IP/Mask 選擇成員、從 DHCP 用戶選擇成員及使用者自訂。（圖 4-6）

圖 4-6 內部網路群組建立方式

(一)從位址表選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入資訊部。
- 設定群組成員，從左列【所有使用者】名單挑選群組成員，移至右列【被選擇的使用者】。按下【新增】鈕。（圖 4-7）

圖 4-7 新增內部網路群

步驟2. 完成內部網路群組設定。（圖 4-8）

圖 4-8 完成內部網路群組

(二)從範圍表選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入業務部。
- 設定群組成員，可輸入網段內開始跟結束的 IP 位址，並可選擇是否要綁定 MAC 帳號。（圖 4-9）

圖 4-9 新增內部網路群

步驟2. 完成內部網路群組設定。（圖 4-10）

圖 4-10 完成內部網路群組

(三)從 IP/Mask 表選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入管理部。
- 設定群組成員，可直接輸入 IP 與網路遮罩。
- 可以啟用 IP-MAC 位址綁定的功能。（圖 4-11）

圖 4-11 新增內部網路群

步驟2. 完成內部網路群組設定。（圖 4-12）

圖 4-12 完成內部網路群組

(四)從 DHCHP 用戶選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入訪客 DHCP。
- 設定從 DHCP 用戶選擇成員，會直接套用管理員設定的 DHCP 配發範圍。
- 可以啟用 IP-MAC 位址綁定的功能。（圖 4-13）

圖 4-13 新增內部網路群

步驟2. 完成內部網路群組設定。（圖 4-14）

圖 4-14 完成內部網路群組

(五)使用者自訂

步驟1. 於【使用者自訂】中新增下列設定：

- 【群組名稱】輸入網路印表機。
- 設定群組成員，可直接輸入 IP 位址。
- 可以啟用 IP-MAC 位址綁定的功能。（圖 4-15）

圖 4-15 新增內部網路群，使用者自訂

(六)選擇 MAC 位址群組

步驟1. 於【使用者自訂】中新增下列設定：

- 【群組名稱】輸入 Ping。
- 設定群組成員，可直接輸入單筆或多筆 MAC 位址。
- 可以啟用 IP-MAC 位址綁定的功能。（圖 4-16）

圖 4-16 新增內部網路群，使用者自訂

4-1-2、非軍事區 IP 位址

非軍事區 IP 位址表

非軍事區位址表建立方式同之前我們所介紹內部 IP 位址建立方式一樣，在此單元我們僅以 NAT 模式下的 IP 結合 MAC 方式做示範。

步驟1. 於【新增電腦名稱及 IP 位址】中新增下列設定：

- 【電腦名稱】輸入 WEB SV。
- 【IP 位址/網路遮罩】輸入 172.172.1.250。
- 【MAC】可藉由輔助選取增加。
- 取得 MAC：如果此部電腦有透過設備上網過，按下『取得 MAC』，設備會自動填入 MAC 位址。
- 按下【新增】鈕。（圖 4-17）

圖 4-17 新增單筆非軍事 IP 位址表

步驟2. 完成單筆非軍事 IP 位址表設定。（圖 4-18）

圖 4-18 完成非軍事 IP 位址表建立

非軍事區群組新增

HSecurity+非軍事區群組增加方式有五種：從位址表選擇成員、從範圍選擇成員、從IP/Mask 選擇成員、從 DHCP 用戶選擇成員、使用者自訂。（圖 4-19）

圖 4-19 內部網路群組建立方式

(一)從位址表選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入 SERVER_GROUP。
- 設定群組成員，從左列【所有使用者】名單挑選群組成員，移至右列【被選擇的使用者】。按下【新增】鈕。（圖 4-20）

圖 4-20 新增非軍事區網路群

步驟2. 完成非軍事區群組設定。（圖 4-21）

圖 4-21 完成非軍事區網路群組

(二)從範圍表選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入 Switch_Group。
- 設定群組成員，可輸入網段內開始及結束 IP 位址，並可選擇是否要綁定 MAC 帳號。（圖 4-22）

圖 4-22 新增非軍事區網路群

步驟2. 完成非軍事區網路群組設定。（圖 4-23）

圖 4-23 完成非軍事區網路群組

(三)從 IP/MASK 選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入無線基地台。
- 設定群組成員，可直接輸入 IP 與網路遮罩(IP 範圍對應的遮罩有工具可以計算)。
- 可以啟用 IP-MAC 位址綁定的功能。（圖 4-24）

圖 4-24 新增非軍事內部網路群

步驟2. 完成非軍事網路群組設定。（圖 4-25）

圖 4-25 完成非軍事網路群組

(四)從 DHCHP 用戶選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入 MIS_DHCP。
- 設定從 DHCP 用戶選擇成員，會直接套用管理員設定的 DMZ DHCP 配發範圍。（圖 4-26）

圖 4-26 新增非軍事網路群

步驟2. 完成非軍事網路群組設定。（圖 4-27）

圖 4-27 完成非軍事網路群組

(五)使用者自訂

步驟2. 於【使用者自訂】中新增下列設定：

- 【群組名稱】輸入網路印表機。
- 設定群組成員，可直接輸入 IP 位址。
- 可以啟用 IP-MAC 位址綁定的功能。（圖 4-28）

圖 4-28 新增內部網路群，使用者自訂

(六)使用者自訂

步驟1. 於【使用者自訂】中新增下列設定：

- 【群組名稱】輸入會計人員。
- 設定群組成員，可直接輸入 MAC 位址。（圖 4-29）

圖 4-29 新增內部網路群，使用者自訂

4-1-3、外部 IP 位址

外部 IP 位址表

步驟1. 於【外部 IP 位址表】中新增下列設定：

- 【電腦名稱】輸入 Ping_HOME。
- 【IP 位址/網路遮罩】輸入 112.34.56.78/255.255.255.255，按下【新增】鈕。(圖 4-30)

圖 4-30 單筆外部 IP 位址表

步驟2. 完成單筆外部 IP 位址表設定。(圖 4-31)

圖 4-31 單筆外部 IP 位址表建立

外部網路群組

外部網路群組建立方式有五種：從位址表選擇成員、從範圍選擇成員、從 IP/Mask 選擇成員、輸入指定 IP 選擇成員以及輸入 Domain 來解出對方 IP。

(一)從位址表選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入 RD_HOME。
- 設定群組成員，從左列【所有使用者】名單挑選群組成員，移至右列【被選擇的使用者】。按下【新增】鈕。（圖 4-32）

圖 4-32 新增外部網路群組

步驟2. 完成外部網路群組設定。（圖 4-33）

圖 4-33 完成外部網路群組

(二)從範圍表選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入 XXX_GOV(某某政府單位)。
- 設定群組成員，可輸入網段內開始及結束 IP 位址 。(圖 4-34)

圖 4-34 新增外部網路群

步驟2. 完成外部網路網路群組設定。(圖 4-35)

圖 4-35 完成外部網路群組

(三)從 IP/MASK 選擇成員

步驟1. 於【新增群組名稱及選擇成員】中新增下列設定：

- 【群組名稱】輸入 XXX_GOV。
- 設定群組成員，可直接輸入 IP 與網路遮罩。（圖 4-36）

圖 4-36 新增外部網路群組

步驟2. 完成外部網路群組設定。（圖 4-37）

圖 4-37 完成外部網路群組

(四)使用者自訂 Domain

步驟2. 於【使用者自訂】中新增下列設定：

- 【群組名稱】輸入 Facebook。
- 設定群組成員，可直接輸入目標網域，HSecurity+會去解出對方網域下所帶的 IP。（圖 4-38）

圖 4-38 新增外部網路群組，使用者自訂

註 1：LAN 或 DMZ 下以自動透過 HERHSIANG HSecurity+內建的 DHCP 伺服器取得 IP 之 PC，就會被配發在位址表內指定之 IP 給相對映的 MAC Address。

註 2：在【位址表】之【內部 IP 位址表】功能中，HERHSIANG HSecurity+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 IP 位址表】、【非軍事區 IP 位址表】一樣有代表整個網域的 Outside_Any 與 DMZ_Any 預設位址表設定。

註 3：【位址表】之【內部 IP 位址表】與【非軍事區 IP 位址表】其設定模式與【內部 IP 位址表】相同；唯一的不同是【外部 IP 位址表】無法設定 MAC 位址。

4-2、服務表

TCP 協定和 UDP 協定提供各種不同的服務，每一個服務都有一個 TCP 埠(TCP Port)號碼或 UDP 埠(UDP Port)號碼代表，如 TELNET(23)，FTP(21)，SMTP(25)，POP3(110)，...等。

基本服務表包含了比較常用已預告定義的 TCP 服務或 UDP 服務。此類服務不能修改也不可刪除。此外使用者也可依自己的需求到自訂服務表設定適當 TCP 埠和 UDP 埠號碼。在自訂服務時，客戶端埠(Client Port)設定的區間一般為 1024：65535，伺服器端埠(Server Port)號碼則是設定在 0:65535 之間。

HSecurity+在此單元中，將一些常用的網路服務列入各項表列的服務選單中（基本服務、自訂服務與服務群組）。系統管理員只需依照下列操作說明，將網路協定與出入埠號碼定義在各種網路通訊應用中，用戶端即可與各種不同伺服器連線，傳輸資料。

如何運用服務表

系統管理員可以在【服務表】的【服務群組】選項中，新增服務群組名稱，將要提供的服務包含進去。

有了服務群組的功能，管理員在制訂管制條例時可以簡化許多流程。例如，有 10 個不同 IP 位址可以對伺服器存取 5 個不同的服務，如 HTTP、FTP、SMTP、POP3 和 TELNET，如果不使用服務群組的功能，總共需制定 10x5=50 條管制條例，但使用服務群組名稱套用在服務選項上，則只需一條管制條例即可達到 50 條管制條例的功能。

4-2-1、基本服務表

【服務表】名詞解釋：

基本服務: : 視窗表格內圖示與名詞名稱：**(圖 4-39)**

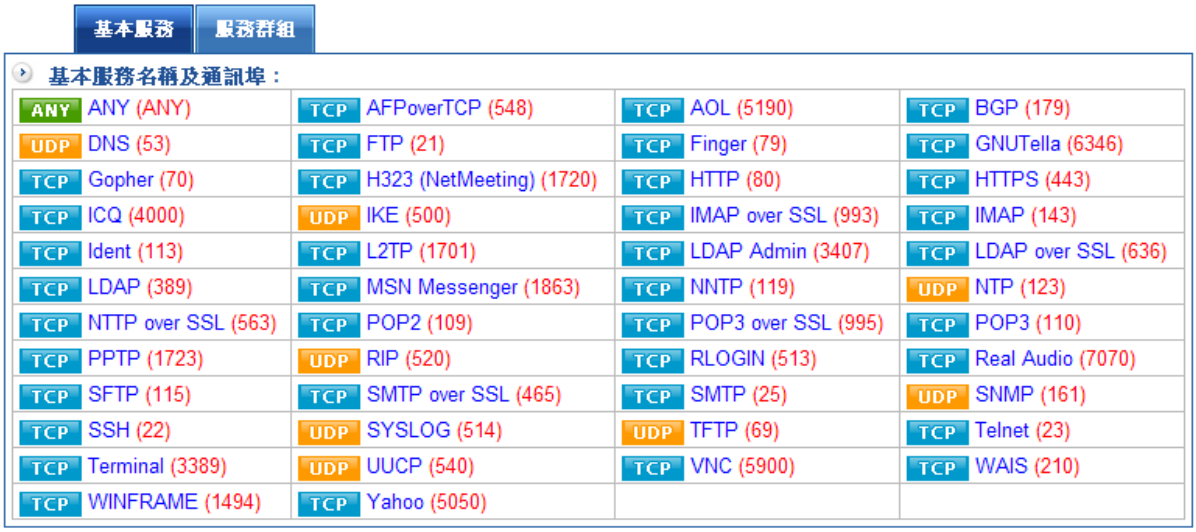

圖 4-39 基本服務表

基本服務列表：

圖示	說明
ANY	任何服務。
TCP	TCP 服務，如：Gepher、ICQ、Ident、LDAP、NTTP over SSL、PPTP、SFTP、SSH、Terminal、WINFRAME、AFPoverTCP、FTP、H323、L2TP、MSN Messenger、POP2、SMTP over SSL、Yahoo、AOL、Finger、HTTP、IMAP over SSL、LDAP Admin、NNTP、POP3 over SSL、RLOGIN、SMTP、VNC、BGP、GNUTella、HTTPS、IMAP、LDAPover SSL、POP3、Real Audio、Telnet、WAIS
UDP	UDP 服務，如：DNS、TFTP、NTP、SNMP、IKE、SYSLOG、RIP、UUCP 等。

服務群組名稱

系統管理員可在此為自訂的服務命名。

通訊協定

設備彼此之間溝通所需求之協定，一般常用為 TCP 和 UDP 模式。

使用的通訊埠

自訂服務時，客戶端埠(Client Port)設定的區間一般為 1024：65535，伺服器端埠(Server Port)號碼則是設定在 0:65535 之間。

4-2-2、服務群組

新增單筆服務表

步驟1. 在【服務表】的【服務群組】功能中，新增下列設定：（圖 4-40）

- 設定【服務群組名稱】為預定的名稱 Port_88。
- 【通訊協定】選擇為 TCP，【使用的通訊埠】設為 88：88，按下【新增】鈕。
- 輔助選取：按下『輔助選取』按鈕，系統會開啟，讓管理者選取預設的服務。
- 系統預設為 8 組通訊埠組合，按下『More』按鍵後可以擴充到 16 組。

圖 4-40 自訂服務 Web UI 設定畫面

完成後列表如下：（圖 4-41）

圖 4-41 VoIP 自訂服務設定完成

新增服務群組

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【服務表】的【服務群組】功能中，新增下列設定：

- 按下【新增】鈕。（圖 4-42）
- 設定【名稱】為自訂的名稱 Web_Port。

圖 4-42 新增 Main_Server 服務群組

- 藉由輔助選取，在【可選取的服務】欄位中選取 HTTP、HTTPS、DNS，按下【選擇】鈕，每次只能選取一個服務。（圖 4-43）

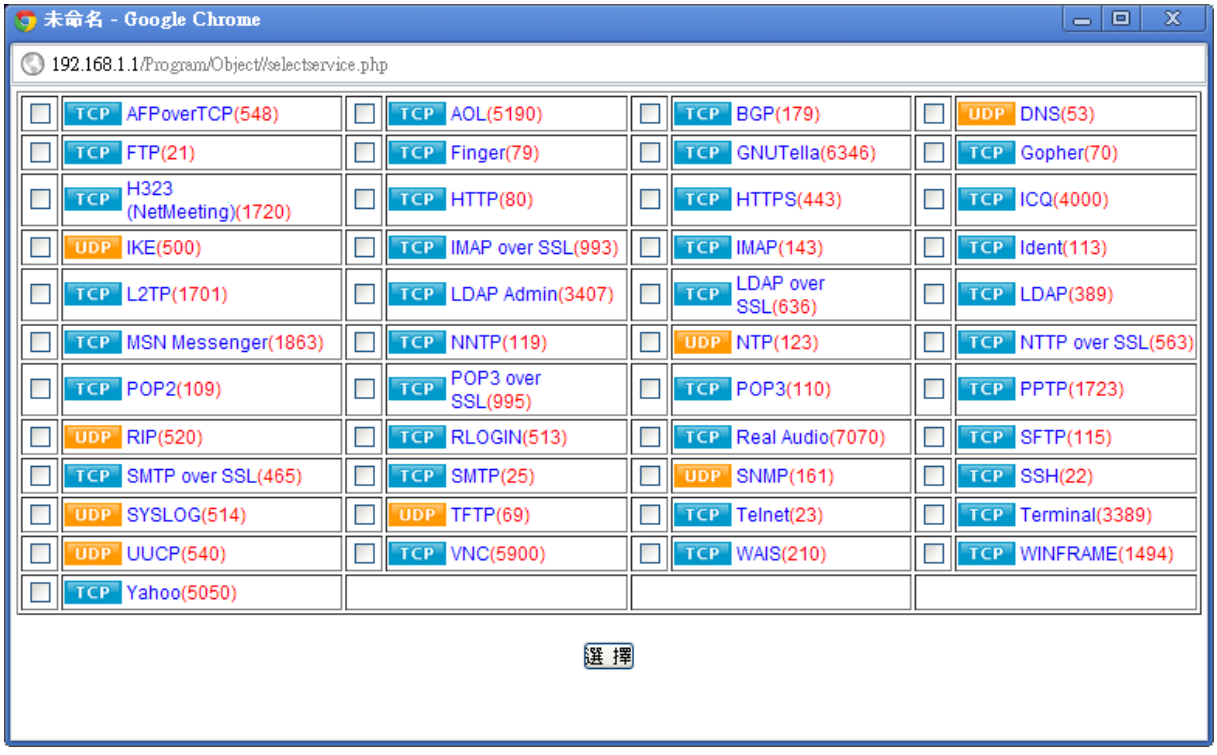

圖 4-43 藉由輔助選取新增服務群組

完成後列表如下：（圖 4-44）

圖 4-44 完成服務群組新增

4-3、時間表

HSecurity+在此單元中提供系統管理員，在時間表中定義網路系統連結與執行的時間區段。以便在【管制條例】功能中，選擇特定時間內開放資料封包的出入。利用時間表的自動執行功能，系統管理員可以節省許多管理時間，同時讓網路系統發揮最大的效能。

如何運用排程表

系統管理員可利用時間表功能，設定系統在多個不同的時間區段內，自動執行設定封包流向的【管制條例】。

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【時間表】功能中，新增下列設定：

- 設定時間表名稱為【時間】。
- 設定每天時間表運作之時間，包含開始時間及結束時間，按下【新增】鈕，完成設定。（圖 4-45）

圖 4-45 時間表 Web UI 設定畫面

完成後列表如下：（圖 4-46）

圖 4-46 時間表設定完成

註：HSecurity+時間表讓管理者可以一目了然掌握控管的時間。

步驟2. 將時間表套用至【管制條例】上。（圖 4-47）

圖 4-47 建立 LAN 對 WAN 管制條例設定

完成後列表如下，在管制行為中會出現 的圖示 ：（圖 4-48）

圖 4-48 完成時間表套用至管制條例設定

註 1：時間表必須配合【管制條例】使用。

註 2：當您設定全天候時間(00:00~24:00)，則建立該筆時間表時會以 表示。

4-4、頻寬管理

HSecurity+經由頻寬表的參數設定，可以控管其上傳下載的頻寬，管理人員可依據外部網路所能提供的頻寬，來設定

下載速度： 保證頻寬 及 最大頻寬

上傳速度： 保證頻寬 及 最大頻寬

優先權：設定 上傳 或 下載 未設定使用的頻寬分配優先權

HSecurity+依據不同頻寬表，來設定對外的頻寬，並藉由管制條例選擇適合的頻寬表設定加以控管，可有效分配頻寬，便利系統管理員，針對所能使用的頻寬達到最佳之利用。

HSecurity+ 採用 IMQ 技術，所以跟傳統作 NAT / Routing 的 linux 伺服器的頻寬管理機制不一樣，他可以單獨控制每一個網路介面的上、下載速度。

例如，可以控制 LAN 介面的上、下載速度，就可以控制內部用戶的上、下載速度，而不需要將上、下載速度分別在 LAN 及 WAN 的介面上。

目前 HSecurity+ 支援 3 種頻寬控制機制，分別是『每個條例能使用的頻寬』、『每個內部來源 IP 能使用的頻寬』、『每個外部來源 IP 能使用的頻寬』。

其中『每個內部來源 IP 能使用的頻寬』又可以選擇啟用 Smart QoS 機制，啟用這個機制後，系統會根據內部使用者目前開機狀態，每隔 2 分鐘，根據剩餘的頻寬，動態調整。

Smart QoS 機制只控制內部網路或是非軍事區的介面頻寬，因為 IMQ 技術的關係，所以控制單一個網路介面就可以完整控制上、下載速度。

【頻寬管理】名詞解釋：

介面

指內部網路 LAN、非軍事區網路 DMZ、外部網路 WAN 1 、WAN2 的線路。

上傳速度

所申請線路運用的上傳頻寬之 保證頻寬 及 最大頻寬 設定。

下載速度

所申請線路運用的下載頻寬之 保證頻寬 及 最大頻寬 設定。

優先權

設定 上傳 或 下載 未使用的頻寬分配優先權，分成 1 ~7 個不同等級，數字越小，優先權越高。

保證頻寬

該頻寬表的最少基本頻寬，套用此頻寬表的【管制條例】，將會至少保留所設定的頻寬。

最大頻寬

該頻寬表的最大頻寬，有套用此頻寬表的【管制條例】其頻寬將不會超過所設定的頻寬。

Smart QoS

根據條例下的電腦開機數量，每 2 分鐘動態的上調或下降每個人可以分配的頻寬。

模式一、每個條例能使用的頻寬

套用此頻寬管理，條例上的所有 IP 位址及服務均共用設定的頻寬。

步驟1. 在【頻寬表】功能中，新增下列設定：

- 按下【新增】鈕。（圖 4-49）
- 於【名稱】處設定此頻寬表之名稱。
- 選擇頻寬設定模式為『每個條例能使用的頻寬』。
- 在網路介面 LAN、DMZ、WAN1、WAN2 中，輸入所要限定之頻寬大小。
- 決定頻寬表之【優先權】，按下【新增】鈕。

圖 4-49 頻寬表 Web UI 設定畫面

模式二、每個內部來源 IP 能使用的頻寬

套用此頻寬管理，條例上的每一個 IP 位址及服務，可以分配到的頻寬，例如，分配給每個 IP 位址可以下載 512K，當內部有 100 台電腦上網時，總頻寬可能用到 512K*100 = 51.2Mbps 的需求。

步驟1. 在【頻寬表】功能中，新增下列設定：

- 按下【新增】鈕。（圖 4-50）
- 於【名稱】處設定此頻寬表之名稱。
- 選擇頻寬設定模式為『每個內部來源 IP 能使用的頻寬』。
- 在網路介面 LAN、DMZ、WAN1、WAN2 中，輸入所要限定之頻寬大小。
- 決定頻寬表之【優先權】，按下【新增】鈕。

圖 4-50 內部每個來源 IP 頻寬設定

啟用 Smart QoS 機制後，除了內部網路/非軍事區外，其他的頻寬設定都無法輸入，因為會自動調整分配到 WAN 的頻寬，所以一開始給 LAN 的上、下載速度，系統會自動調整分配頻寬到 WAN 的介面。

模式三、每個外部來源 IP 能使用的頻寬

套用此頻寬管理，條例上的每一個外部來源 IP 位址，可以分配到的頻寬，例如，不希望某一個 外部 IP 位址將對外伺服器的頻寬用完，就可以套用此規則，來自外面的 IP 位址對伺服器最多只能用多少上、下載速度，確保頻寬服務正常。

步驟1. 在【頻寬表】功能中，新增下列設定：

- 按下【新增】鈕。（圖 4-51）
- 於【名稱】處設定此頻寬表之名稱。
- 選擇頻寬設定模式為『每個外部來源 IP 能使用的頻寬』。
- 在網路介面 LAN、DMZ、WAN1、WAN2 中，輸入所要限定之頻寬大小。
- 決定頻寬表之【優先權】，按下【新增】鈕。

圖 4-51 外部每個來源 IP 頻寬設定

套用完畢後，在頻寬表列表中會清楚地列出，每一個頻寬表的控制方式及方法。（圖 4-52）

None：每個條例能使用的頻寬。

Outgoing：每個內部來源 IP 能使用的頻寬。

Outgoing (Smart) ：每個內部來源 IP 能使用的頻寬，並啟用 Smart Qos 機制。

Incoming：每個外部來源 IP 能使用的頻寬。

選擇	QoS 名稱	優先權	來源屬性	介面	User 下載速度		User 上傳速度	
☐	每個條例能使用的頻寬	1	None	內部網路				
				非軍事區				
				外部網路_1	1024(Kbps)	2048(Kbps)	1024(Kbps)	2048(Kbps)
				外部網路_2				
☐	每個內部來源IP能使用的頻寬	1	Outgoing	內部網路	10240(Kbps)	10240(Kbps)	10240(Kbps)	10240(Kbps)
				非軍事區				
				外部網路_1				
				外部網路_2				
☐	每個外部來源IP能使用的頻寬	1	Incoming	內部網路				
				非軍事區				
				外部網路_1	2048(Kbps)	4096(Kbps)	2048(Kbps)	4096(Kbps)
				外部網路_2				
☐	Smart QoS	1	Outgoing (Smart) 40%	內部網路	10240(Kbps)	10240(Kbps)	10240(Kbps)	10240(Kbps)
				非軍事區				
				外部網路_1				
				外部網路_2				

圖 4-52 頻寬列表說明

4-5、應用程式管理

應用程式管理的項目非常多，但是有很多是使用者比較少再使用的，如果將這些管制全開的話，可能或多或少會影響系統運作效能。因此，為了維持系統運作的順暢，HSecurity+將應用程式區分為常用與不常用類別，方便管理者進行管制：

常用：P2P 軟體管制、即時通訊軟體管制、VOIP 管制、WEB 的應用管制、WEB Mail 管制、娛樂軟體管制、其他

不常用：P2P 軟體管制、即時通訊軟體管制、WEB 副檔名下載管制、WEB 副檔名上傳管制、影音應用軟體管制、娛樂軟體管制、防病毒、惡意軟體管制、禁用股票軟體、其他

（一） 常用：

P2P 軟體管制：

管制 ares (Ares)、bittorrent (Bit Torrent)、edonkey (Edonkey)、ezpeer (ezpeer)、foxy (Foxy)、gogobox (GoGoBox)、clubbox(Clubbox)、imesh (iMesh)、soulseek (P2P)、winmx (WinMX)、xunlei(Thunder5)使用。

即時通訊軟體：

管制 aim (ICQ/AIM)、googletalk (Google Talk)、msnmessenger (MSN)、qq (QQ)、webim (WebIM)、yahoo (Yahoo)登入的權限。

VOIP 管制：

管制 h323 (H.323)、jabber (An open instant messenger protocol)、sip (SIP)使用的權限。

WEB 的應用管制

http-audio (Audio over HTTP)、http-video (Video over HTTP)

WEB Mail 管制

webmail_163 (163/126/Yeah)、webmail_gmail (Gmail)、webmail_hinet (Hinet)、webmail_live (Hotmail)、webmail_pchome (PChome)、webmail_qq (QQ)、webmail_seednet (Seednet)、webmail_sohu (Sohu)、webmail_yahoo (Yahoo)

娛樂軟體管制

管制 ppstream (PPStream)、cradio (Tornado Broadcast)、hinedo (Hinedo Broadcast)、qqlive (QQLive)、funshion (Funshion Video)、kuaibo (Kuaibo Video)、pplive (PPLive)、baofeng (baofeng)

其他管制

管制 facebook(Facebook)、netpas (NETPAS ACC)、phproxy (HTTP proxy written in PHP)、rdp (Remote Desktop)、vnc (VNC)、teamviewer(TeamViewer)

（二） 不常用

P2P 軟體管制

管制 100bao (100bao)、fasttrack (Fasttrack)、freenet (Anonymous information retrieval)、gnotella (Gnotella)、gnucleuslan (LAN-only P2P)、gnutella (P2P)、goboogy (Korean P2P)、hotline (An old P2P)、limewire (Limewire)、mactella (gnutella)、morpheus (Morpheus)、mute (MUTE)、mxie (bittorrent, edonkey)、napster (P2P)、openft (A P2P filesharing protocol)、poco (Chinese P2P)、soribada (A Korean P2P)、thecircle (P2P)、vagaa (P2P)、tesla (P2P)、applejuice (AppleJuice)、audiogalaxy (AudioGalaxy)、bearshare (BearShare)、directconnect (DirectConnect)、kazaa (KaZaa)、

即時通訊軟體管制

管制 aimwebcontent (AIM web content)、chikka (Chikka - SMS service)、cimd (SMSC protocol by Nokia)、irc (Internet Relay Chat)、msn-filetransfer (MSN File Transfer)、stun (Simple Traversal of UDP Through NAT))使用的權限。

WEB 副檔名下載管制

exe、flash、gif、html、jpeg、mp3、ogg、pdf、perl、png、postscript、rar、rpm、rtf、tar、zip。

WEB 副檔名上傳管制

uexe、uflash、ugif、uhtml、ujpeg、ump3、uogg、updf、uperl、upng、upostscript、urar、urpm、urtf、utar、uzip。

影音應用軟體管制

Live365(An Internet radio site)、feplaytv-ivs(ReplayTV Internet Video Sharing)、shoutcast(streaming audio)。

娛樂軟體管制

armagetron (Armagetron Advanced)、battlefield1942 (Battlefield 1942)、battlefield2 (Battlefield 2)、battlefield2142 (Battlefield 2142)、counterstrike-source (network game)、dayofdefeat-source (game Half-Life2 mod)、doom3 (Doom3-computer game)、halflife2-deathmatch (Half-Life 2)、liveforspeed (A racing game)、mohaa (Medal of Honor Allied Assault)、quake-halflife (Half-Life 1)、quake1 (Quake)、subspace (Subspace)、teamfortress2、worldofwarcraft (World of Warcraft)、xboxlive (Xbox Live)登入的權限。

防病毒、惡意軟體管制：

管制 code_red、nimda。

禁用股票軟體：

管制 cjis (中投卓越)、dqs (大趨勢)、dzh (大智慧)、gtja (國泰君安)、gzs (廣州證券)、hexun (和訊股道)、pobo (博易大師)、qianlong (錢龍)、stockstar (證券之星)、westfutu (西部期貨)、whsp (文華財經)。

其他

ciscovpn (Cisco VPN server)、citrix (Citrix ICA)、ncp (Novell Core Protocol) pcanywhere (pcAnywhere)、 radmin (Famatech Remote Administrator)、 ssh (Secure SHell)、uucp (Unix to Unix Copy)、validcertssl、httpcachehit (Proxy Cache hit)、httpcachemiss (Proxy Cache miss)、http-dap (Download Accelerator Plus)、 http-freshdownload (Fresh Download)、 http-itunes (iTunes)、 http-rtsp (RTSP tunneled)、 skypetoskype (Skype-to-Skype)、 teamspeak (Teamspeak)、ventrilo (Ventrilo)

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【應用程式管理】之【P2P 軟體】功能中，設定下列資料：

- 管制名稱設定為【P2P 管制】。
- 在應用程式分類中選 P2P 軟體，選擇要管制的 P2P 軟體或者是全選，再按【新增】鈕，就完成一個 P2P 的管制。（圖 4-53）

圖 4-53 點對點軟體管製錶設定畫面

完成後列表如下：（圖 4-54）

圖 4-54 完成 P2P 管制設定畫面

步驟2. 於【應用程式管制】條例裡，可立即看出目前 P2P 管制項目有哪些。（圖 4-55）

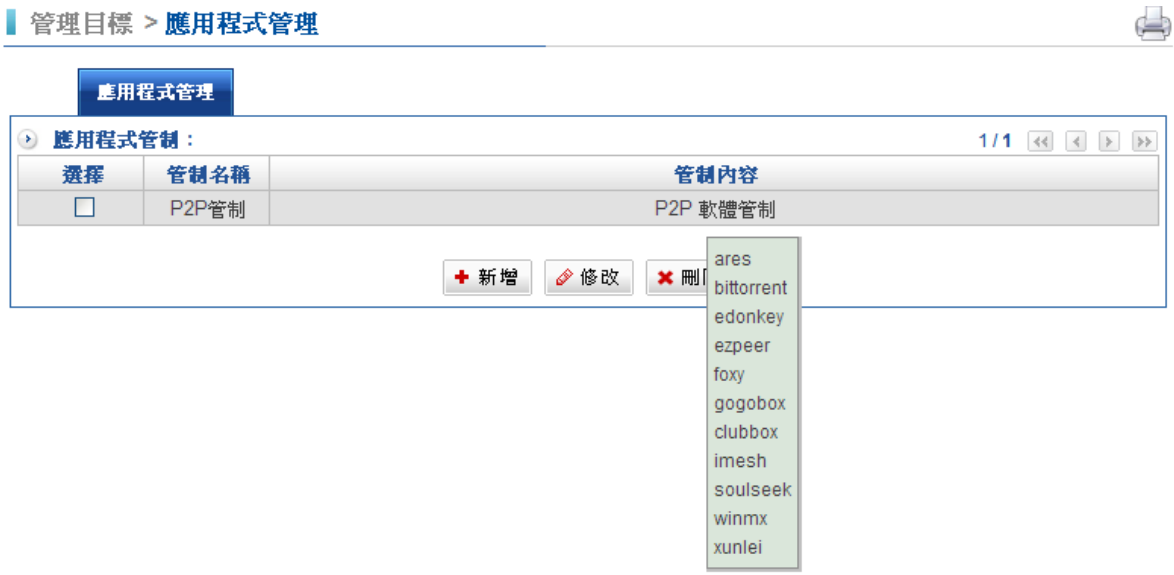

圖 4-55 顯示目前控管哪些 P2P 管制項目

步驟3. 就算管制條例目前正在運作，管理者還是可以直接從應用程式管理直接增加管制項次，點選 P2P 欄位直接選取，按下選擇鍵後，新的應程式管制馬上生效。

即時通訊服務管制

步驟1. 在【應用程式管理】之【即時通訊軟體】功能中，設定下列資料：

- 管制名稱設定為【即時通訊管制】。
- 在應用程式分類中選即時通訊軟體，選擇要管制的軟體或者是全選，再按【新增】鈕，就完成一個即時通訊軟體的管制。（圖 4-56）

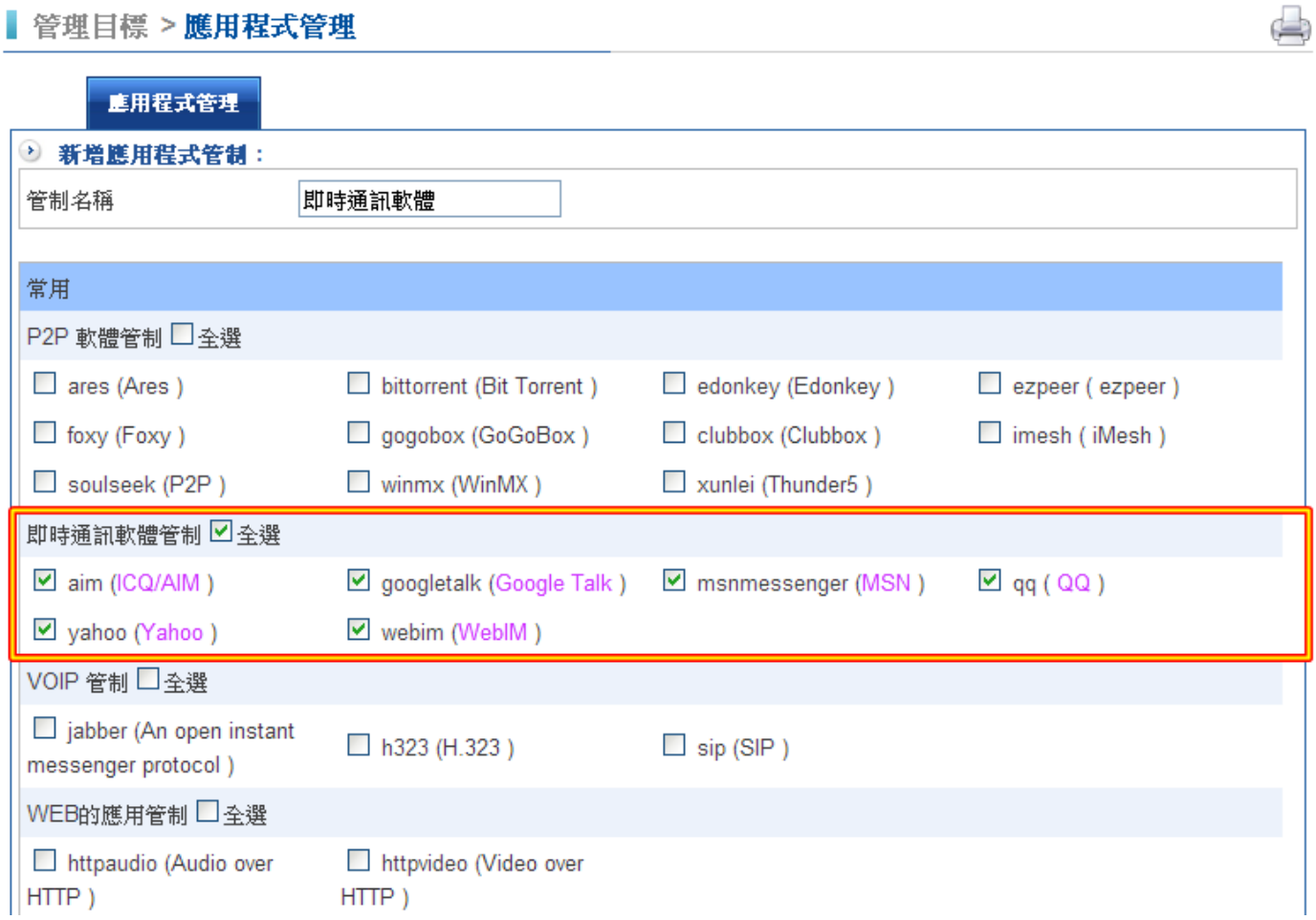

圖 4-56 即時通訊管製錶設定畫面

步驟2. 於【應用程式管制】條例裡，可立即看出目前即時通訊管制項目有哪些。（圖 4-57）

圖 4-57 顯示目前控管哪些即時通訊管制項目

步驟3. 就算管制條例目前正在運作，管理者還是可以直接從應用程式管理直接增加管制項次，點選即時通訊欄位直接選取，按下選擇鍵後，新的應程式管制馬上生效。

WEB 應用服務管制

步驟1. 在【應用程式管理】之【WEB 的應用管制】功能中，設定下列資料：

- 管制名稱設定為【WEB 的應用管制】。
- 在應用程式分類中選 WEB 應用，選擇要管制的軟體或者是全選，再按【新增】鈕，就完成一個 WEB 的應用管制。（圖 4-58）

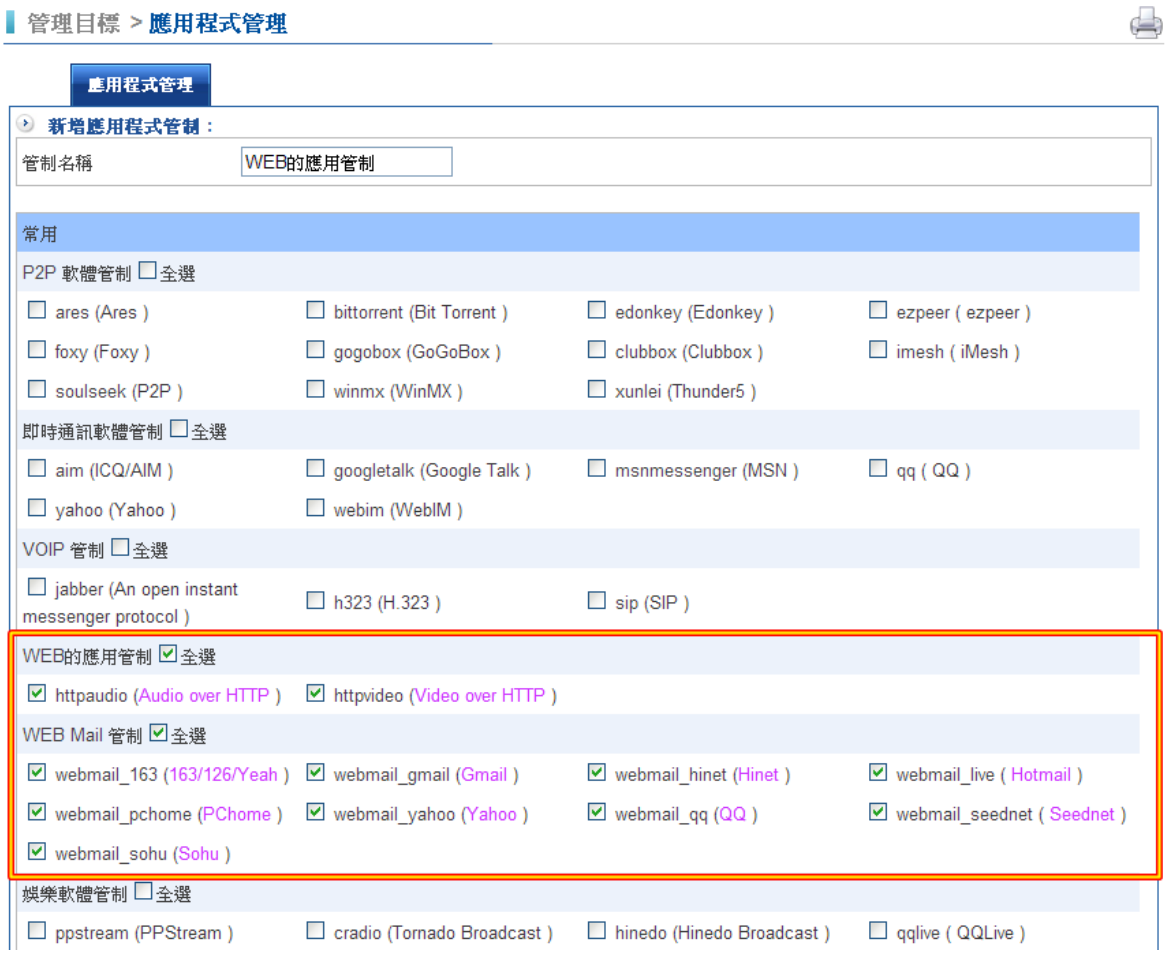

圖 4-58 HTTP 管制設定畫面

步驟2. 於【應用程式管制】條例裡，可立即看出目前 WEB 管制項目有哪些。（如 4-59）

圖 4-59 顯示目前控管哪些 WEB 應用程式

步驟3. 就算管制條例目前正在運作，管理者還是可以直接從應用程式管理直接增加管制項次，點選 WEB 應用欄位選取，按下選擇鍵後，新的應程式管制馬上生效。

娛樂軟體管制

步驟1. 在【應用程式管理】之【娛樂軟體】功能中，設定下列資料：

- 管制名稱設定為【娛樂軟體管制】。
- 在應用程式分類中選娛樂軟體，不勾選【輔助選取】鈕，選擇要管制的軟體或者是全選，再按【新增】鈕，就完成一個娛樂軟體的管制。（圖 4-60）

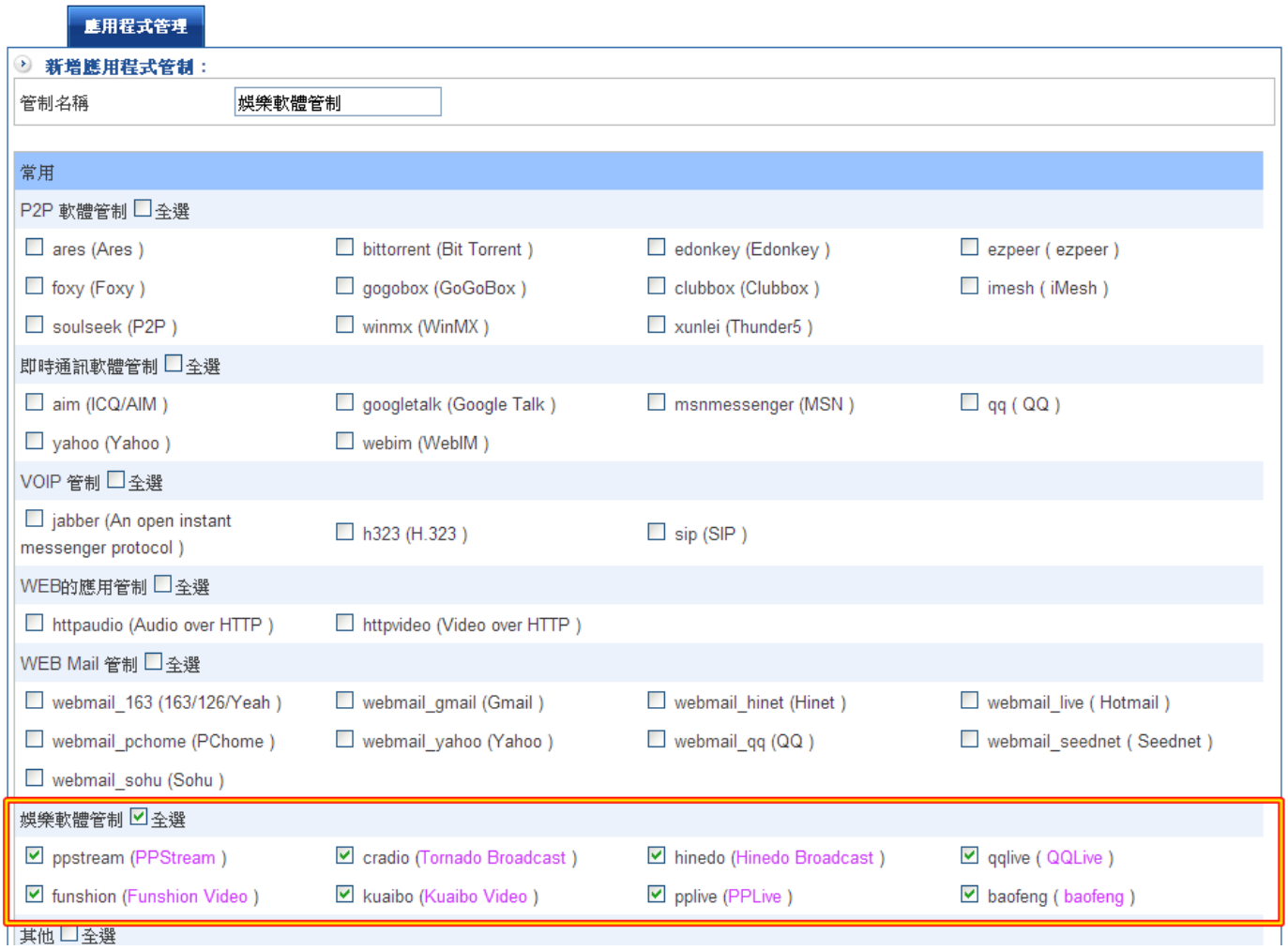

圖 4-60 設定娛樂軟體管制名稱

步驟2. 於【應用程式管制】條例裡，可立即看出目前娛樂軟體管制項目有哪些。（圖 4-61）

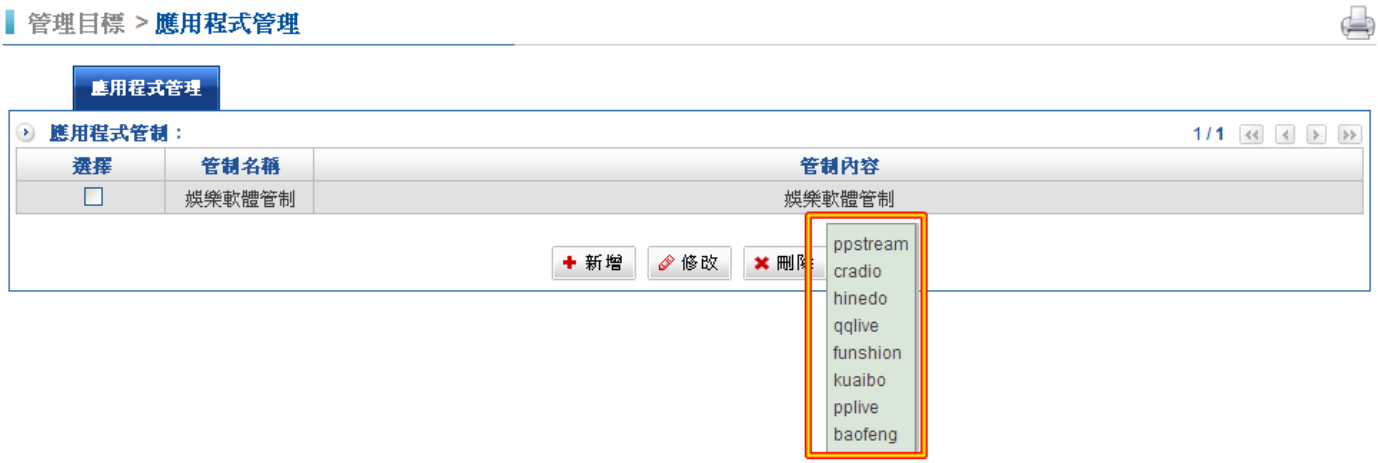

圖 4-61 顯示目前控管哪些娛樂軟體

步驟3. 就算管制條例目前正在運作，管理者還是可以直接從應用程式管理直接增加管制項次，點選娛樂軟體欄位選取，按下選擇鍵後，新的應程式管制馬上生效。

其他通訊管制

在【應用程式管理】之【其他】功能中，設定下列資料，動作跟 P2P 體管制一樣。

4-6、URL 管制

可控管使用者瀏覽的網站，避免員工摸魚、降低工作效率；亦可預先過濾惡意網站，避免使用者在不知情的狀況下遭植入惡意程式、病毒，以確保區域網路安全。

系統管理員可透過完整網功能變數名稱稱、關鍵字、針對特定網站作「允許」或「拒絕」進入的制訂，URL 名稱必須為完整的功能變數名稱名稱或者關鍵字名稱，並透過管制條例達到管制功能。

HSecurity+對網站的控管基準，分為「白名單」、「黑名單」與「群組」三種。

（一）【群組】：系統管理員可組合所設定的【白名單】、【黑名單】項目，制定網站管制規則。

（二）【黑名單】：系統管理員可透過完整網功能變數名稱稱、關鍵字或萬用字元（ * ），設定「阻擋」存取的特定網址。

（三）【白名單】：系統管理員可透過完整網功能變數名稱稱、關鍵字或萬用字元（ * ），設定「開放」存取的特定網址。

【位址表】名詞解釋：

URL 設定

管理者可以輸入關鍵字眼進行 URL 管制，例如要管制最夯的 Facebook 網站，只要輸入 facebook 關鍵字即可，需注意事項，系統只針對網功能變數名稱稱進行關鍵比對，在網功能變數名稱稱後來所帶位址並不能有效過濾阻擋。

例如：下列網址所列，HSecurity+只會針對藍色名稱位址進行關鍵比對過濾，而/後方所列網址並不能過濾阻擋。並需列入詳細網址才能管制。

http://apps.facebook.com/farmgame_tw/index.php?ref=bookmarks

阻擋結果網頁設定

可在此設定連線被被阻擋的網站時，於瀏覽器所顯示的警訊。

黑名單設定

系統管理員可透過完整網功能變數名稱稱、關鍵字或 IP 位址，設定組檔存取的特定網址。

白名單設定

系統管理員可透過完整網功能變數名稱稱、關鍵字或 IP 位址，設定開放存取的特定網址。

預設黑名單

可分為語言暴力、線上影音、藥品、賭博、駭客、成人網站、代理過濾器、轉頁、後門程式、不信任網站、暴力網站與非法盜版。

預設頁面阻擋設定

可在此設定 HSecurity+阻擋網站時，於使用者瀏覽器所顯示的警訊。

比對模式

提供兩種比對模式，分別為「完整」與「模糊」。完整模式為需全部都符合才行，模糊模式是只要關鍵字有部分符合就可以了。

例如：要封鎖 yahoo 網站

如果使用完整模式，則需輸入 www.yahoo.com 或 www.yahoo.com.tw 兩種網址，如選擇模糊模式，則只要輸入 yahoo，就可以將相關與 yahoo 網址有關的封鎖。

4-6-1、URL 管制

範例一：僅允許內部使用者存取特定網站

目的

僅開放特定網站可進入

步驟大綱

先將欲開放網站一一加入網站管制中，可輸入「完整網功能變數名稱稱」、或「關鍵字」名稱 。（如：www.kcg.gov.tw 或 gov）。

在所有欲開放的網站設定完成後，於網站管制中，動作行為設定為「允許」指令，並在下一條條例將所有的 HTTP 服務設為拒絕，則除了開放網站外，其他網站一律禁止 。

步驟1. 在【URL 管理】的【黑白名單設定】功能中，新增並鍵入下列資料：

- 【名稱】設為 White_list
- 【名單模式】選取 白名單模式
- 自訂黑白名單設定中，URL 白名單輸入 google，每一行為一筆資料，如果想管理多個 URL，可以在下一行中輸入新的功能變數名稱。（圖 4-62）
- 也可自行設定 IP 白名單。

圖 4-62 URL 管制建置畫面

步驟2. 於【URL 設定】中設定一筆【允許網站】群組名稱。(圖 4-63)

步驟3. 管理者可以選擇是否要啟動自訂頁面阻擋，並設定顯示頁面的內容與主題名稱。

圖 4-63 設定 URL 群組名稱

步驟4. 套用管制條例，於【管制條例】之【 LAN 對 WAN 管制】功能中新增一條管制條例，並套用【URL 管制】，並把動作設為『允許』。(圖 4-64)

圖 4-64 套用 URL 管制條例

步驟5. 再新增一條所有其他的 HTTP 要求全部禁止。

步驟6. 於【管制條例】之【LAN 對 WAN 管制】功能中，完成僅允許內部使用者透過管制條例存取特定網站的資料，如下圖所示：（圖 4-65）

圖 4-65 完成 url 管制之管制條例設定

範例二：禁止內部使用者存取特定網站

目的

禁止內部用戶進入特定網站

步驟大綱

先將欲管制網站一一加入網站管制中，可輸入「完整網功能變數名稱稱」、或「關鍵字」名稱 。（如：www.kcg.gov.tw 或 gov）。

在所有欲禁止的網站設定完成後，於網站管制中，動作行為設定為「禁止」指令，則所有人要進入這些網站都會被禁止掉。

步驟1. 在【URL 管理】的【黑白名單設定】功能中，新增並鍵入下列資料：

- 【名稱】設為 Black_List 限制
- 【名單模式】選取 黑名單模式
- 自訂黑白名單設定中，URL 黑名單輸入 facebook，每一行為一筆資料，如果想管理多個 URL，可以在下一行中輸入新的功能變數名稱。（圖 4-66）
- 也可自行設定 IP 黑名單。

圖 4-66 URL 管制建置畫面

步驟2. 於【URL 設定】中設定一筆【不允許網站】群組名稱。（圖 4-67）

- ◆ 勾選【啟動自訂頁面阻擋】
- ◆ 設定阻擋主題名稱及欲顯示的內容，管理者可先藉由顯示瀏覽網頁設定。
- ◆ 名單選取【Black_List】
- ◆ 按下新增鈕，完成 URL 群組名稱設定。（圖 4-68）

圖 4-67 設定 URL 群組名稱

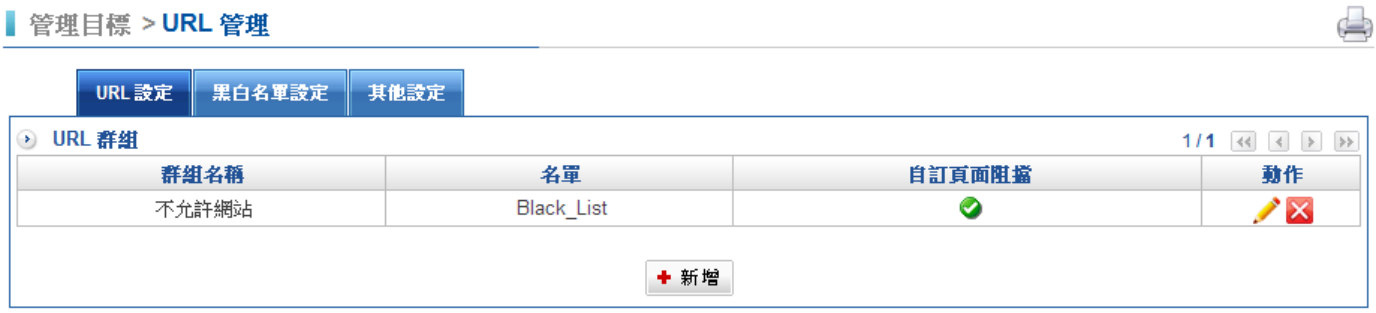

圖 4-68 完成 URL 群組名單設定

步驟3. 於【管制條例】之【 LAN 對 WAN 管制】功能中新增一條管制條例，並套用【URL 管制】，並把動作設為『允許』。（圖 4-69）

圖 4-69URL 管制之管制條例設定

步驟4. 於【管制條例】之【LAN 對 WAN 管制】功能中，完成禁止內部使用者透過管制條例存取特定網站的資料，如下圖所示：（圖 4-70）

圖 4-70 完成 url 管制之管制條例設定

註 1：如果要優先管制特定使用者上網情形，需先將管制條例優先權往前面調整。

4-6-2、其他設定

可在此設定連線被被阻擋的網站時，於瀏覽器所顯示的警訊。（圖 4-71）

圖 4-71 頁面阻擋初值設定

當內部使用者連線至阻擋的網站時，會顯示下列畫面。（圖 4-72）

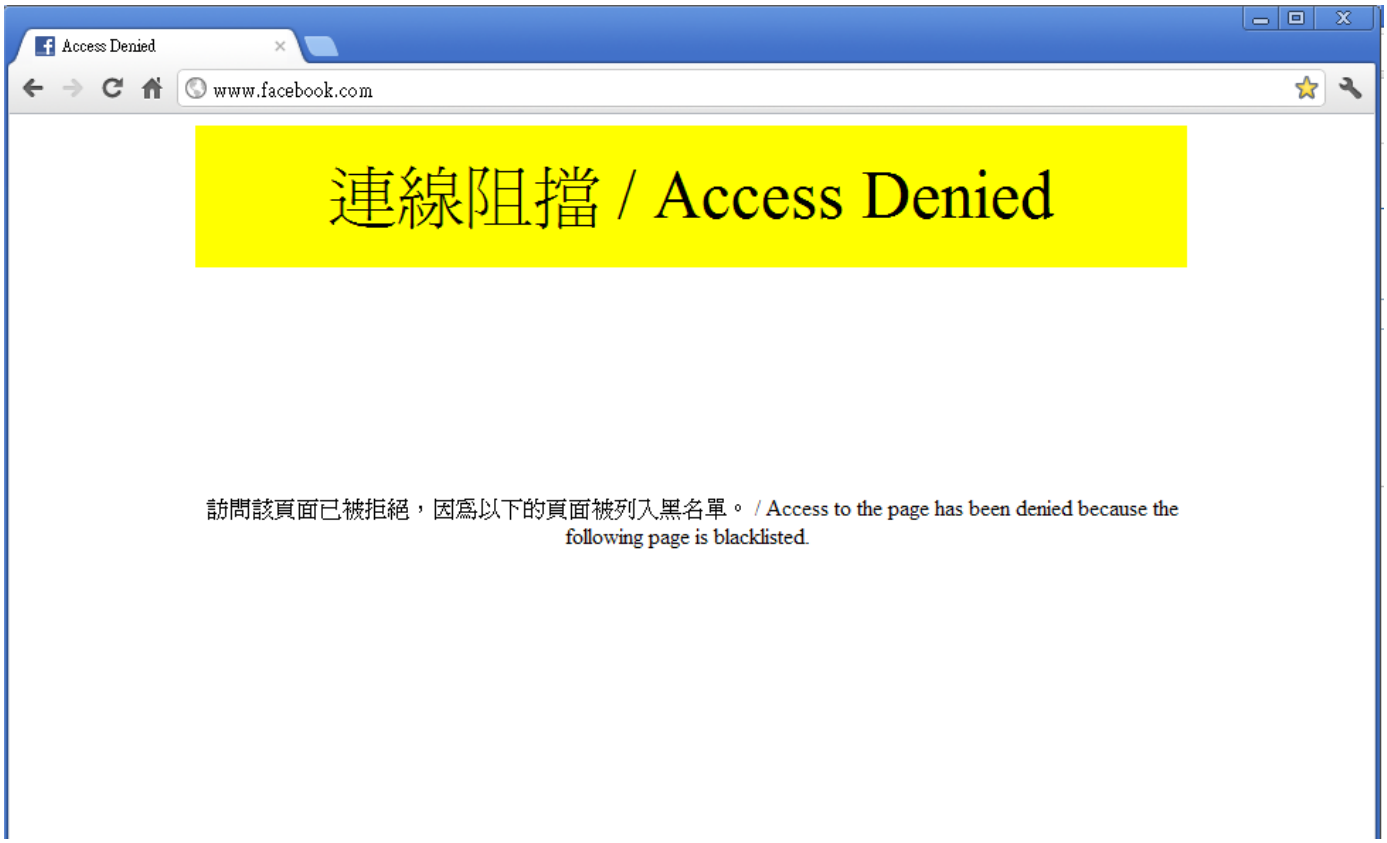

圖 4-72 網站阻擋警訊

4-7、虛擬伺服器

系統管理員在向ISP申請網路連線時，ISP所配發的真實IP位址往往不夠分配給所有使用者。為了有足夠的IP位址分配給每一使用者，大都是使用私有IP位址（Private IP Address），透過 HSecurity+的NAT（Network Address Translation）功能，轉換成真實IP位址(Real IP Address)。

如果對外提供服務的伺服器是置於內部網路時，它的私有IP位址將無法讓外部的使用者直接連線使用，對於此類問題，可使用 HSecurity+的虛擬伺服器功能得以解決。

所謂虛擬伺服器是將HSecurity+外部介面一個真實IP位址，藉由HSecurity+ IP轉換的功能，對映至提供服務的伺服器之私有IP位址。

虛擬伺服器還擁有一項特色，一對多的對映功能，即一個真實 IP 位址可對映到多部提供相同服務的內部網路伺服器的私有 IP 位址。

於本章節，將針對【虛擬伺服器】、【IP 對映】作詳細的介紹與使用說明：

【IP 對映】：因為內部網路是透過 NAT（Network Address Translation）機制轉換的私有 IP 位址，是一對一對映，即一個外部介面真實 IP 位址的所有服務，對映到一個內部網路私有 IP 位址。

【虛擬伺服器】：與 IP 對映作用類似，但虛擬伺服器是一對多對映，即一個真實 IP 位址，對映到多個內部網路私有 IP 位址，只是 埠號不能相同。

【虛擬伺服器】名詞解釋：

外部網路位址：

外部網路 IP 位址(真實 IP 位址)，提供輔助選取功能。

對映到虛擬網路位址：

將外部網路真實 IP 對映至內部伺服器之私有 IP 位址。

外部通訊埠號：

虛擬伺服器所提供的對外服務埠號。若所選擇的服務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；則外部使用者若欲瀏覽網站，就必須更改埠號，方可進入網站）

虛擬伺服器 IP 位址：

虛擬伺服器所對映的外部網路 IP 位址。

啟用伺服器負載：

可將尋求服務的連線，依照連線數分配給內部網路的伺服器群組，可減少單一伺服器的負載，提高伺服器的工作效率。

內部通訊埠（埠號）：

虛擬伺服器所提供的對內服務埠號，同對外埠號。

我們在此範例設定中，總共架設了 2 種虛擬伺服器應用環境。

適用範圍	範例環境
虛擬伺服器	將內部提供單一服務之多台伺服器，以虛擬伺服器的方式透過管制條例來對外服務。(以 Web 服務為例)
IP 對映	將內部提供 FTP、Web、Mail 等多項服務之單一伺服器，透過管制條例來對外服務。

4-7-1、虛擬伺服器

虛擬伺服器是將一個外部 IP 位址，對應到內部 IP 的管理動作，以 TCP/UDP 各有 0 ~ 65535 個埠號，如果將一個通訊協定的埠號，對應到內部一個 IP 位址的相同埠號，總共可以建立 65536 * 2 = 131,072 個虛擬伺服器。

虛擬伺服器建立 IP 位址及埠號對映完畢後，還必須到管制條例的【外對內】或是【外對 DMZ】中將對應的埠號設為『允許』，這樣才完成一個虛擬伺服器。

範例：

外部使用者使用 VNC，對內部網路 VNC 伺服器連線（VNC 使用的埠號：tcp 5900），網路示意圖如下：（圖 4-73）

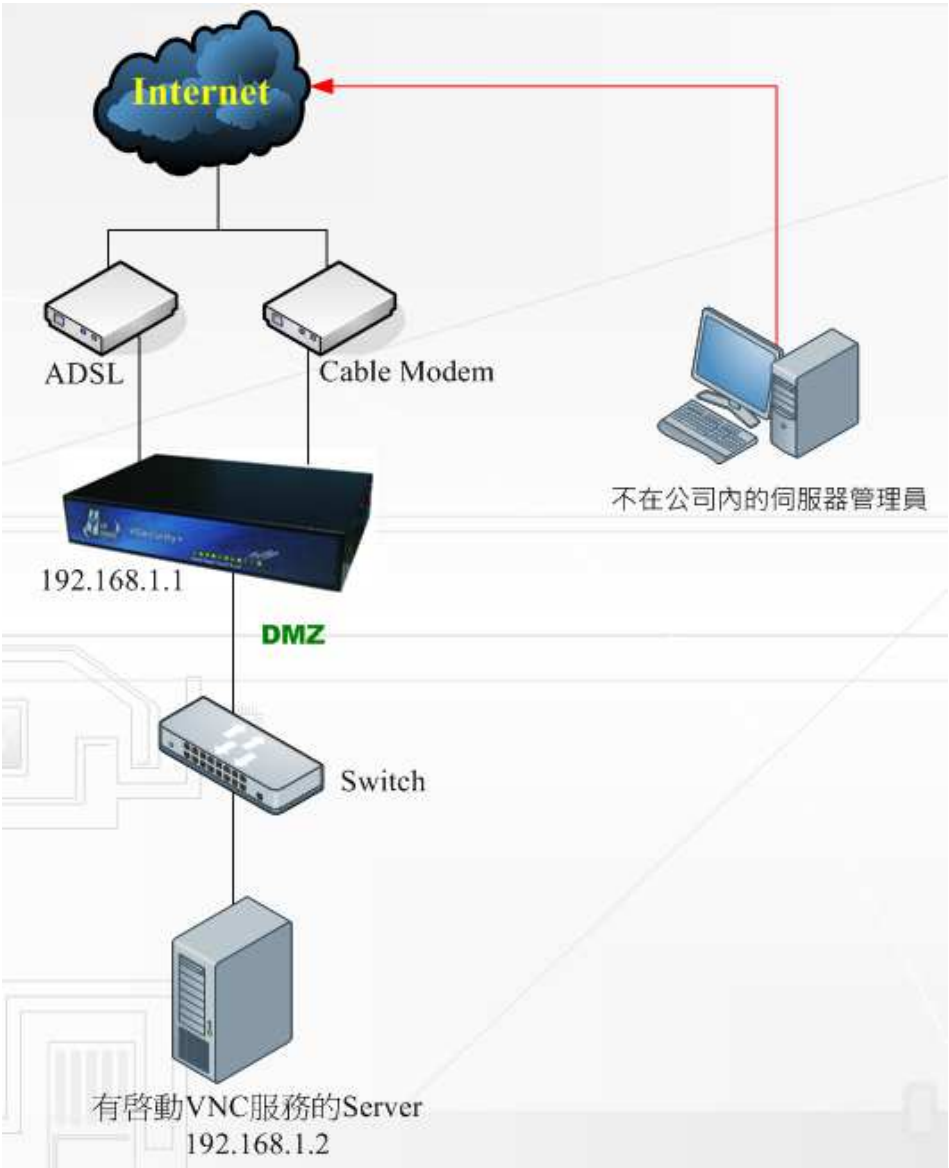

圖 4-73 虛擬伺服器的網路示意圖

步驟1. 內部網路中提供 VNC 伺服器，其 IP 位址分別為 192.168.1.2。

步驟2. 輔助選取：可以選取目前外部網路可以使用的 IP 位址。

步驟3. 在【虛擬伺服器】的【新增虛擬伺服器】功能中，輸入【外部網路 IP 位址】，可藉由輔助選取(範例以內部網路模擬 HSecurity+的 WAN1)，按下【新增】鈕。（圖 4-74）

圖 4-74 VNC 虛擬伺服器對外 IP 設定畫面

步驟4. 在虛擬伺服器列表中，選定要增加的虛擬伺服器 IP 位址，在『編輯/刪除』中選擇 ，他會在這個外部 IP 位址下新增虛擬伺服器。（圖 4-75）

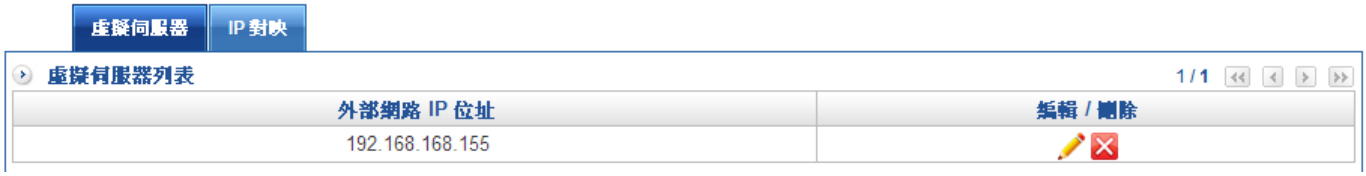

圖 4-75 完成 VNC 虛擬伺服器對外 IP 設定

◆ 在鍵入虛擬伺服器相關設定，外部通訊埠為 TCP 5900。（圖 4-76）

圖 4-76 新增 VNC 虛擬伺服器相對應埠號設定

- 按下【新增】鈕。
- VNC 的虛擬伺服器對外設定完成。（圖 4-77）

圖 4-77 完成 VNC 虛擬伺服器相對應埠號設定畫面

再到管制條例的內對外新增一個管制條例這樣就可以讓外面的 VNC 可以跟內部的 VNC 伺服器互通。

4-7-2、IP 對映

一樣是透過 NAT（Network Address Translation）機制轉換的私有 IP 位址，但是 IP 對映是一對一對映，即一個外部介面真實 IP 位址的所有服務，對映到一個內部網路私有 IP 位址。

雖然是所有的服務對映，但是要讓哪些服務通過跟不通過，依然是由管制條例控制。

一樣是使用前面 VNC 的示意圖，只不過將它改成用 IP 對映的方式達成。

步驟1. 內部網路中提供 VNC 伺服器，其 IP 位址分別為 192.168.1.2。

步驟2. 在【虛擬伺服器】的【IP 對映】功能中，輸入【外部網路 IP 位址】及【對映到虛擬網路位址】，按下【新增】鈕即可建立完畢，【外部網路 IP 位址】可以用輔助選取的方式取得。（圖 4-78）

圖 4-78VNC 虛擬伺服器對外 IP 設定畫面

- 目前為止，只是跟 HSecurity+ 說，哪一個外部 IP 位址對映到內部那一個 IP 位址，至於開放哪些服務，則需要到管制條例中放行。
- 如果 DMZ 也是設成 NAT 模式，設備會根據【對映到虛擬網路位址】上所設定的 IP 判斷是屬於那個介面，在那個介面管制區的基本設定就會出現『Mapped IP 』字樣。（圖 4-79）

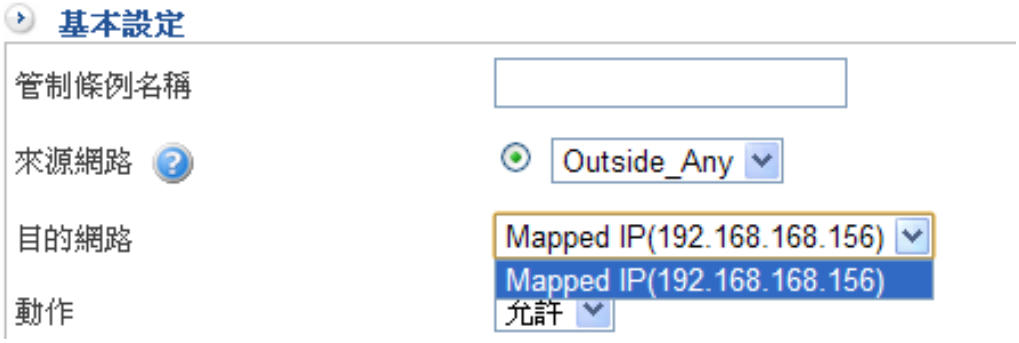

圖 4-79 IP 對映的管制

M

最後再選擇要開放哪些服務進來。(圖 4-80)

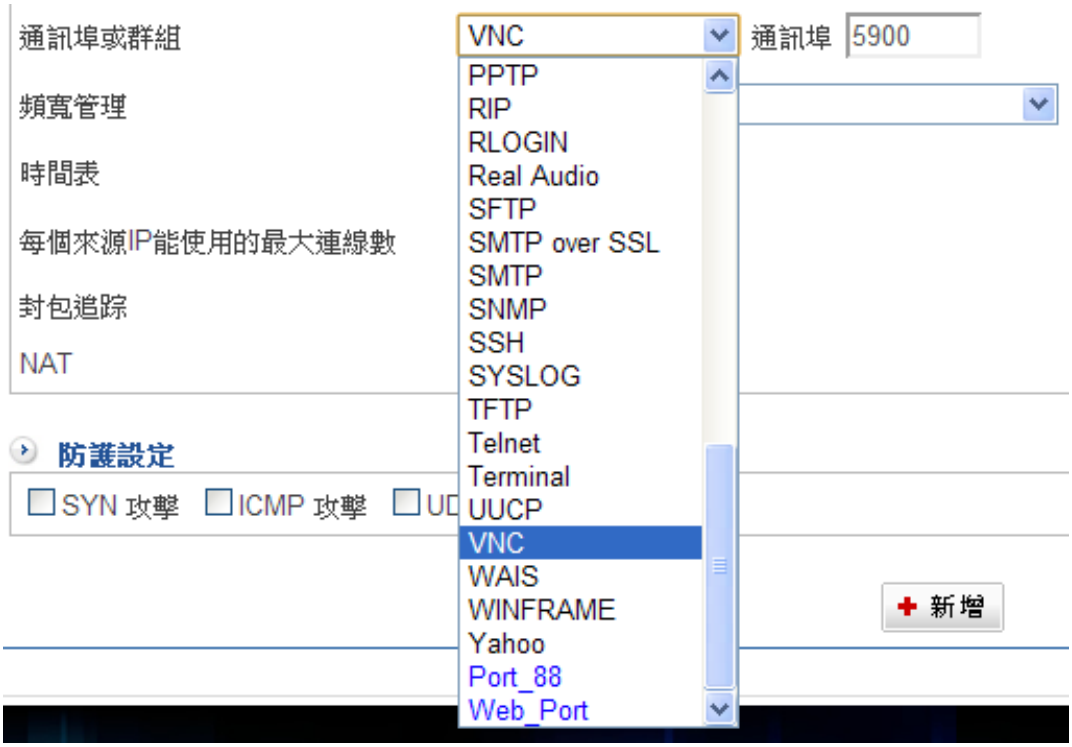

圖 4-80 IP 對映的埠 開放

4-8、防火牆功能

內建 SPI 技術，主動攔截、阻擋駭客攻擊，不論是 DOS、DDOS、UDP Flood 等攻擊方式都可以阻擋，甚至可以抵擋疾風病毒的攻擊，確保內部用戶的安全。

如果攻擊者不是從外部到內部，而是由內部互相攻擊呢？在 ICSA 中就沒有定義這樣的攻擊模式，可是在現實的環境中，這樣的任意攻擊卻是真實的存在。

Hsecurity+套用合理流量及連線數的觀念，認為同一部電腦，不會同時產生太多的連線數，萬一超過合理的流量及連線數時，結合管制條例的運用，防火牆會要求將多餘的連線阻擋。

常見的駭客攻擊方式

SYN 攻擊：

SYN Flood 是當前最流行的 DoS（拒絕服務攻擊）與 DDoS（分散式拒絕服務攻擊）的方式之一，這是一種利用 TCP 協議缺陷，發送大量偽造的 TCP 連接請求，使得被攻擊方資源耗盡（CPU 滿載或記憶體不足）的攻擊方式。

ICMP 攻擊：

ICMP（Internet Control Message Protocol）是 TCP/IP 通訊協定中定義封包的一種，主要功能是用來在網路上傳遞一些簡單的控制訊號。ICMP DoS 攻擊主要有以下兩種手法：Ping of Death 與 Smurf 攻擊。

UDP 攻擊：

利用 UDP 協議，發送大量偽造的 UDP 連接請求，使得被攻擊方資源耗盡（CPU 滿載、頻寬被占滿或記憶體不足）的攻擊方式。

4-8-1、防火牆功能

設定 SYN 攻擊、ICMP 攻擊與 UDP 攻擊設定值：（圖 4-81）

步驟1. 設定 SYN 攻擊設定值

允許最大流量：每一個防火牆保護的外部 IP 位址能夠承受的每秒最大封包要求，預設值是 10,000 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

允許每個來源位址最大流量：網路上同一個 IP 位址同一時間能傳送的數量，預設值是 100 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

阻擋時間：一旦防火牆判斷被攻擊，自動丟棄來自攻擊者 IP 位址封包的時間，預設是 60 秒。

步驟2. 設定 ICMP 攻擊設定值

允許最大流量：預設值是 10,000 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

允許每個來源位址最大流量：預設值是 100 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

阻擋時間：一旦防火牆判斷被攻擊，自動丟棄來自攻擊者 IP 位址封包的時間，預設是 60 秒。

步驟3. 設定 UDP 攻擊設定值

允許最大流量：預設值是 10,000 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

允許每個來源位址最大流量：預設值是 100 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

阻擋時間：一旦防火牆判斷被攻擊，自動丟棄來自攻擊者 IP 位址封包的時間，預設是 60 秒。

圖 4-81 防火牆的防護設定

這些防護規則，可以套用在 HSecurity+的外部 IP 位址，或是使用 IP 對應的虛擬伺服器上，只要來自網際網路的攻擊超過設定值，HSecurity+就會自動將攻擊者 IP 位址的封包阻擋，確保對外伺服器的安全。

4-8-2、防護記錄

HSecurity+記錄所有攻擊行為，管理者可針對攻擊類型、攻擊來源 IP 位址、被攻擊 IP 位址進行搜尋，系統會詳細列出遭受攻擊時間、攻擊類型、協定、通訊埠、攻擊來源 IP 位址與被攻擊 IP 位址。（圖 4-82）

圖 4-82 防護記錄

4-9、上網認證

HSecurity+ 多功能防火牆可經由認證表的設定，來控管使用者的連線權限。使用者必須通過 HSecurity+的認證機制，方可連線。

HSecurity+提供四種認證模式。一是內建的認證【本機使用者】；另一是利用自行架設的【RADIUS】、【POP3】和【AD】認證伺服器。系統管理員可利用這四種模式，來管理 HSecurity+多功能防火牆的認證機制。

當管理者希望內部的使用上網際網路前，先經過認證程式，認證過後，才可以使用網路，此時就需要這個功能。

當管制條例要求使用者認證後才能上網際網路，使用者打開網頁後，會出現要求輸入帳號密碼的視窗，輸入管理者給予的帳號密碼，正確無誤後，系統就會自動開啟預設首頁或是管理者自訂的網址。

使用者的帳號密碼來源可以從自訂的帳號密碼、從 AD 伺服器選取的帳號密碼或是從郵件伺服器來的帳號密碼。

管理者可以任意從上述的 3 種來源挑選組合，組合的名稱就是一個認證群組，此時就可以在管制條例中挑選特定的認證群組套用。

當管制條例將特定的內部 IP 位址套用認證群組時，代表這些 IP 位址打開瀏覽器要上網際網路時，HSecurity+ 會要求這些用戶輸入合格的帳號及密碼。

【上網認證】名詞解釋：

認證模式：

HSecurity+ 目前支援 3 種認證模式，自訂的帳號密碼、 AD 伺服器選取的帳號密碼及郵件伺服器來的帳號密碼，管理者可以任意組合上網認證是要啟用，其中一種或是全部。

認證埠號：

當 HSecurity+啟用認證之機制時，內部使用者需通過認證方可連線至外部網路。而認證埠號則為該認證機制所用之埠號，其預設為 82。

同時最大連線數：

管制目前經由上網認證最多 PC 連線數量。

當閒置多久要求重登：

用戶認證過後，瀏覽器多久沒使用，系統會自動將這個認證成功狀態結束，超過這個時間後，如果使用者要再用網路，則需要重新登入。

使用者登入多久之後要求重登：

使用者登入成功後，超過這個時間設定，系統會要求用戶重新登入，預設是 24 小時，當設為 0 時，代表關閉這項功能。

允許修改密碼：

使用者登入成功後，可以修改自己的密碼，下次登入時，就可以使用新的密碼。

拒絕重複登入：

啟用這項功能後，每個帳號及密碼只允許一個 IP 位址登入，當另一個 IP 位址要求使用相同的帳號密碼時，會被 HSecurity+ 的認證機制拒絕。

登入失敗次數超過多少暫時封鎖：

為了避免有心人士嘗試利用別人帳號密碼來進行非法事情，管理者可以自行設定當帳號登入失敗次數超過設定值時，暫時先將該組帳號密碼封鎖。

多久解除被暫時封鎖的 IP：

當使用者帳號被封鎖時，需隔多少時間才能解除封鎖。當設為 0 時，代表永不解除。

登入失敗次數超過多少永久封鎖：

對於多次以錯誤密碼嘗試之使用者，管理者除了暫時封鎖外，還可以選擇永久封鎖。

解除 IP 封鎖

解除被封鎖的使用者。

登入成功的使用者要被轉向的 URL：

管理者可以讓每一個登入成功的使用者開啟一個特定的網頁，例如公司的網頁或是訊息通知的網頁，如果這裡是空白的，當使用者認證成功後，自動開啟使用者瀏覽器所設定的首頁。

使用者帳號 ：

所設定認證表之使用者帳號。

密碼 ：

建立認證時所需要的密碼。

確認密碼 ：

鍵入與密碼欄一致的字串。

當下次登入時要求使用者更改密碼：

於啟用此後能後，內建認證用戶進行首次認證時，會強制其變更認證密碼。

帳號有效期限

設定【認證用戶】帳號的使用期限

AD 登入帳號/密碼：

具有管理權限的管理者帳號，HSecurity+ 會利用這個帳號及密碼，跟設定的 AD 伺服器詢問，正在上網認證的使用者帳號及密碼正確與否。

忽略的 AD 群組及使用者：

當具有管理權限的管理者跟設定的 AD 伺服器詢問時，AD 伺服器會回應所有的群組及帳號，其中包含無用的公用帳號及群組，例如，guest 帳號，如果不希望這些帳號及群組被列入認證帳號的『被選擇目標』，可以在這裡設定忽略的群組及帳號。

4-9-1、認證設定

管理者在這裡設定一些上網認證會使用的共同設定，如登入的 timeout 、認證模式、登入畫面的設定等。

共同設定 (圖 4-83)

步驟1. 『認證通訊埠』：輸入認證通訊埠，預設值為 82。 (範圍 : 1 ~ 65535，0 代表認證功能不啟動)

步驟2. 『同時最大連線數』：輸入同時最大連線數 10，範圍可從 10~256。

步驟3. 『當閒置多久要求重登』：預設是 60 分鐘。(範圍為 1~1000 分鐘)

步驟4. 『使用者登入之後多久要求重登』：預設是 24 小時，當設為 0，代表關閉此項功能，也就是使用者一旦認證過後，除非重新開機，否則永久有效。

步驟5. 『允許修改密碼』：要不要允許使用者修改密碼，預設是不允許。

步驟6. 『拒絕重複登入』：預設是不管，也就是同樣帳號可以在不同 IP 位址登入。

步驟7. 『登入失敗次數超過多少暫時封鎖』：主要是避免有外來者在測試內部使用者帳號密碼，占是封鎖該帳號登入。

步驟8. 『多久解除暫時封鎖的 IP』：當 IP 被封鎖後須隔多久時間才能解除， 0 代表不限制，亦即永久不解除。

步驟9. 『登入失敗次數超過多久永久封鎖』：登入失敗次數超過多久永久封鎖，避免駭客攻擊將該帳號永久封鎖。

步驟10. 『解除 IP 封鎖』：由於並沒有需解除 IP，不做解除設定。

步驟11. 設定登入成功的使用者要被轉向的 URL，導向 www.herhsiang.com，如果空白，系統會用使用者瀏覽器預設的首頁為認證成功後開啟的頁面。

步驟12. 選擇認證模式，HSecurity+ 支援 4 種認證模式，本機帳號、AD 帳號、POP3 帳號與 Radius，管理者可以選用其中一種、兩種或全部。

圖 4-83 認證的共用設定

Client 端登入畫面設定 (圖 4-84)

設定使用者登入時的畫面及說明文字，管理者也可以上傳一個圖形，增加認證時的美觀，預設的圖形是 Herhsiang 的 logo。

步驟1. 輸入主旨歡迎光臨某公司網路認證系統，可以任何文字。

步驟2. 輸入內容，管理者可以輸入任何一段文字描述這個認證說明。

例如：請輸入公司配發的認證帳號及密碼。

步驟3. 上傳一個圖形。

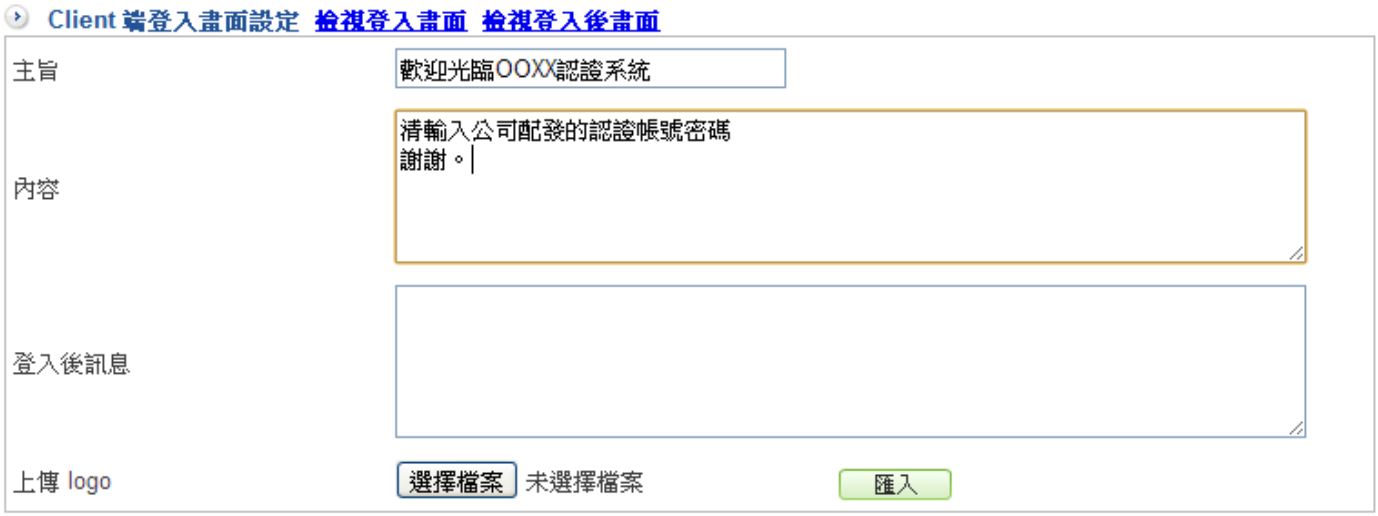

圖 4-84 認證登入畫面設定

步驟4. 管理者可以按下『檢視』字樣，查看一下用戶端認證時的畫面是否符合設定的目標。 (圖 4-85)

圖 4-85 認證登入畫面

帳號建立方式：本機、POP3、 Radius、AD

4-9-2、本機使用者

建立本機使用者帳號 (圖 4-86)

步驟1. 輸入名稱【Ping Liu】，任何容易描述這個使用者的文字。

步驟2. 輸入使用者帳號【ping】，最多 16 個文字。

步驟3. 輸入密碼【ping!@# 】，要想使你的密碼更安全，可以採取以下方法：

- 使用字母和數字
- 使用特殊字元(如@，但逗號與冒號不允許使用)
- 混合使用大小寫

步驟4. 再次確認輸入密碼，避免密碼輸入錯誤造成無法登入。

步驟5. 【當下次登入時要求使用者更改密碼】：要不要讓使用者登入如修改密碼，預設是不允許。

步驟6. 這個帳號的使用期限，系統會自動帶出日期讓管理者挑選，如果空白,代表這個帳號永遠不會過期。

步驟7. 建立成功後，HSecurity+ 會列出所有的本機帳號。

圖 4-86 本機使用者設定

4-9-3、POP3、RADIUS 使用者帳號設定

POP3 使用者設定

建立外部帳號---至 POP3,RADIUS 使用者新增 POP3 伺服器 (圖 4-87)

步驟1. 輸入 POP3 伺服器的網功能變數名稱稱。

步驟2. 輸入可以使用的網功能變數名稱稱，因為一個 POP3 伺服器可能擁有數個網域，輸入使用者額外要認證要用的網域。

圖 4-87 POP3 認證伺服器設定

步驟3. 設定完成 POP3 網域後，在新增一個群組時，需要匯入 POP3 的帳號，帳號的格式是每一個帳號一行，目前提供兩種 POP3 匯入方式，一種為單筆新增、一種會整批匯入。(圖 4-88)

- ◆ 單筆新增：輸入帳號，一行一組設定；格式如：

  ping

  mira

  但是系統保留 POP3、RADIUS、Organization、Group、Account、Office/AD User、Department / AD User、Company / AD User

- ◆ 整批匯入：匯入檔案格式有.txt 或.csv

  建立方式一筆一行

圖 4-88POP3 帳號設定

RADIUS 使用者設定

在 Radius 設定功能中輸入 IP(RADIUS 伺服器)、Port(RADIUS 伺服器通訊埠)和共用密碼(需與 RADIUS 伺服器相同)(圖 4-89)

步驟1. 輸入 RADIUS 名稱，例如：my_radius

步驟2. 輸入 RADIUS 伺服器 IP 位址，例如：172.192.10.10。

步驟3. 輸入 RADIUS 伺服器通訊埠，預設值為 1812。

步驟4. 輸入密鑰，此為 HSecurity+與 Radius 伺服器進行認證時所需的密碼。

圖 4-89 Radius 網域認證設定

步驟5. 設定完成 RADIUS 伺服器後，在新增一個群組時，需要匯入 RADIUS 的帳號，帳號的格式是每一個帳號一行，目前提供兩種 RADIUS 匯入方式，一種為單筆新增、一種會整批匯入。(圖 4-90)

- ◆ 單筆新增：輸入帳號，一行一組設定；格式如：

  Jean

  Randoll

  但是系統保留 POP3、RADIUS、Organization、Group、Account、Office/AD User、Department / AD User、Company / AD User

- ◆ 整批匯入：匯入檔案格式有.txt 或.csv

  建立方式一筆一行

圖 4-90Radius 帳號設定

4-9-4、AD 帳號設定

建立外部帳號---AD 網域伺服器 (圖 4-91)

步驟1. 輸入 AD 網域伺服器的 IP 位址，例如：192.168.1.150。

步驟2. 輸入 AD 網域伺服器的網功能變數名稱稱，例如：herhsiang.com。

步驟3. 輸入 AD 網域伺服器具有管理權限的管理者帳號及密碼，例如：帳號 administrator / 密碼 qwertyui。

步驟4. 設定不要被使用的 AD 群組及使用者，例如，guest，如果沒有填入，在挑選認證帳號時，所有的群組及使用者都會成為被挑選目標。

步驟5. 當設定完成時，管理者可先行連線測試，看是否可正常運作。

圖 4-91 AD 網域認證設定

4-9-5、使用者群組

步驟1. 輸入認證群組的稱，可以是任何文字。(圖 4-92)

步驟2. 認證設定，可以使用之前已經設定完成的共同設定值，或是針對這個認證群組，自行定義一次諸如『當閒置多久要求重登』、『使用者登入之後多久要求重登』、甚至連『認證模式』2 都可以修改。

步驟3. 選擇要挑選的類型，如果選本機，則左邊會出現所有本機帳號供管理者挑選，如果有設定外部帳號伺服器認證，在此選擇 AD 、POP3 或 RADIUS ，左邊的被挑選目標就會出現帳號，供管理者挑選。

圖 4-92 建立認證群組

步驟4. 建立完成認證群組後，再到內到外或是 DMZ 到外設定認證機制。（圖 4-93）

步驟5. 挑選要認證的 IP 位址或群組。

步驟6. 挑選認證群組，HSecurity+ 會自動列出所有已經設定完成的認證群組，讓管理者可以挑選。

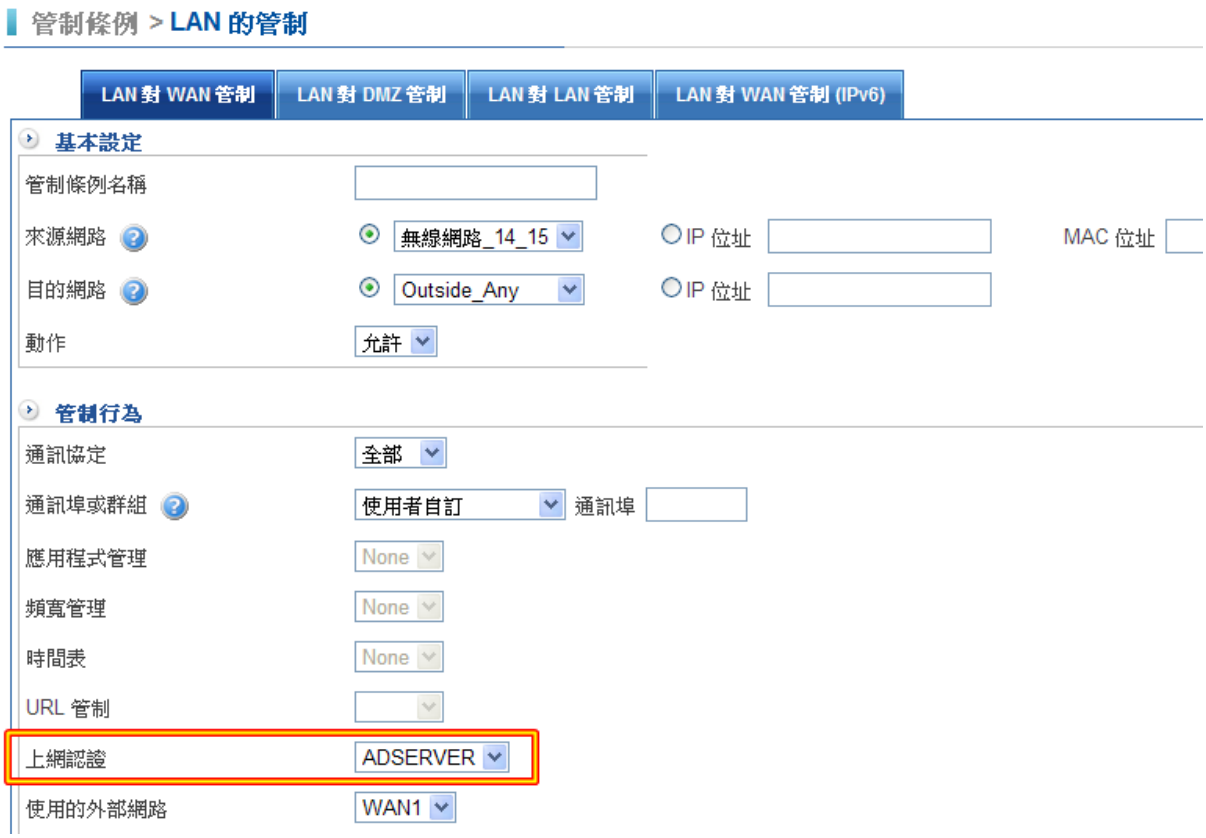

圖 4-93 套用在管制條例上

4-9-6、認證紀錄

如果使用曾經使用認證群組，HSecurity+ 會自動將登入跟登出的時間、使用者帳號、登入 IP 位址、狀態、認證方法條列出來。管理者也可以藉由搜尋條件快速搜尋 (圖 4-94)

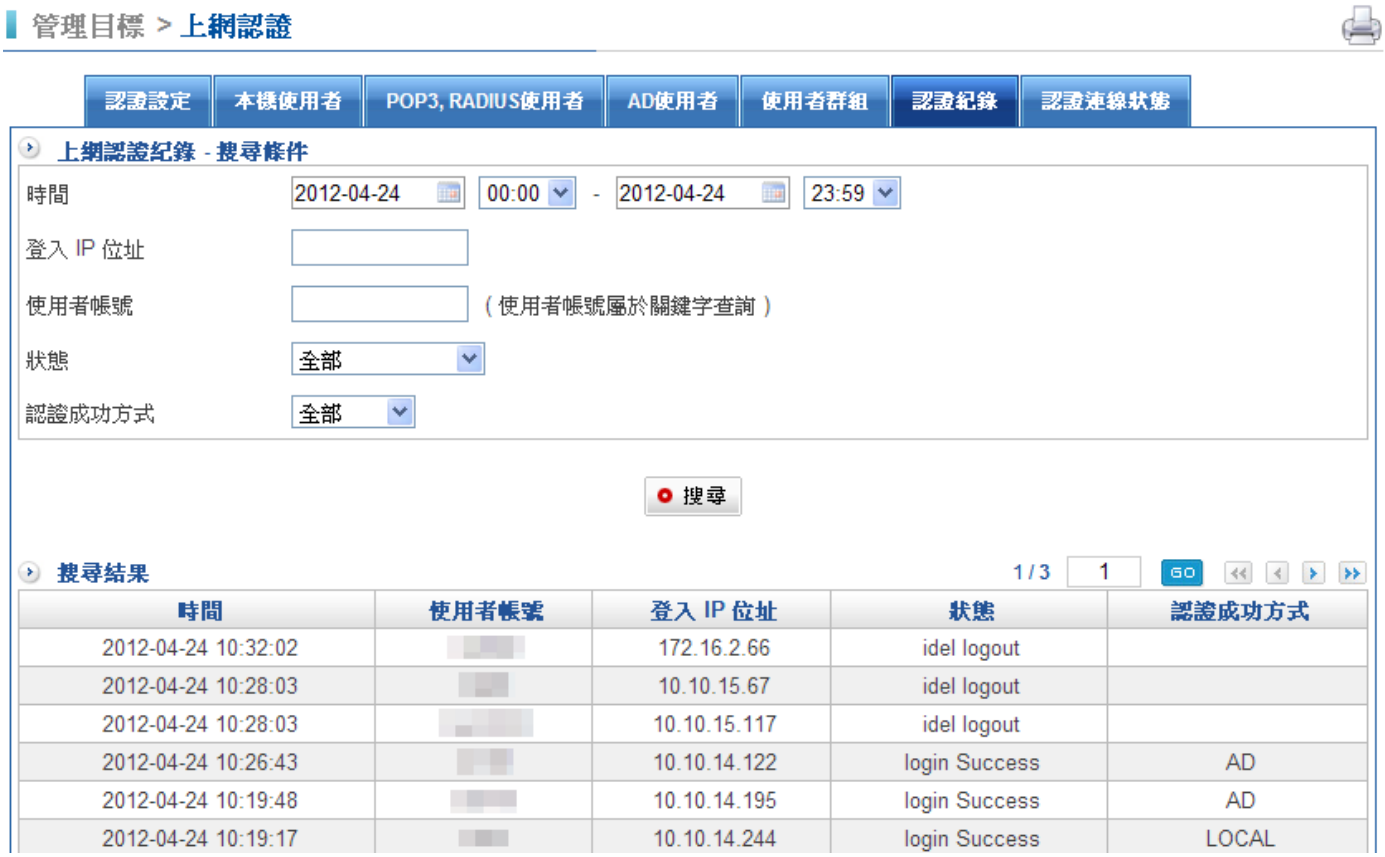

圖 4-94 認證登入紀錄

4-9-7、上網認證連線狀態

列出所有上網認證連線狀態，防火牆會自動將群組名稱、使用者帳號、使用者 IP、剔除與群組剔除紀錄條列出來。（圖 4-95）

圖 4-95 認證登入紀錄

註：當將使用者剔除時，則使用者無法連線到外部網路，必須在重新登入才可進行連線。

第五章 網 路 服 務

使用者可隨時由系統狀態中，得知目前網路服務狀態，如 DHCP 服務、DDNS 服務、DNS 伺服器、WEB 服務、FTP 服務、病毒引擎、高可用性與異常 IP 分析等各項資訊。

（一）【DHCP 服務】：

當啟動 DHCP 功能時，內部 PC 可透過 HSecurity+的 LAN 或 DMZ 介面，取得 IP 位址、DNS 伺服器等資訊。

（二）【DDNS 服務】：

DDNS 意思是動態 DNS，是指不固定 IP 的主機，隨 IP 的改變去設定網功能變數名稱與 IP 的對應關係。如果不固定 IP 的主機(如使用 PPPOE 的 ADSL，DHCP 的 Cable，撥接用戶)，欲架設 Web、Mail 或者 FTP 等 Server，或者使用者需要網路身份(網功能變數名稱稱)者即需動態 DNS。

（三）【DNS 伺服器】：

DNS 的全稱是 Domain Name Service，是一套系統軟體，讓大家所使用及管理的電腦網路系統，能夠作領功能變數名稱稱與 IP 位址之間的轉換。

（四）【高可用性】：

HSecurity+的硬體備援機制，採 Master/Backup 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。

（五）【SNMP】：

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。

5-1、DHCP 伺服器

【DHCP】名詞解釋：

一台電腦要連上網路必須要先設定 IP、子網路遮罩、路由、DNS 等。一般使用者對這些網路設定並不熟，所以要讓使用者自己去建立非常麻煩。如果企業裡有上百台的電腦，需要由網管人員去分配每一台的 IP、設定電腦實在是一件痛苦的事情。因此如果有 DHCP 伺服器，網路上的電腦只要設定好自動取得 IP，系統開機後就可以自動取得網路設定。網管人員就不需要一台一台去設定。

在設定 DHCP 伺服器時，我們會設定要讓使用者自動取得的 IP 位址範圍、路由、DNS，在啟動 DHCP 伺服器之後，這些資訊就會放到記憶體中等客戶端來問。當一台使用 DHCP 自動取得 IP 的電腦連上網路後，它會以廣播的方式詢問網路上有沒有 DHCP 伺服器，而 DHCP 伺服器會回應，並送給客戶端網路設定的資料。客戶端收到這些資訊後，就將它設定為自己的 IP、DNS 等。

如果以 DHCP 常用的話語來說，DHCP 分配出一個 IP 的情形叫做 DHCP「出租」IP 給客戶端。DHCP 的租約是有期限的，時間到了之後，客戶端就必須重新取得一次 IP，不過客戶端可以要求繼續使用同一個 IP。為了避免有機器一直要求使用同一個 IP，我們也可以設定同一個 IP 最長的租期是多久。

除了動態的分配 IP 外，DHCP 也可以同時設定指派固定 IP。每一張網路卡都會有一個固定的網路卡位址 (MAC、Physical Address)，例如，我們可以在 FreeBSD 中使用指令 ifconfig 或是在 Windows 中使用 ipconfig/all 來看到 MAC 的資訊。以下列為例：

```
# ifconfig
fxp0: flags=88c3<UP,BROADCAST,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
options=b<RXCSUM,TXCSUM,VLAN_MTU>
inet6 fe80::202:b3ff:fe48:7c74%fxp0 prefixlen 64 scopeid 0x1
inet 10.0.0.1 netmask 0xff000000 broadcast 10.255.255.255
ether 00:08:c3:96:8c:22
media: Ethernet autoselect (100baseTX <full-duplex>)
status: active
```

上列藍字部份「00:08:c3:96:8c:22」就是網路卡位址，我們可以設定某個網路卡位址一定使用固定 IP，如此一來，只要這一台機器使用 DHCP 要求 IP 時，DHCP 伺服器都會給它固定的位址。

【DHCP 服務】名詞解釋：

起始位址

內部網路所屬網域廣播開始位址。

結束位址

內部網路所屬網域廣播結束位址。

主要的 DNS

設定主要 DNS IP 位址。

次要的 DNS

設定次要 DNS IP 位址。

預設租約時間(分)

預設機器使用同一個 IP 時間。

最大租約時間(分)

為了避免有機器一直要求使用同一個 IP，我們也可以設定同一個 IP 最長的租期是多久。

預設閘道器

內部網路預設閘道。

於【DHCP 服務】之【DHCP 列表】功能中，記錄 HSecurity+內建的 DHCP 伺服器所配發的 IP 使用情況：（圖 5-1）

- 【IP 位址】：DHCP Server 所配發給該電腦之動態 IP 位址。
- 【MAC 位址】：該動態 IP 位址所對映之 MAC 位址。
- 【起始時間~結束時間】：該動態 IP 位址之有效時間(起始時間 / 結束時間)（年/月/日/時/分/秒）。
- 【主機名稱】：接受 DHCP 伺服器配發 IP 之電腦的網路識別名稱。

圖 5-1 DHCP 用戶表 Web UI 畫面

設置 DHCP 伺服器

步驟1. 於【DHCP 服務】之【DHCP 列表】功能中，做如下設定：

- 內部網路介面位址，於左邊欄位鍵入第一組可使用的起始 IP 位址，於右邊欄位鍵入第一組可使用的結束 IP 位址，預設為 192.168.1.50 到 192.168.1.60。（須為同一網域）
- 主要的 DNS：鍵入欲配發 DNS 伺服器 1 之 IP 位址。
- 次要的 DNS：鍵入欲配發 DNS 伺服器 2 之 IP 位址。
- 填入預設租約時間，預設值為【3600】，單位為分鐘。
- 填入最大租約時間，預設值為【3600】，單位為分鐘。
- 設定預設閘道器位址為【192.168.1.1】，不一定是 LAN 或 DMZ 的 GateWay 位址。
- 輸入網功能變數名稱稱，管理者可以修改域設的功能變數名稱。
- 勾選【啟動】鈕，完成【儲存】設定。（圖 5-2）

圖 5-2 LAN DHCP 伺服器 設定視窗

註： DMZ (非軍事區)DHCP 伺服器設定方式跟 LAN 的 DHCP 伺服器相同。

除了動態的分配 IP 外，DHCP 也可以同時設定指派固定 IP。

步驟1. 在內部或是 DMZ 區的位址表中，新增一個位址。

步驟2. 設定方式選擇 皆設定 IP 和 MAC 位址。

步驟3. 啟用 Get static IP address from DHCP Server 的功能，這個 IP 或是 MAC 位址上線時，均會取得固定 IP 位址。（圖 5-3）

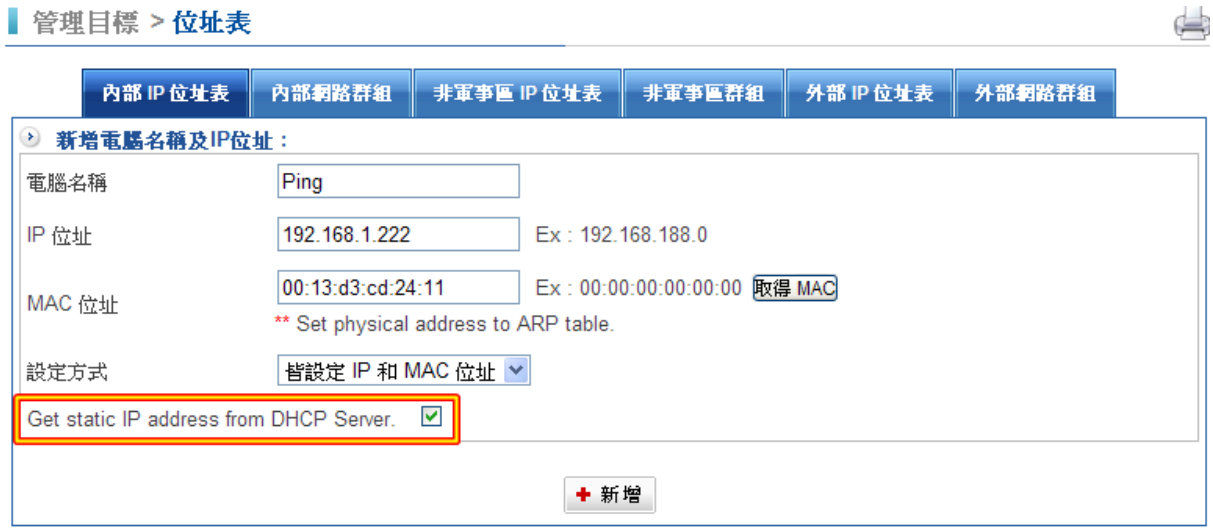

圖 5-3 DHCP 固定 IP 位址 設定視窗

◆ 按下【新增】建立完成，在 DHCP 固定 IP 位址會出現下表。（圖 5-4）

圖 5-4 完成 DHCP 固定 IP 位址設定

5-2、DDNS 服務

DDNS 允許網際網路的使用者使用網址名稱來連線到您的虛擬伺服器，而不是使用 IP 位址，這也解決了動態 IP 位址的問題，動態 IP 位址，當您要從網際網路端連接回來時，IP 位址變更而造成您連接的困難。

HSecurity+ DDNS 服務的運作如下：

1.您必須在“已註冊的 DDNS 服務” 下拉選單中選取一個供應商來註冊服務。

2.註冊完成後，跟著服務供應商的步驟申請一個網功能變數名稱稱。

3.在 HSecurity+的 DDNS 畫面中輸入您的 DDNS 的資料。

4.HSecurity+會自動地將您目前使用的 IP 位址紀錄在 DDNS 伺服器上。

5.從網際網路端，使用者將可以使用您註冊的網功能變數名稱稱來連接到您開啟的虛擬伺服器。

【DDNS】名詞解釋：

服務廠商

點選已註冊 DDNS 服務供應商的名稱。

主機名稱

輸入已申請網功能變數名稱稱。

外部介面

對外所屬網路介面。

帳號

填入您申請的 DDNS 服務的使用者名稱。

密碼

內部網路所屬網域。

註解

DDNS 備註說明。

紀錄

正常的話，訊息應該要顯示 “ Update OK”

建立一個新的 DDNS

步驟1. 於【網路服務】的【DDNS】功能中，新增下列資料。(圖 5-5)

- 點選下方【新增】按鈕。
- 【主機名稱】輸入所申請的網功能變數名稱稱。
- 選擇所要對應的外部網路介面為【WAN1】。
- 於【帳號】和【密碼】欄位中，輸入所申請的帳號密碼。
- 鍵入註解為【HSecurity+測試】，點選【啟動】鈕。

圖 5-5 DDNS WebUI 設定視窗

- 按下【新增】完成設定。

DDNS 狀態

HSecurity+ 會列出每一個 DDNS 目前的狀態。(圖 5-6)

- ：代表更新正常，：代表服務無法順利運作。
- 記錄：按鈕會顯示系統跟 DDNS 伺服器的通聯資料。
- 立即更新：讓 HSecurity+ 立刻執行 DDNS 更新的動作。

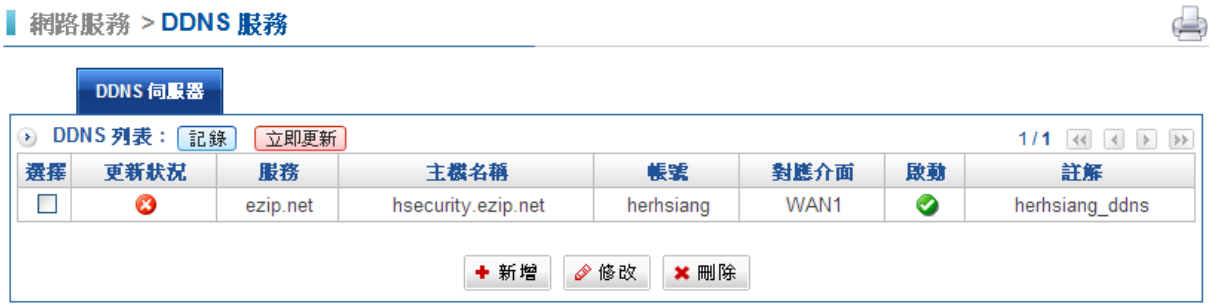

圖 5-6 DDNS 狀態

5-3、DNS 伺服器

網路是由無限多的電腦連線所構成，為了確保資料流動的正確性，每台電腦都有「固定而且單一」的「位址」，即是 0～255 數字所組成的 IP 位址。

隨著連線主機的增加，對於一般使用者來說 IP 的位址不適合記憶與管理，因此會有 Domain 的出現。就像我們每個人一出生都會有一組身分證字號，但是一大串的身分證號碼難記憶，因此就會有名字或別名出現，方便稱呼。

網址是由主機名稱與網功能變數名稱稱兩部分組合而成。例如：網路中文名稱為：www.herhsiang.com.tw，透過 DNS 解析，即可以指到：211.22.160.28 這台主機，因此我們不必要記誦這串難記的數碼，只要輸入網功能變數名稱稱就可以連上該網站。而 www.herhsiang.com.tw 與 211.22.160.28 之間的對應，中間就需要 DNS Server 來轉換了。

我們可以知道，網路上是用 IP 來定址的，如果要使用讓人好記的 Domain Name 來連結，就要先在一台 DNS 伺服器上紀錄該網域內的名稱資料和 IP 的對應記錄，供人查詢出相對應的 IP。

HSecurity+ DNS 伺服器只提供代理查詢的功能，可幫防火牆下面的伺服器向外部查詢 DNS 功能。

一般設定

內建的 DNS 伺服器可以接受使用者的代理查詢，例如，內部的使用者可以將 DNS 伺服器指向 HSecurity+ ，當使用者要查詢 www.abc.com 時，HSecurity+ 會代理這項 DNS 查詢服務，並將結果回應給內部的使用者。

步驟1. 於【DNS 伺服器】>>【一般設定】中，新增下列資料。

- 接受代理查詢服務的 IP 位址：指 HSecurity+要幫內部的 IP 位址或是區段，做代理查詢，如果設定為 192.168.188.110，表示 HSecurity+只允許此 IP 做代理查詢，而它就不用在連到外部去查詢 DNS 了。
- 接受網域抄送的 IP 位址：HSecurity+具有 DNS Server 功能，而要不要讓其他的 DNS Server 抄寫我們的資料做備份，只要輸入其 IP 即表是允許它抄寫。例如：輸入 192.168.188.100 代表把我們上面 DNS 資料抄寫到它的主機上面。（圖 5-7）

圖 5-7 DNS 伺服器一般設定畫面

5-4、高可用性

HSecurity+ 提供高可用性的配置，管理者可以配置 2 台相同的設備互為備援，HSecurity+ 的備援機制為 Active and Standby，也就是一台為主另一台為輔。

HSecurity+提供高可用性（High Availability）功能，供企業內部網路(Intranet)和網際網路(Internet)之間傳送電子資料時，其控管網路使用的 **MASTER** HSecurity+發生故障時，可即時由 **BACKUP** HSecurity+取而代之成為運作中的 MASTER 主機，來保持內/外部網路不斷線的運作，避免錯失商機。網管人員亦可立即獲得新主機的訊息，來對原本故障的主機做修復保養的工作，使其能夠盡快恢復運作，來保障網路永續通暢。

【高可用性】名詞解釋：

模式

總共有 2 種模式可以選擇，master 跟 backup。

管裡 IP

因為 2 台設備的 lan IP 位址不能一樣，所以多了一個管理 ip 位址，不論哪一台正在運作，都可以用這個 ip 位址登入。

在啟用高可用性（High Availability）功能後，用來分別登入 MASTER 與 BACKUP SHSecurity+的 Web UI 做管理動作之 IP（須與 LAN Port Interface 為同網段之 IP，但彼此 IP 不可相同）

可用性的設定步驟：

步驟1. 個別至二台主機設定自己的 LAN IP 位址，2 台主機的 LAN IP 位址必須在同網段內的不同 IP 位址，否則會造成 IP 位址衝突。

步驟2. 設定 Master 主機 (圖 5-8)

點選 master 主機的 網路服務 > 高可用性

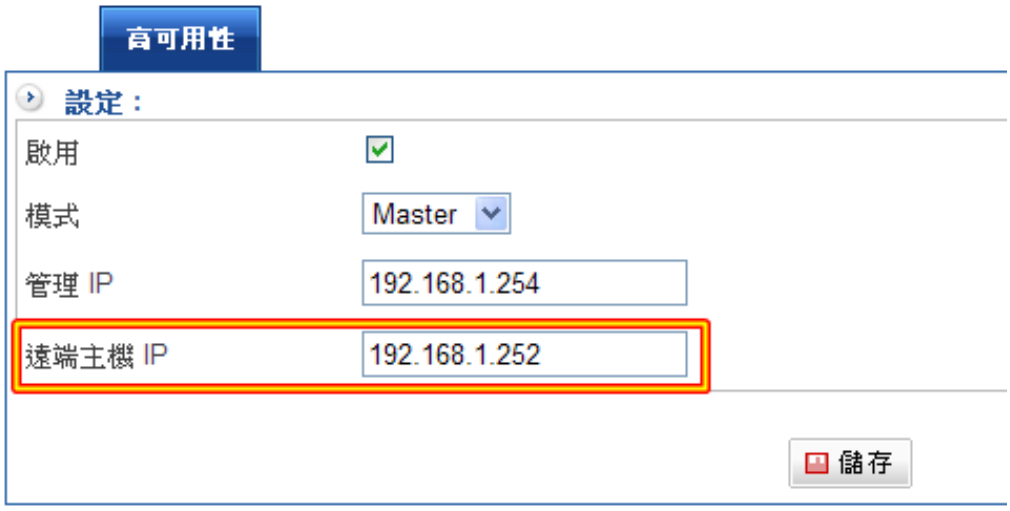

圖 5-8 高可用性設定-Master 部份

以上圖為例，當本機設為 Master，遠端主機位址設為 192.168.1.252，則 192.168.1.252 就是備援主機，按下儲存之後，HSecurity+會向遠端主機 192.168.1.252 檢查型號群組和版本是否相同，檢查成功後才可以做同步動作。

步驟3. 設定 Backup 主機 (圖 5-9)

點選 Backup 主機的 網路服務 > 高可用性

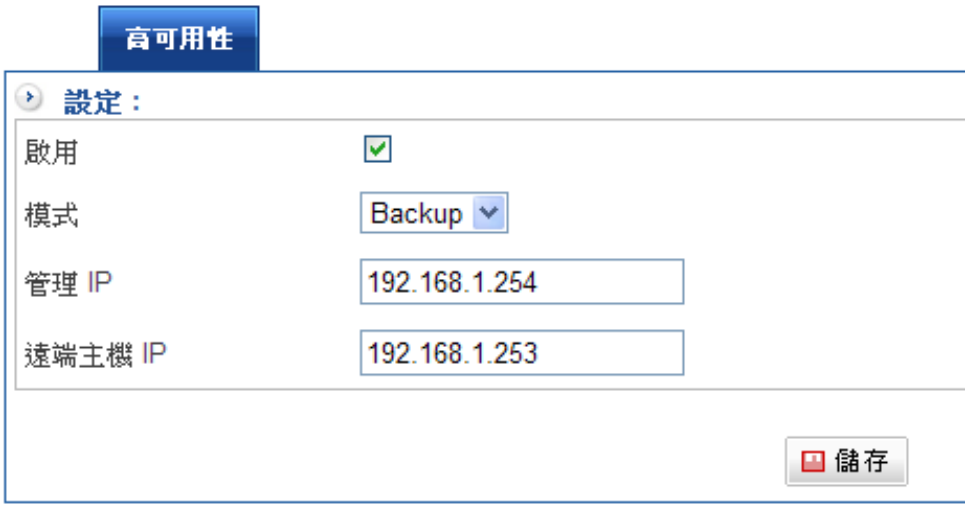

圖 5-9 高可用性設定-Backup 部份

當模式設為 Backup，且遠端主機設為 192.168.1.253，則遠端主機就是 Master 主機，再按下儲存之後， 一樣會做型號群組和版本檢查，檢查成功後才可以做同步動作。

當模式設為 Backup 時， 會顯示最近資料同步時間，HSecurity+ 會每隔間 5 分鐘向 Master 要求同步資料， 或則可以手動按立即同步。

步驟4. 確認現在由那一台機器接手？（圖 5-10）

請用 共同管理 IP 登入， 查看首頁上的 HA 狀態

有服器服務	
DHCP 服務	✓
DDNS 服務	✓
IPSec VPN 服務	✓
HA	✗

圖 5-10 高可用性的運作

如首頁的 HA 是 Master， 表示現在是由當初設為 Master 的 192.168.1.253 那台接手，如果是顯示 Backup， 表示已經切換當初設為 Backup 的 192.168.1.252 那台接手。

注意事項

1、當 HA 切換至 Backup，在 Backup 主機所做的任何修改設定，Master 復原起來後，系統不會向 Backup 同步回差異資料。如果需要將 Backup 的資料同步回 Master，可以將二台角色做互換， Master 改為 Backup， Backup 改為 Master， 這樣資料就會以最初設定的 Backup 為準。

2. 不會被同步的資料， 列舉如下：

系統操作日誌

系統/網路狀態圖

電腦成員列表

5-5、SNMP

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。

對外連線

SNMPv3

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。

安全等級 說明如下：

SNMPv3 規定了三個認證和隱私等級：

◆第一等級是無隱私，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。

◆第二等級是無隱私認證，即 AuthNoPriv。

◆第三等級是 AuthPriv。它不僅要進行認證，而且要對 SNMP 資料進行加密。

用戶名稱 說明如下：

管理系統在取得 HERHSIANG HSecurity+的運作資訊時，所要輸入的認證名稱。

認證協議 說明如下：

支援 HMAC_MD5_96、HMAC_SHA_96 認證協議。

認證密碼 說明如下：

管理系統在取得 HERHSIANG HSecurity+的運作資訊時，所要輸入的認證密碼。

加密協議 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。

加密密碼 說明如下：

管理系統以加密方式取得 HERHSIANG HSecurity+的運作資訊時，所要輸入的密碼。

步驟1. 於【網路服務】之【SNMP】功能中，勾選【啟動 SNMP Agent】並新增下列資料：

- 【裝置名稱】預設為 Firewall，可更動之。(圖 5-11)
- 【裝置所在地】預設為 Taipei, Taiwan.，可更動之。
- 【登入名稱】預設為 public，可更動之。
- 【聯絡人】預設為 help@common.com，可更動之。
- 【註解】預設為 Firewall，可更動之。

圖 5-11 SNMP Agent WebUI 設定視窗

步驟2. 於【SNMP】之【SNMP Agent】功能中，勾選【啟動 SNMPv3】並新增下列資料：

- 【安全等級】：預設是 AuthPriv。
- 【用戶名稱】預設為 public，可更動之。
- 【認證協議】預設為 MD5，可更動之。
- 【認證密碼】輸入 HSecurity+運作資訊時需確認之密碼。
- 【加密協議】預設為 DES，可更動之。
- 【加密密碼】輸入加密密碼數值。
- 點選【儲存】鈕。
- 完成【SNMP Trap】設定，由此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 HERHSIANG HSecurity+的異常警訊。（會將連線/斷線及駭客攻擊時的訊息轉送到設定的 SNMP Trap 訊息接收位址）（如圖 5-12）

圖 5-12 SNMP Trap WebUI 設定視窗

第六章 VPN

HSecurity+採 VPN 方式建立安全的網路連接，以整合企業的各個遠地網路與全球外勤人員遠地個人電腦，提供公司企業與遠端使用者一個安全便利的網路加密方式， 讓企業在網際網路上傳遞資料時，得到最佳的效能及保密效果，更節省管理者管理太多鑰匙的麻煩。

HSecurity+ 支援 3 種 VPN 建立的方式

【IPSec 】：系統管理員可以利用 IPSec 協定，建立 Site to Site 的 VPN 通道，通道 2 端的溝通資料，都會以 DES、3DES、AES 之一種加密，無法讓其他人就算攔截通道的封包也無法順利解出其中傳地的內容。

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

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

如何運用網路驗證

建立虛擬私有網路驗證 Virtual Private Network (VPN)，需先將 IPSec 自動加密、PPTP 伺服器或 PPTP 用戶端的連線彼此連線，即可為連線兩端建立安全保密的網路通訊。

6-1、IPSec Tunnel

【IPSec Tunnel】專有名詞解釋：

啟動

可設定開啟或關閉 IPSec Tunnel 伺服器。

VPN 通道名稱

定義 IPSec 自動加密名稱，此名稱可以是任何中英文文字，方便管理者辨識。

使用的介面

本地端使用的網路介面。

本地端網路

本地端的子網路區段。

遠端網路

目的端的子網路區段。

Preshared Key

VPN 雙方進行連線時用來進行 IPSec 加密用的金鑰。

ISAKMP 演算法

「IP Security Association Key Management Protocol」(ISAKMP) 就是提供一種方法供兩個設備建立安全性關聯 (SA)。

SA(Security Association) 對兩台電腦之間進行連線編碼，指定使用哪些演算法和什麼樣的金鑰長度或實際加密金鑰。事實上 SA 不止一個連線方式：從兩台電腦 ISAKMP SA 作為起點，必須指定使用何種加密演算法 (DES、triple DES、40 位元 DES 或根本不用)、使用何種認證。

IPSec 演算法

VPN 連線的資料加密模式。

DES/3DES

3DES 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

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。

SHA1 安全雜湊演算法 (Secure Hash Algorithm，SHA)

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

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。

遠端 ID / 本地 ID

一般而言，IPSec 通道會利用 WAN 的 IP 位址，當作雙方溝通辨識的依據，管理者可以自訂 ID 取代 WAN 的 IP 位址，ID 的格式有下列 2 種，@1.1.1.1 的 ip 位址格式或是@abc.com 的功能變數名稱格式，設定時一定要注意，2 端的資料一定要戶相對稱。

DPD (Dead Peer Detection) 偵測 VPN 斷線機制說明如下：

DPD 是一種自動偵測 VPN 斷線機制的標準協定，可自動判別 VPN 另一方聯機是否存在，再配合 VPN 狀態查詢，即可清楚明白的看到目前是否聯機，以確保 VPN 斷線時，可做出第一時間的反應與處理。

範例：兩台 HSecurity+建立的 IPSec VPN 連線，存取特定網段的資源

甲公司　**WAN IP 為 111.11.11.11，LAN IP 為 192.168.1.0/24**

乙公司　**WAN IP 為 222.22.22.22，LAN IP 為 192.168.2.0/24**

IPSec Tunnel 連線環境架構圖（圖 6-1）

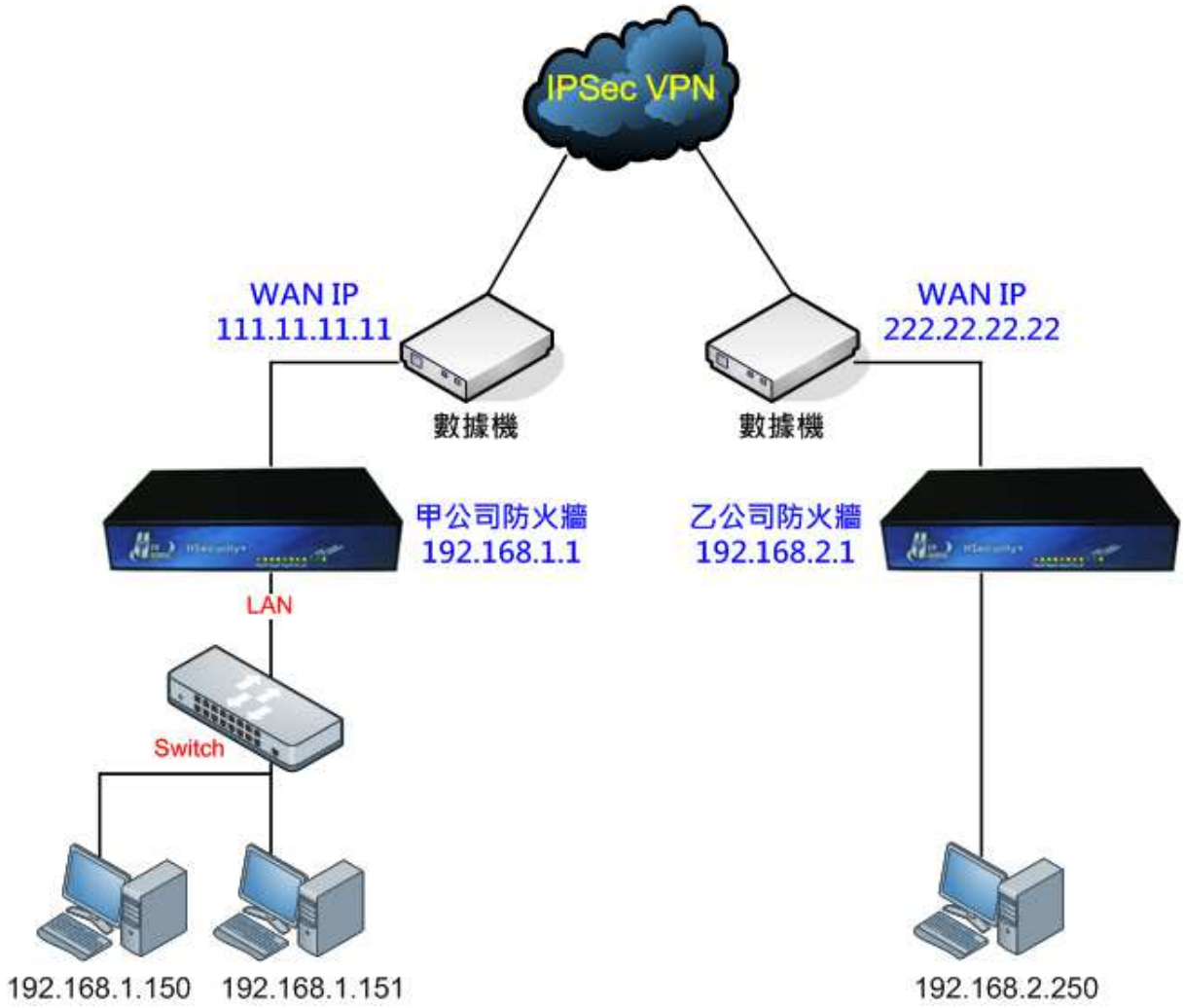

圖 6-1 IPSec VPN 連線之架設環境

IPSec VPN 設定步驟

預設閘道為 HSecurity+的 LAN IP 192.168.1.1，以下為其設定步驟：

步驟1. 進入甲公司 HSecurity+預設位址 192.168.1.1 的管理介面，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Tunnel】次功能選項。並點選【新增】功能。（圖 6-2）

圖 6-2 IPSec VPN 通道新增視窗

步驟2. 於【新增 VPN 通道】中，啟動 VPN 連線並填寫所使用的 VPN 連線名稱為【乙公司連線】，選擇甲公司的 HSecurity+用來建立 VPN 連線的【外部網路介面】位址 WAN1（圖 6-3）

步驟3. 於甲公司端填寫使用的網路區段。

- 本地端網路（甲公司）內部網路位址 192.168.1.0 及遮罩 255.255.255.0(/24)。
- 填入遠端網路（乙公司）內部網路位址 192.168.2.0 及遮罩 255.255.255.0(/24)

圖 6-3 IPSec VPN 連線名稱和使用的外網路介面設定表單

IKE 設定(Phase1)

步驟4. 選擇連線模式，UTM 防火牆支援 Main Mode 跟 Aggressive Mode2 種模式管理者根據需求選擇適當的模式套用。（圖 6-4）

步驟5. 填入連線的【加密金鑰】，『herhsiang』。

步驟6. 【ISAKMP 演算法】雙方開始進行連線溝通時，選擇建立連線時所需的演算法，可以選擇的【加密演算法】為 DES、3DES、AES 等 3 種，預設是 DES。

【認證演算法】，可以選擇 MD5 或 SHA1，預設是 MD5 認證方式。

啟用 自動配對機制時，系統會將所有的演算組合匯入條例中，如果 HSecurity+ 當 SERVER 端，代表系統會自動找出相同的組合跟遠端連線。

DH Group ，當加密協定是 AES 時，可以選擇 2、5、14、15、16、17、18，當加密協定為 DES 或 3DES 時，只可以選 1、 2、5。

步驟7. 本地端 ID，預設是用 WAN IP 位址當作 ID，管理者可以選擇用功能變數名稱當作 ID，使用範例為 @1.1.1.1 或是 @abc.com

步驟8. 遠端 ID 使用方式跟本地 ID 一樣。

步驟9. IKE SA 生存時間，預設是 3 小時，當 IKE 建立後超過設定時間，系統會重新產生一個新的 IKE SA。

圖 6-4 IPSec 加密及認證方法設定

IPSec 設定(Phase2)

步驟10. 【IPSec 演算法】表單中，可以選擇的【加密演算法】為 DES、3DES、AES 等 3 種，預設是 DES。

【認證演算法】，可以選擇 MD5 或 SHA1，預設是 SHA1 認證方式。

啟用 自動配對機制時，系統會將所有的演算組合匯入條例中，如果他 HSecurity+ 當 SERVER 端，代表系統會自動找出相同的組合跟遠端連線。

步驟11. Perfect Forward Secrecy (PFS)，預設是不啟動，啟動後可以選 DH Group。

DH Group ，當加密協定是 AES 時，可以選擇 2、5、14、15、16、17、18，當加密協定為 DES 或是 3DES 時，只可以選 2、5。

步驟12. IPSec SA 生存時間，1~3 小時可供選擇，預設是 3 小時。

步驟13. 設定 DPD 的偵測時間，DPD 的偵測間隔【30】秒，逾時【300】秒就認為是斷線。（圖 6-5）

步驟14. 關閉網路芳鄰協定，關閉後 網路芳鄰的協定會被阻擋。

圖 6-5 IPSec 偵測斷線機制設定

註 1；啟用 DPD功能，當ＶＰＮ偵測對方沒反應時，hold 代表系統會保留原來 IPSec SA ，等待資料，Clear 代表會將這個通道清除等待新的連線， Restart 會將這個 IPSec SA 刪除，重新建立ＶＰＮ通道。

乙公司的設定步驟

乙公司的預設閘道為 HSecurity+的 LAN IP 192.168.2.1，以下為其設定步驟：

步驟1. 進入乙公司 HSecurity+預設位址 192.168.2.1 的管理介面，在左方的功能選項中，點選【VPN】功能，再點選【IPSec Tunnel】次功能選項。並點選【新增】功能。（圖 6-7）

圖 6-7 IPSec VPN 通道新增視窗

步驟2. 於【新增 VPN 通道】中，啟動 VPN 連線並填寫所使用的 VPN 連線名稱為【甲公司連線】，選擇乙公司的 HSecurity+用來建立 VPN 連線的【外部網路介面】位址 WAN1。（圖 6-8）

步驟3. 於乙公司端填寫使用的網路區段。

- 本地端網路（乙公司）內部網路位址 192.168.2.0 及遮罩 255.255.255.0(/24)。
- 填入遠端網路（甲公司）內部網路位址 192.168.1.0 及遮罩 255.255.255.0(/24)

圖 6-8 IPSec VPN 連線名稱和使用的外網路介面設定表單

IKE 設定(Phase1)

步驟4. 選擇連線模式，UTM 防火牆支援 Main Mode 跟 Aggressive Mode2 種模式管理者根據需求選擇適當的模式套用。(圖 6-9)

步驟5. 填入連線的【加密金鑰】，『herhsiang』。

步驟6. 【ISAKMP 演算法】雙方開始進行連線溝通時，選擇建立連線時所需的演算法 ，可以選擇的【加密演算法】為 3DES、DES、AES 等 3 種，預設是 DES。

【認證演算法】，可以選擇 MD5 或 SHA1，預設是 MD5 認證方式。

啟用 自動配對機制時，系統會將所有的演算組合匯入條例中，如果他當 SERVER 端，代表系統會自動找出相同的組合跟遠端連線。

DH Group ，當加密協定是 AES 時，可以選擇 2、5、14、15、16、17、18，當加密協定為 DES 或是 3DES 時，只可以選 1、2、5。

步驟7. 本地端 ID，預設是用 WAN IP 位址當作 ID，管理者可以選擇用功能變數名稱當作 ID，使用範例為 @1.1.1.1 或是 @abc.com

步驟8. 遠端 ID 使用方式跟本地 ID 一樣。

步驟9. IKE SA 生存時間，預設是 3 小時，當 IKE 建立後超過設定時間，系統會重新產生一個新的 IKE SA。

IPSec 設定(Phase2)

步驟10. 【IPSec 演算法】表單中，可以選擇的【加密演算法】為 3DES、DES、AES 等 3 種，預設是 DES。

【認證演算法】，可以選擇 MD5 或 SHA1，預設是 MD5 認證方式。

啟用 自動配對機制時，系統會將所有的演算組合匯入條例中，如果他當 SERVER 端，代表系統會自動找出相同的組合跟遠端連線。

步驟11. Perfect Forward Secrecy (PFS)，預設是不啟動，啟動後可以選 DH Group。

DH Group ，當加密協定是 AES 時，可以選擇 2、5、14、15、16、17、18，當加密協定為 DES 或是 3DES 時，只可以選 1、 2、5。

步驟12. IPSec SA 生存時間，1~3 小時可供選擇，預設是 3 小時。

圖 6-9 IPSec 認證方法設定表單

步驟13. 設定 DPD 的偵測時間，DPD 的偵測間隔【30】秒，逾時【300】秒就認為是斷線。（圖 6-10）

步驟14. 關閉網路芳鄰協定，關閉後 網路芳鄰的協定會被阻擋。

圖 6-10 IPSec 偵測斷線機制設定表單

步驟15. 完成 IPSec Tunnel 設定。（圖 6-11）

圖 6-11 IPSec Tunnel 設定完成畫面

VPN 通道控制方法

- 【介面】：目前 IPSec VPN 使用的實體介面，  ：代表 WAN1，  ：代表 WAN2。
- 【狀態】：  ：代表斷線，  ：代表連線。
- 【啟動】：控制 IPSec VPN 啟動與暫停的按鈕，  ：代表目前是啟動中，  ：這一條 VPN 被暫停。
-  ：代表修改這個通道的設定。
- 【紀錄】：  ：這一條 VPN 的通聯記錄，IPSec VPN 通道如果跟對方有溝通紀錄，按下去會開啟新視窗，資料是照時間排序，最新的訊息在最後一頁。（圖 6-12）

時間	號碼	事件
2010-04-23 16:50:03		terminating SAs using this connection
2010-04-23 16:50:03		terminating SAs using this connection
2010-04-23 16:50:03		terminating SAs using this connection
2010-04-23 16:50:03	#2	initiating Main Mode

圖 6-12 IPSec Tunnel 的通聯記錄

6-2、PPTP 伺服器

【PPTP 伺服器】名詞解釋：

PPTP 伺服器

可設定啟動或關閉 PPTP 伺服器。

遠端 IP

PPTP 用戶端連入 PPTP 伺服器時，分配給遠端用戶端網路位址。

DNS1、DNS 2

PPTP 用戶端連入 PPTP 伺服器時，分配給遠端用戶端的 DNS 伺服器位址。

WINS1、WINS 2

PPTP 用戶端連入 PPTP 伺服器時，分配給遠端用戶端的 WINS 伺服器位址。

設定 PPTP 伺服器

啟用 HSecurity+的 PPTP 伺服器，讓遠端用戶可以利用 PPTP 的撥接軟體跟 HSecurity+ 的 PPTP 伺服器建立加密的 VPN 連線，以下為其設定步驟：

步驟1. 進入 HSecurity+的管理介面，在左方的功能選項中，點選【VPN】功能，再點選【PPTP 伺服器】次功能選項。

步驟2. 先啟用 PPTP 伺服器功能。（圖 6-13）

- 【啟用】：要不要啟用 PPTP 伺服器。
- 【分配的 IP 位址範圍】：要分配給撥進來用戶端分配的 IP 位址及範圍。
- 【DNS1-2】：分配給遠端用戶端的 DNS 伺服器位址。
- 【WINS1-2】：分配給遠端用戶端的 WINS 伺服器位址。

圖 6-13 PPTP 伺服器設定

建立帳號

步驟3. 選擇【新增帳號】選項，在此要建立用戶端的撥入帳號。(圖 6-14)

- 【啟用】：要不要啟用這個帳號。
- 【帳號】：PPTP 用戶端撥入使用的帳號。
- 【密碼】：PPTP 用戶端撥入使用的密碼。
- 【用戶端的 IP 位址】：PPTP 用戶端撥入使用的 IP 位址，除了可以由 PPTP 伺服器按照設定的範圍分配外，管理者也可以給特定的帳號，給予特定的 IP 位址或是範圍。

  使用 IP 位元址及範圍的選項需要搭配遠端的 PPTP 伺服器，其目的是利用 PPTP 通道技術，建立一個 Site to Site 的 VPN ，它的作用跟 IPSec 通道有異曲同工之意。

圖 6-14 PPTP 帳號建立

註：用戶端 IP 位址的建立有三種建立方式，分別為使用配給的 IP 位址、自行輸入 IP 位址與輸入 IP 位址及範圍。

PPTP 通道控制方法

步驟4. 建立好的 PPTP 帳號會在【PPTP 帳號列表】中出現，管理者可以在此控制，每一個 PPTP 帳號的啟用與關閉。（圖 6-15）

- 【帳號】：PPTP 用戶端撥入使用的帳號。
- 【狀態】：：代表斷線，：代表連線。
- 【啟動】：控制 PPTP VPN 啟動與暫停的按鈕，：代表目前是啟動中，：這一個 PPTP 帳號是被暫停，點選暫停用戶無法利用 PPTP 它來撥接。

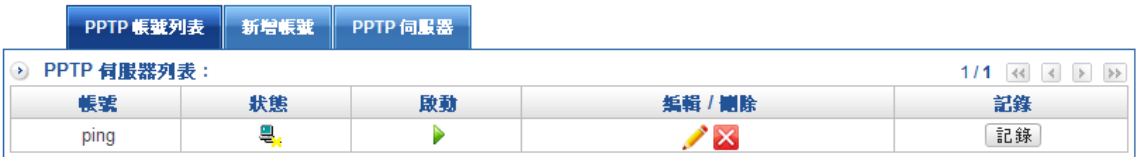

圖 6-15 PPTP 帳號列表控制

步驟5. 【紀錄】：記錄：這一條 VPN 的通聯記錄，PPTP 用戶如果有撥入，在此會顯示其撥接紀錄，按下去會開啟新視窗。（圖 6-16）

- 【時間】：PPTP 用戶端撥入開始的時間。
- 【遠端網路 IP】：PPTP 用戶端使用的 IP 位址。
- 【事件】：PPTP 用戶端撥入開始或是結束事件，結束的事件系統會自動計算總共使用的時間，單位是『小時:分』，低於 1 分鐘的時間統統被紀錄成 00:00。

通道名稱 : hao　每三十秒　自動更新　匯出　清除　1 / 38　1　GO

時間	IP 位址	事件
04-25 08:08	192.168.160.190	Login
04-24 18:20	192.168.160.190	Logout , used time (01:36)
04-24 16:44	192.168.160.190	Login
04-24 16:20	192.168.160.190	Logout , used time (03:06)
04-24 13:14	192.168.160.190	Login
04-24 13:12	192.168.160.190	Logout , used time (05:05)
04-24 08:07	192.168.160.190	Login
04-23 17:58	192.168.160.190	Logout , used time (09:53)

圖 6-16 PPTP 帳號紀錄

6-3、PPTP Client

【PPTP 用戶端】名詞解釋：

帳號

PPTP 用戶端連入 PPTP 伺服器帳號。

密碼

PPTP 用戶端連入 PPTP 伺服器密碼。

遠端伺服器

PPTP 用戶端連入 PPTP 伺服器網路位址。

遠端子網路

PPTP 伺服器端的內部網路區段。

建立 PPTP 用戶端

啟用 HSecurity+的 PPTP 用戶端，讓本地端用戶利用 PPTP 建立的 VPN 跟遠端的 PPTP 伺服器建立加密的 VPN 連線，以下為其設定步驟：

步驟1. 進入 HSecurity+的管理介面，在左方的功能選項中，點選【VPN】功能，再點選【PPTP Client】次功能選項。

步驟2. 新增一個 PPTP 用戶端。（圖 6-17）

- 【名稱】：這個 PPTP 用戶端的名稱，可以是任何中英文。
- 【啟動】： PPTP 用戶端要不要啟動。
- 【帳號】：PPTP 用戶端撥入使用的帳號。
- 【密碼】：PPTP 用戶端撥入使用的密碼。
- 【遠端伺服器】：PPTP 伺服器的 IP 位址，也就是 PPTP 用戶端要撥接的 IP 位址。
- 【遠端子網路 IP】：PPTP 伺服器的內部 IP 區段。
- 【遠端子網路遮罩】：PPTP 伺服器的內部 IP 子網路遮罩。

圖 6-17 建立 PPTP 用戶端

PPTP 通道控制方法

步驟3. 建立好的 PPTP 帳號會在【PPTP 列表】中出現，管理者可以在此控制，每一個 PPTP 帳號的啟用與關閉。（圖 6-18）

- 【名稱】：PPTP 用戶端的容易辨識的名稱。
- 【帳號】：PPTP 用戶端撥入使用的帳號。
- 【遠端伺服器】：PPTP 伺服器的 IP 或網功能變數名稱。
- 【遠端子網路】：PPTP 伺服器端的內部網路。
- 【狀態】：：代表斷線，：代表連線。
- 【啟動】：控制 PPTP VPN 啟動與暫停的按鈕，：代表目前是啟動中，：這一條 VPN 被暫停。

圖 6-18 PPTP 用戶端列表

步驟4. 【紀錄】：這一條 VPN 的通聯記錄，PPTP 用戶端如果有撥入，在此會顯示其撥接紀錄，按下去會開啟新視窗。（圖 6-19）

- 【時間】：PPTP 用戶端撥出或是斷線的時間。
- 【事件】：PPTP 用戶端撥出的事件，它會紀錄這個 VPN 通道，何時是『通』何時是『斷』。(註明 UP=撥通 DOWN=中斷)

圖 6-19 PPTP 用戶端的通聯記錄

6-4、VPN 管制

【VPN 對內部管制】名詞解釋：

來源網路位址（來源網路）& 目的網路位元址（目的網路）：

來源網路位址（來源網路）與 目的網路位元址（目的網路）是以 HSecurity+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元址，除了從『管制目標』中選擇外，也可以直接輸入使用者 IP 位址與 MAC 位址。

VPN 通道的管制有 2 個方向，外對內及內對外。

外對內的來源 IP 位址有下列預設名稱：

VPN_any 會代表所有 VPN 通道的外部區段，不論是用 IPSec 、PPTP 建立的 Site to Site 或是 PPTP 伺服器建立的單一個撥接帳號 ，都符合這個條件。

PPTP 伺服器的預設 IP 位址也會被列入預設的來源 IP 位址。

內對外的目的 IP 位元址有下列預設名稱：

VPN_any 會代表所有 VPN 通道的外部區段，不論是用 IPSec 、PPTP 建立的 Site to Site 或是 PPTP 伺服器建立的單一個撥接帳號 ，都符合這個條件。

管理者可以針對網路的需求，允許或是拒絕特定的 VPN 通道另一端進來的 IP 位址、通訊服務甚至時間。

預設的管制規則是一但 VPN 通道建立後，雙方的資料都可以自由的互相溝通、交換，除非來 VPN 管制處禁止它進來。

動作：

主要動作有兩種，分別為拒絕與允許，當設為允許動作時，任何滿足『基本設定』、『管制行為』的封包就會被放行，設為拒絕則此封包會被丟棄。

通訊協定：

可單獨管制 UDP 或 TCP 埠號，或全部管控。

通訊埠或群組：

系統管理員可以在【服務表】的【服務群組】選項中，新增服務群組名稱，將要提供的服務包含進去。

有了服務群組的功能，管理員在制訂管制條例時可以簡化許多流程。例如，有 10 個不同 IP 位址可以對伺服器存取 5 個不同的服務，如 HTTP、FTP、SMTP、POP3 和 TELNET，如果不使用服務群組的功能，總共需制定 10x5=50 條管制條例，但使用服務群組名稱套用在服務選項上，則只需一條管制條例即可達到 50 條管制條例的功能。

頻寬管理：

設定該條 VPN 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用）。

時間表：

設定該條 VPN 管制條例的生效時間。

VPN 對內部管制

以往對 VPN 的管制，大多都是從管制條例中進行或者是無法可管，但是 Herhsiang HSecurity+系列針對 VPN 的管制卻是直接從 VPN 中控管。VPN 對內部的管制，管控外點藉由 VPN 連線連到企業內部網路時，其連線通訊埠號、連線頻寬與連線時間等行為。

步驟1. 進入 HSecurity+的管理介面，在左方的功能選項中，點選【VPN】服務，再點選【VPN 管制】次功能選項。

步驟2. 新增一個 VPN 對內部管制。

步驟3. 設定相關基本設定與管制行為動作。

- 設定管制條例名稱、來源網路與目的網路位元址。
- 管制條例動作設定為「允許」或是「拒絕」。
- 通訊埠或群組可以任意選擇在「管制目標」>> 「服務表」中所建立的服務群組或是預設服務。
- 頻寬與時間表跟通訊埠一樣，可以從「管制目標」的「頻寬」跟「時間表」選擇須管制的項目。
- 啟用封包追蹤後，所有透過這一條 VPN 通道互相溝通的封包通聯紀錄，都可以查看。
- 按下「新增」，即可完成建立。（圖 6-20）

圖 6-20 新增 VPN 對內部管制條例

完成之後 VPN 的管制如下，管制條例是從優先權 1 開始執行，符合條件的項目就會執行，如果想要禁止非管制的資料進入內部網路，需要在最後一條將所有進入內部的封包全部禁止。（圖 6-21）

圖 6-21 完成 VPN 對內部管制條例建立

註 1：優先權：設定 VPN 管制條例使用分配的優先權。

註 2：預設的管制條例是不管，只要ＶＰＮ建立成功後，雙向的電腦就可以互通，如果期望只有管制的目標才通，建議在最後一條管制條例禁止所有的連線。

內部對 VPN 管制

是指透由內部經由 VPN 連到外部分點的連線，管制來源網路到目的網路所有行為動作，包含 VPN 連線通訊埠、頻寬與時程。

步驟1. 進入 HSecurity+的管理介面，在左方的功能選項中，點選【VPN】功能，再點選【VPN 管制】次功能選項。

步驟2. 新增一個 【內部對 VPN 管制】。

步驟3. 設定相關基本設定與管制行為動作。

- 設定管制條例名稱、來源網路與目的網路位元址。
- 管制條例動作設定為「允許」或是「拒絕」。
- 通訊埠或群組可以任意選擇在「管制目標」>> 「服務表」中所建立的服務群組或是預設服務。
- 頻寬與時間表跟通訊埠一樣，可以從「管制目標」的「頻寬」跟「時間表」選擇須管制的項目。
- 啟用封包追蹤後，所有透過這一條 VPN 通道互相溝通的封包通聯紀錄，都可以查看。

步驟4. 按下「新增」，即可完成建立。（圖 6-22）

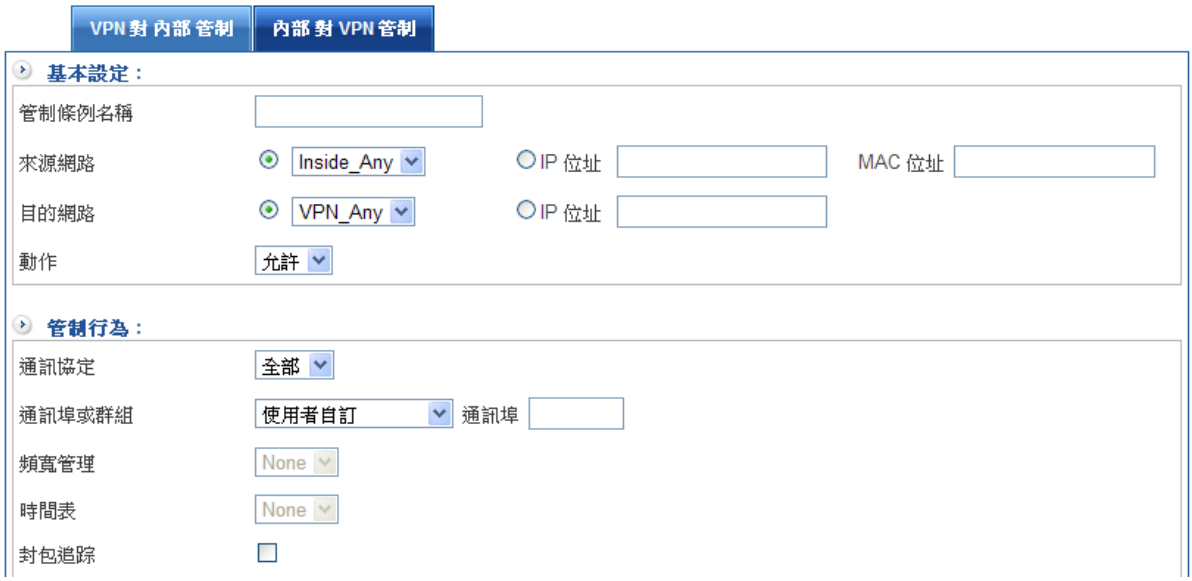

圖 6-22 新增內部對 VPN 管制條例

完成之後 VPN 的管制如下，管制條例是從優先權 1 開始執行，符合條件的項目就會執行，如果想要禁止非管制的資料到 VPN 通道的另一端，需要在最後一條將所有進入 VPN_any 的封包全部禁止。（圖 6-23）

圖 6-23 完成內部對 VPN 管制條例建立

第七章 網 路 工 具

使用者可由系統主動發送封包（Ping、Traceroute、DNS Query、Server Link），得知目前連外線路的資料傳輸品質和狀態。

【網路工具】名詞解釋：

PING

一般碰到網路不通的情況，很自然的就會使用 PING（Windows 跟 Linux 都相同）這個命令來檢查自己跟對方網路是否暢通，它使用 ICMP 協定。

Traceroute

traceroute，它可顯示封包在 IP 網絡經過的路由器的 IP 位址。

DNS Query

查詢 DNS 的詳細資料，目前可以查詢 ANY、SOA、NS、A、MX、CNAME、PTR 等資料，可以使用本機或是特定的 DNS 伺服器作為查詢依據。

Server Link

查詢 Server Link 的詳細資料，目前可以查詢伺服器開啟哪些服務埠，包含 FTP、SSH、TELNET、SMTP、DNS、HTTP、POP3、SAMBA、IMAP、SNMP、PROXY、MySQL、SMTPS、POP3、IMAPS 等服務使用情形。

IP Route / Rule

查詢目前 IP Route 與整個設備路由表。

Interface Information

查詢網路介面(WAN / LAN /DMZ)綁了哪些位址。

Wake UP

支援 Wake on Lan 的機制。

7-1 PING

於【線路偵測】之【Ping】功能中，可直接由 HSecurity+用 Ping 指令，發送封包到特定位址，以確認連外線路的資料傳輸狀況：（圖 7-1）

- 輸入封包發送的【目標 IP 或網功能變數名稱稱】。
- 輸入每個發送【封包大小】（預設為 32 Bytes）。
- 輸入【回應次數】（預設為 4）。
- 輸入【等待時間】（預設為 1 秒）。
- 選擇封包發送的來源【介面位址】，可以選擇 LAN、 WAN1、 WAN2、 DMZ 等四個網路介面。

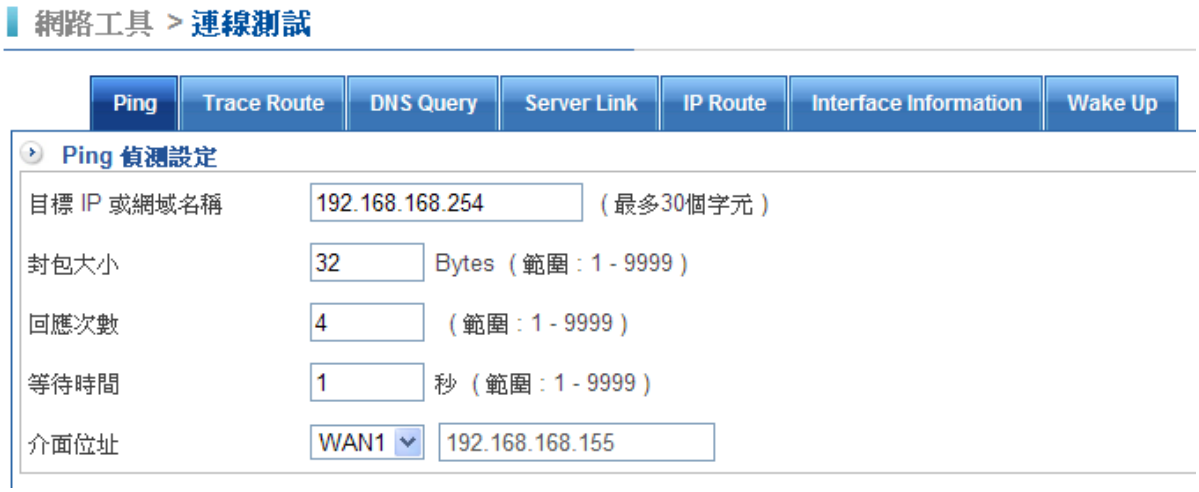

圖 7-1 Ping 偵測設定

- 按下【確定】鈕。（圖 7-2）

```
PING 192.168.168.254 (192.168.168.254) from 192.168.168.155 : 32(60) bytes of data.
40 bytes from 192.168.168.254: icmp_seq=1 ttl=64 time=0.780 ms
40 bytes from 192.168.168.254: icmp_seq=2 ttl=64 time=0.720 ms
40 bytes from 192.168.168.254: icmp_seq=3 ttl=64 time=0.638 ms
40 bytes from 192.168.168.254: icmp_seq=4 ttl=64 time=0.779 ms
```

圖 7-2 Ping 偵測結果

7-2 Traceroute

【線路偵測】之【Traceroute】功能中，可直接由 HSecurity+用 Traceroute 指令，發送封包到特定位址，以確認連外線路的資料傳輸狀況：（圖 7-3）

- 輸入封包發送的【目標 IP 或網功能變數名稱稱】。
- 輸入每個發送【封包大小】（預設為 40 Bytes）。
- 輸入【最大存活時間】（預設為 30 節點）。
- 輸入【等待時間】（預設為 2 秒）。
- 選擇偵測方式，可以用 ICMP、TCP、UDP 等方式。
- 選擇封包發送的【來源位址】。

圖 7-3 Traceroute 偵測設定

- 按下【確定】鈕。（圖 7-4）

```
traceroute to 168.95.1.1 (168.95.1.1), 30 hops max, 40 byte packets
 1  192.168.168.254 (192.168.168.254)  0.824 ms  0.781 ms  0.915 ms
 2  60-248-243-254.HINET-IP.hinet.net (60.248.243.254)  18.986 ms  20.866 ms  21.503 ms
 3  h214.s210.ts.hinet.net (168.95.210.214)  23.075 ms  23.158 ms  24.706 ms
 4  SKC1-3011.hinet.net (220.128.24.130)  29.029 ms  29.710 ms  30.404 ms
 5  220-128-16-22.HINET-IP.hinet.net (220.128.16.22)  34.524 ms  34.603 ms  34.682 ms
 6  202-39-179-185.HINET-IP.hinet.net (202.39.179.185)  34.628 ms  22.040 ms  24.051 ms
 7  dns.hinet.net (168.95.1.1)  24.065 ms  22.172 ms  23.741 ms
```

圖 7-4 Traceroute 偵測結果

7-3 DNS Query

查詢 DNS 的詳細資料，目前可以查詢 ANY、SOA、NS、A、MX、CNAME、PTR 等資料，可以使用本機或是特定的 DNS 伺服器作為查詢依據。

於【線路偵測】之【DNS Query】功能中，可直接由 HSecurity+用 DNS 查詢工具指令，發送封包到特定位址，以確認 DNS 資料傳輸狀況：（圖 7-5）

- 輸入代表使用本機為查詢的【DNS 伺服器 IP 位址名稱】。
- 輸入【查詢對象的名稱或 IP 位址】（最多 50 各字元）。
- 輸入欲查詢的【類型】。

圖 7-5 DNS 查詢工具

- 按下【確定】鈕。（圖 7-6）

註：【查詢對象的名稱或 IP 位址】：正向或是反查資料均可以在這裡填入相對應的 IP 位址或是網功能變數名稱稱。

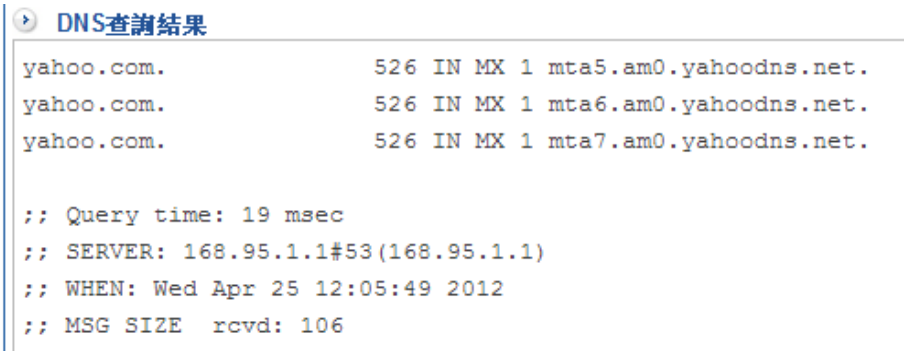

圖 7-6 DNS Query 偵測結果

7-4 Server Link

查詢 Server Link 的詳細資料，目前可以查詢伺服器開啟哪些服務埠，包含 FTP、SSH、TELNET、SMTP、DNS、HTTP、POP3、SAMBA、IMAP、SNMP、PROXY、MySQL、SMTPS、POP3、IMAPS 等服務使用情形。

於【線路偵測】之【Server Link】功能中，可直接由 HSecurity+檢查目前伺服器服務埠使用狀況：（圖 7-7）

- 輸入 IP 位址功能變數名稱名稱。

圖 7-7 DNS 查詢工具

- 按下【確定】鈕。（圖 7-8）

圖 7-8 Server Link 偵測結果

7-5 IP Route

點選 IP Route / Rule，HSecurity+會帶出目前設備路由表資料。（圖 7-9）

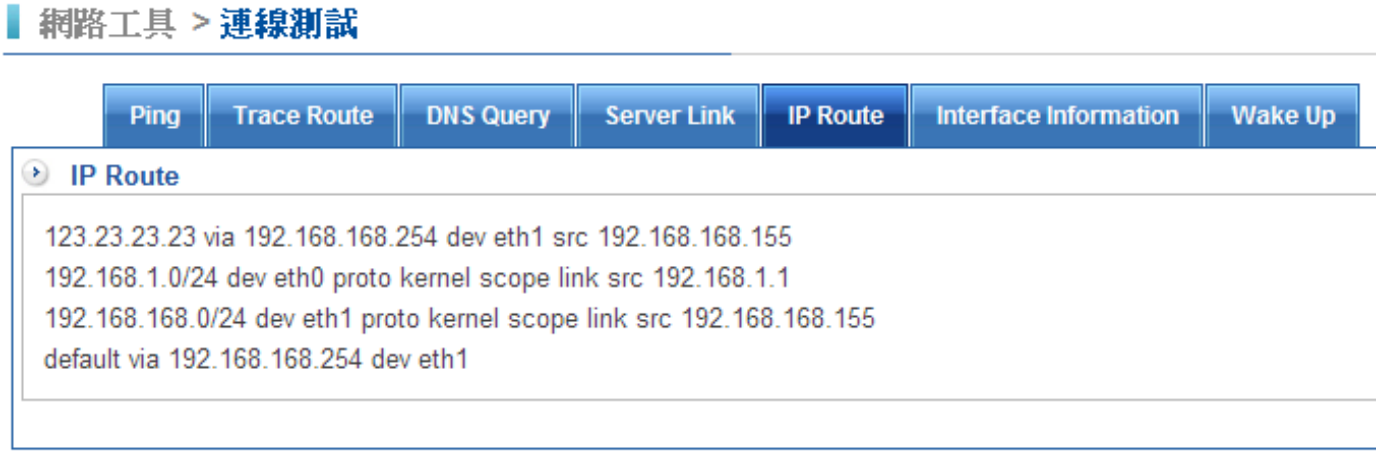

圖 7-9 IP Route / Rule 查詢工具

7-6 Interface information

選定來源位址(DMZ、WAN1、WAN2、LAN)，系統會秀出目前該網路介面概況。（圖 7-10）

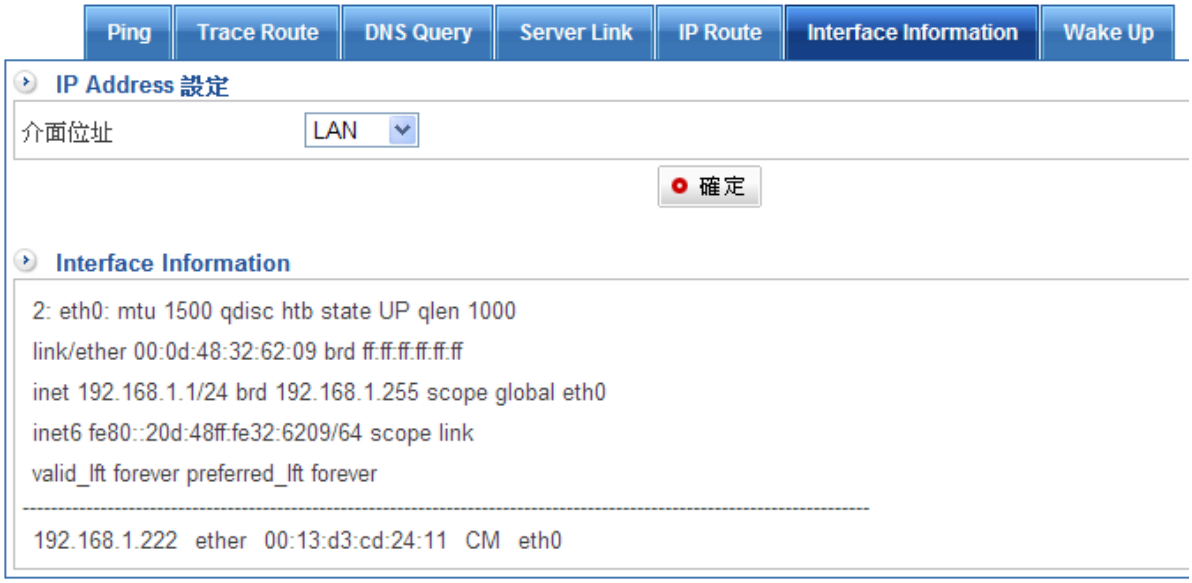

圖 7-10 IP Addr Show 查詢工具

7-7Wake Up

可透過 LAN 或 DMZ 介面，喚醒內部網路的電腦，被喚醒的電腦需要支援 Wake on Lan 的網路卡。（圖 7-11）

圖 7-11 Wake Up 工具

第八章 日誌

【登入事件】當 HSecurity+偵測到系統發生某些事件時，系統管理員可經由此事件登入功能，瞭解事件發生的時間詳細說明。

【登入事件】的名詞解釋及搜尋條件

電腦名稱

依電腦名稱做搜尋條件。

IP 位址

依 IP 位址做搜尋條件。

登入設定

記錄使用者登入主機時間。

系統設定

紀錄使用者登入管理介面更動時間設定、管理員、備份與升級、語系設定時間。

網路介面及路由

紀錄使用者登入管理介面更動網路介面、路由設定時間。

管制條例

紀錄使用者登入管理介面更動 LAN 的管制、DMZ 的管制、WAN 的管制時間。

管理目標

紀錄使用者登入管理介面更動位址表、服務表、頻寬管理、時間表、應用程式管理、URL 管理與虛擬伺服器設定時間。

網路服務

紀錄使用者登入管理介面更動 DHCP 服務、DNS 代理服務、DDNS 服務、DNS 服務、Web 代理服務與掃毒服務時間。

VPN

紀錄使用者登入管理介面更動 IPSec Tunnel、PPTP 伺服器、PPTP Client 時間。

事件紀錄保留

預設可保留一年(12 個月)。

系統操作

查詢登入事件的詳細資料，任何權限的管理者（VRead、Write），在 HSecurity+ 做的任何事情（新增、修改、刪除、查詢、下載）都會在這裡詳細的紀錄。（圖 8-1）

事件列表的說明如下：

- 【時間】：發生該事件的時間。
- 【帳號】：那個管理者帳號，觸發這個事件。
- 【IP 位址】：管理者帳號使用的 IP 位址。
- 【功能路徑】：管理者進入那一個管理畫面。
- 【動作】：管理者執行的動作，有（登入、新增、修改、刪除、搜尋、下載）等。
- 【內容】：管理者執行的動作前及後的詳細內容。

圖 8-1 事件列表

搜尋 說明如下：

- 可依照特定 IP 或相關事件特徵，來尋找儲存在 HSecurity+內所有符合條件之記錄。
- 【帳號】：登入帳號。
- 【電腦名稱】：用哪一個電腦登入系統。
- 【IP 位址】：用哪一個 IP 位址登入系統。
- 設定搜尋指定相關條件的記錄，按下【搜尋】鈕。（圖 8-2）

圖 8-2 事件搜尋

第九章 系 統 狀 態

使用者可隨時由系統狀態中，得知目前網路連線狀態。如區域網路與外部網路的 IP 位址、子網路遮罩、預設閘道、DNS 伺服器連線 IP 位址等各項資訊。

（一）【系統效能】：顯示目前 HSecurity+ CPU 使用率，負載、記憶體負載，系統負載，每個介面的上下傳流量也可以查詢上述資訊的歷史流量。

（二）【連線狀態】：記錄 HSecurity+之連線使用情況，包含上線數量、封包的紀錄等。

9-1、系統狀態

系統狀態

【系統效能】之【系統狀態】功能中，會顯示目前 HSecurity+系統狀態之相關訊息，總結來說計有【CPU 負載圖】、【記憶體負載圖】、【系統負載圖】等 3 種，其中【系統負載圖】需要管理者啟動才會出現。

- 【CPU 負載圖】：顯示 HSecurity+ CPU 目前使用狀況。（圖 9-1）

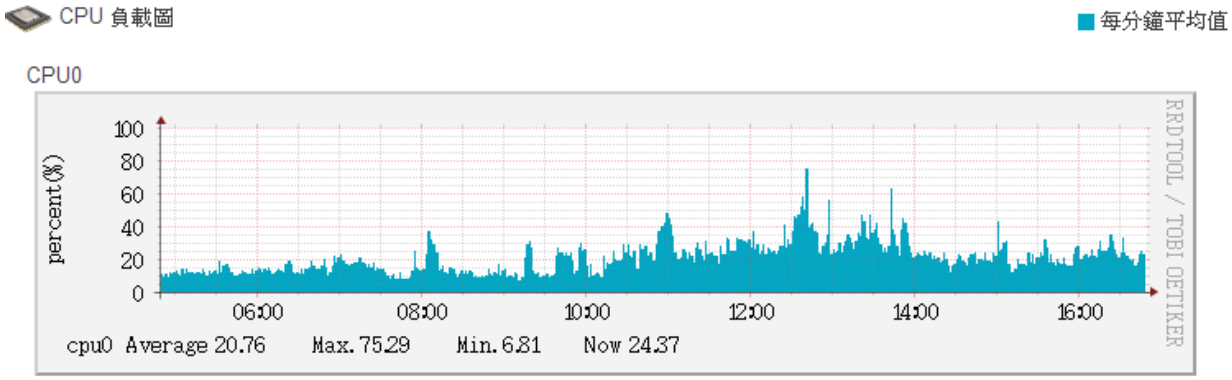

圖 9-1 CPU 負載

- 【記憶體負載圖】：顯示 HSecurity+ 記憶體使用狀況。（圖 9-2）

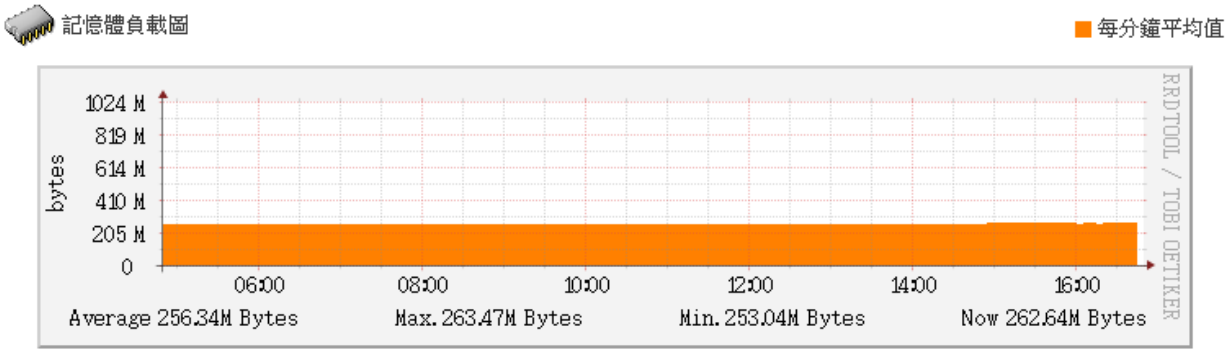

圖 9-2 記憶體負載

- 【系統負載圖】：顯示 HSecurity+ 系統的綜合效能，必須啟動『開啟系統負載圖』才會出現。（圖 9-3）

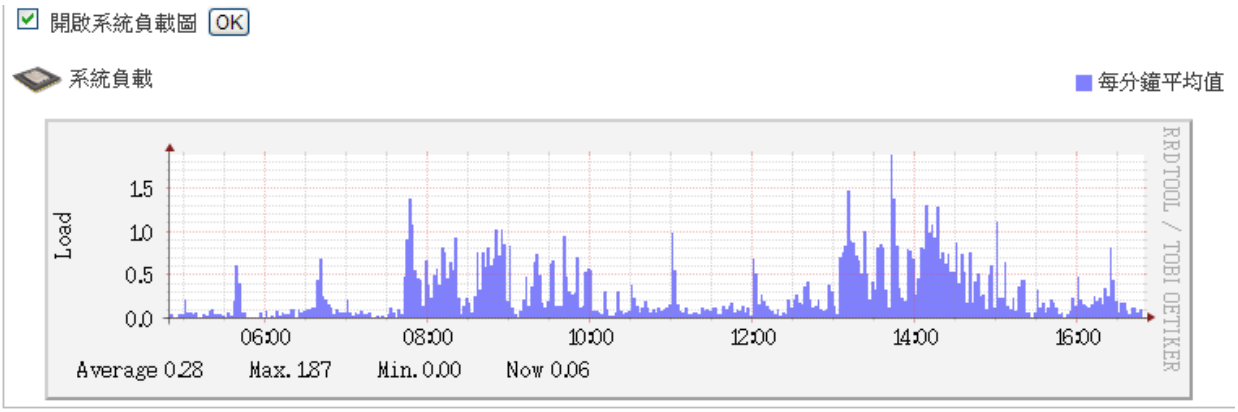

圖 9-3 系統負載

網路流量

於【系統效能】之【網路流量】功能中，會顯示目前 HSecurity+所有介面（LAN 、WAN1、 WAN2、 DMZ）網路流量之相關訊息，藍色（圖形上方）是上傳流量，綠色（圖形下方）是下載流量，以 WAN1 的圖示為例。（圖 9-4）

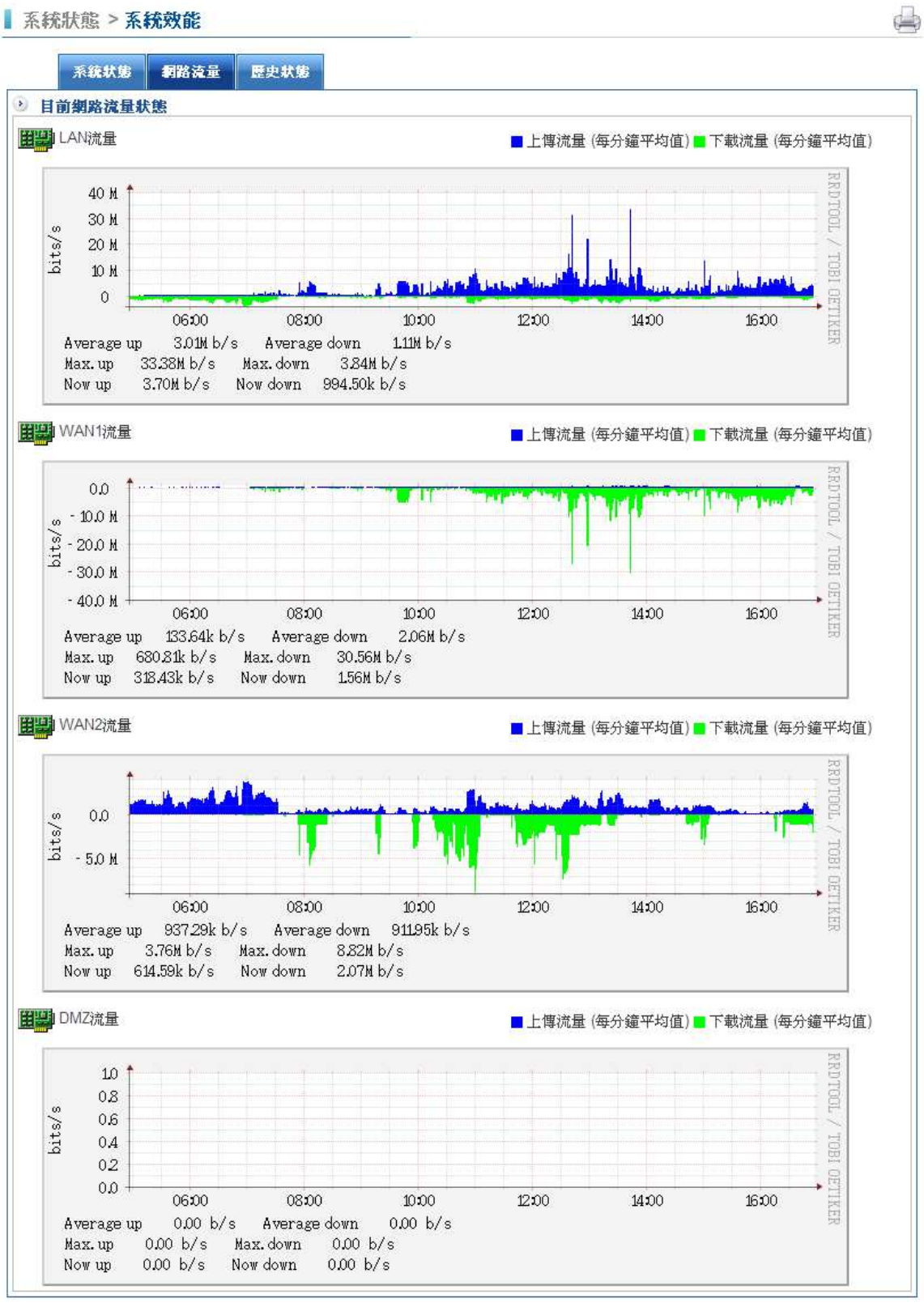

圖 9-4 網路介面流量

歷史狀態

搜尋特定時間區間內的訊息，如 CPU 負載、記憶體負載，系統負載、LAN 、WAN1、WAN2、 DMZ 網路流量等，選擇要查詢的區間及項目，按下搜尋鍵就可以。

- 設定查詢目標【CPU 負載】。
- 設定搜尋日期，2011-10-06 00：00 ~ 2011-10-06 23：00。
- 按下【查詢】鈕。（圖 9-5）

圖 9-5 CPU 負載搜尋

9-2、連線狀態

成員列表

【連線狀態】之【成員列表】功能中，會顯示目前 HSecurity+內網電腦的狀態，是開機或是關機，從那一個網路介面來（LAN 或是 DMZ），也可以按照大小排序。（圖 9-6）

- 【OS】內網電腦作業系統偵測是一個相當難的動作，HSecurity+會主動偵測內部電腦的作業系統及目前對外開放的服務，不論是在掌握公司內部的資源或是預防木馬跳板上，都有非常好的參考價值。
- 【啟用 OS 偵測功能】：可以關閉或是啟用偵測機制，當選擇啟用偵測機制時也可以設定(例外 IP)，排除不想被偵測的區段。
- 【電腦名稱】：該部電腦的 NETBIOS 名稱。
- 【IP 位址】：該部電腦的 IP 位址。
- 【MAC 位址】：該部電腦的 MAC 位址。
- 【介面】：該部電腦的來源介面，是 LAN 還是 DMZ。
- 【狀態】：：代表電腦開機中，：代表電腦關機中。
- 【目前上線成員數】：內部網路，包含 DMZ 區，總共有多少台設備是開機中的。
- 【立即更新】：按鈕，按下後馬上更新所有的訊息。
- 【】：按照大小排序。

圖 9-6 成員列表

連線追蹤

藉由網路封包的分析及追蹤，分析每一個使用者網路使用行為，分析的資料是從電腦開機到關機，每個用戶利用網路，在幾點幾分，花了多少時間、作了哪些事情。

此主要是以來源端名稱作為分類，顯示目前所有使用者之紀錄，包含 IP 位址、連線數、上傳流量、下載流量、紀錄(紀錄所使用協定、來源 IP、目的 IP、通訊埠、上傳封包、下載封包、上傳 Bytes、下載 Bytes)。

【連線狀態】之【連線追蹤】功能中，會顯示目前 HSecurity+內網電腦所有使用者上傳、下載流量統狀態：（圖 9-7）

- 【總連線數】：顯示當下的連線數，顯示的格式為 ，這個頁面聯線數總和/全部連線數。
- 【電腦名稱】：顯示目前該電腦 IP 位址。
- 【IP 位址】：該部電腦的 IP 位址。
- 【連線數】：該部電腦目前對外已經建立的連線數。
- 【上傳流量】：該部電腦目前的上傳流量，單位是 Kbytes/Second。
- 【下載流量】：該部電腦目前的下載流量，單位是 Kbytes/Second。

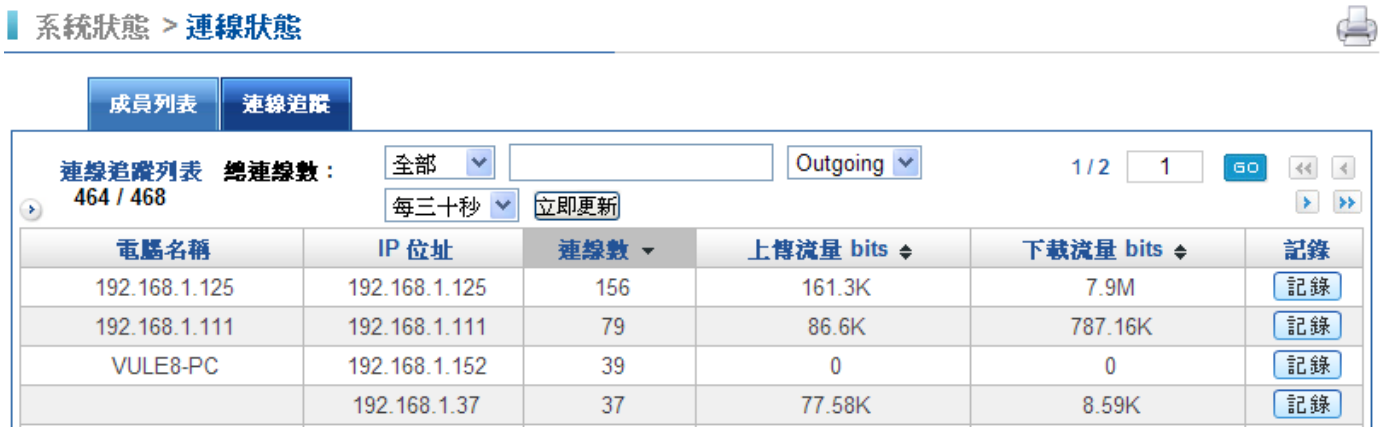

圖 9-7 連線數及流量列表

選擇項目：

- 【全部】：只顯示打一條對外線路的資料。
- 【　　】：（圖 9-7）紅色框框內可以單獨輸入一個 IP 位址，空白是顯示全部。
- 【Outging/Incoming 】：顯示哪一個方向的連線數。
- 【時間 】：每隔幾秒鐘顯示一次。
- 【立即更新 】：按下後可以馬上更新連線數資訊。

按下【紀錄】按鈕後，會出現更詳細的封包通聯訊息。（圖 9-8）

- 【目的 IP 搜尋】：指定搜尋特定的目的 IP 位元址。
- 【時間 】：每隔幾秒鐘顯示一次。
- 【Clear /Clear all 】：清除顯示資訊。
- 【Refresh 】：按下後可以馬上更新連線數資訊。
- 【匯出 】：將資料表匯出，以供查詢。
- 【來源 IP 】：該部電腦的 IP 位址。
- 【目的 IP】：目的 IP 位元址。
- 【通訊埠】：來源及目的通訊埠。
- 【上傳】：目前的上傳量。
- 【下載】：目前的下載量。
- 【上傳 Bytes】：累積的上傳量。
- 【下載 Bytes】：累積的下載量。
- 【自動更新】：按照設定的時間，自動更新封包統計值。

協定	來源 IP	目的 IP	通訊埠	外部網路	上傳封包	下載封包	上傳 bps	下載 bps
tcp	192.168.1.153	69.171.227.60	52817 -> 443	1	421	663	1.78M	2.39M
tcp	192.168.1.153	117.104.136.19	52907 -> 443	1	22	29	29.74K	194.15K
tcp	192.168.1.153	69.171.229.13	52607 -> 443	1	514	674	1.83M	4.77M
udp	192.168.1.153	60.28.205.36	6000 -> 25607	2	974	198	388.08K	66.64K
tcp	192.168.1.153	69.171.234.80	52829 -> 443	1	283	436	785.27K	3.38M

圖 9-8 使用者連線狀態

註：如果想監視特定電腦主機的即時連線封包結構，按下該電腦的 IP 位址後，畫面的下方會出現詳細的封包連線狀態，可設定多少時間更新畫面，包含來源 port、目的 IP、通訊埠、上傳封包、下載封包、上傳流量與下載流量。