your future life

2WAN 4LAN VPN 防火牆

具負載平衡，頻寬管理，VPN 與網路安全等功能

繁體中文使用手册

產品功能說明手冊使用許可協定

《產品功能說明手冊（以下稱”手冊”）使用許可協定》（以下稱”協定”）是用戶與俠諾科技股份有限公司（以下稱”俠諾”）關於手冊許可使用及相關方面的權利義務、以及免除或者限制俠諾責任的免責條款。直接或間接取得本手冊檔案以及享有相關服務的用戶，都必須遵守此協定。

重要須知：俠諾在此提醒用戶在下載、閱讀手冊前閱讀本《協定》中各條款。請您審閱並選擇接受或不接受本《協定》。除非您接受本《協定》條款，否則請您退回本手冊及其相關服務。您的下載、閱讀等使用行為將視為對本《協定》的接受，並同意接受本《協定》各項條款的約束。

【1】知識產權聲明

手冊內任何文字表述及其組合、圖示、介面設計、印刷材料、或電子檔等均受我國著作權法和國際著作權條約以及其他知識產權法律法規的保護。當用戶複製"手冊"時，也必須複製並標示此知識產權聲明。否則，俠諾視其為侵權行為，將適時予以依法追究。

【2】"手冊"授權範圍：

用戶可以在配套使用的電腦上安裝、使用、顯示、閱讀本"手冊"。

【3】用戶使用須知

用戶在遵守法律及本協定的前提下可依本《協定》使用本"手冊"。用戶若是違反本《協定》，俠諾將中止其使用權力並立即銷毀此"手冊"的複本。本手冊"紙質或電子檔案"，僅限於為資訊和非商業或個人之目的使用，並且不得在任何網路電腦上複製或公佈，也不得在任何媒體上傳播;及不得對任何"檔案"作任何修改。為任何其他目的之使用,均被法律明確禁止,並可導致嚴重的民事及刑事處罰。違反者將在可能的最大程度上受到指控。

【4】法律責任與免責聲明

【4-1】俠諾將全力檢查文字及圖片中的錯誤，但對於可能出現的疏漏，用戶或相關人士因此而遭受的直接或間接的經濟損失、資料損毀或其他連帶的商業損失，俠諾及其經銷商與供應商不承擔任何責任。

【4-2】俠諾為了保障公司業務發展和調整的自主權，俠諾擁有隨時自行修改或中斷軟體 / 手冊授權而不需通知用戶的權利，產品升級或技術規格如有變化，恕不另行通知，如有必要，修改或中斷會以通告形式公佈於俠諾網站的相關區塊。

【4-3】所有設定參數均為範例，僅供參考，您也可以對本手冊提出意見或建議，我們會參考並在下一版本作出修正。

【4-4】本手冊為解說同系列產品所有的功能設定方式，產品功能會按實際機種型號不同而有部份差異，因此部分功能可能不會出現在您所購買的產品上。

【4-5】俠諾保留此手冊檔案內容的修改權利，並且可能不會即時更新手冊內容，欲進一步瞭解產品相關更新訊息，請至俠諾官方網站流覽。

【4-6】俠諾（和/或）其各供應商特此聲明，對所有與該資訊有關的保證和條件不負任何責任，該保證和條件包括關於適銷性、符合特定用途、所有權和非侵權的所有默示保證和條件。所提到的真實公司和產品的名稱可能是其各自所有者的商標，俠諾（和/或）其各供應商不提供其他公司之產品或軟體等。在任何情況下,在由於使用或檔案上的資訊所引起的或與該使用或運行有關的訴訟中, 俠諾和/或其各供應商就因喪失使用、資料或利潤所導致的任何特別的、間接的或衍生性的損失或任何種類的損失，均不負任何責任，無論該訴訟是合同之訴、疏忽或其他侵權行為之訴。

【5】其他條款

【5-1】本協定高於任何其他口頭的說明或書面紀錄，所定的任何條款的部分或全部無效者，不影響其他條款的效力。

【5-2】本協定的解釋、效力及糾紛的解決，適用於臺灣法律。若用戶和俠諾之間發生任何糾紛或爭議，首先應友好協商解決。若協商未果，用戶在完全同意將糾紛或爭議提交俠諾所在地法院管轄。中國則以「中國國際經濟貿易仲裁委員會」為仲裁機構。

目 錄

一、簡介 1
二、多 WAN VPN 防火牆設定操作流程 3
2.1 系統性設定流程的需要 3
2.2 設定流程表 3
三、硬體安裝 6
3.1 VPN 防火牆 LED 顯示燈 6
3.2 VPN 防火牆的網路連接 8
四、登錄 VPN 防火牆 9
五、確定設備規格、狀態顯示以及登錄密碼和時間的設定 11
5.1 首頁顯示 11
5.2 登錄密碼及時間的修改和設定 16
六、進行廣域網路連線設定 19
6.1 網路設定 19
6.2 多 WAN 設定 32
七、內部區域網路設定 47
7.1 實體埠口管理設定 (預計未來加入) 47
7.2 埠口狀態即時顯示 (預計未來加入) 49
7.3 DHCP 發放 IP 伺服器 51
7.4 DHCP 狀態顯示 53
7.5 IP 與 MAC 位址綁定 54
7.6 IP 群組管理 58
八、QoS 頻寬管理功能 59
8.1 頻寬設定(QoS) 60
8.2 連線數管制 70
8.3 動態智慧頻寬管理（Smart QoS） 73
九、防火牆設定 75
9.1 基本設定 75
9.2 阻擋特定服務 79
9.3 存取規則設定 81
9.4 網頁內容管制 86
十、VPN 虛擬私有網路設定 90
10.1. VPN 虛擬私有網路（VPN） 90
10.2. QnoKey 126
10.3. QVM VPN 功能設定 132

十一、虛擬繞徑設定 138
11.1 虛擬遶徑 服務端（PPTP 伺服器） 140
11.2 虛擬遶徑 用戶端 143
十二、其他進階功能設定 145
12.1 DMZ/虛擬伺服器 145
12.2 UPnP 通訊協定 150
12.3 路由通訊協定 152
12.4 一對一 NAT 對應 155
12.5 DDNS-動態網域名稱解析 157
12.6 廣域網接口 MAC 位址設定 162
十三、工具程式功能設定 163
13.1 線上連線測試 163
13.2 系統軟體更新 165
13.3 系統設定參數儲存 166
13.4 網路管理設定(SNMP) 167
13.5 系統恢復 169
十四、日誌功能設定 171
14.1 系統日誌 171
14.2 系統狀態即時監控 176
14.3 流量統計 178
14.4 特定 IP 及通訊埠狀流量狀態 180
十五、登出 182
附錄一、設定介面及使用手冊章節對照 183
附錄二：常見問題解決 186
（1） 封鎖用戶下載 BT 種子 186
（2） 衝擊波及蠕蟲病毒的防制 187
（3） 阻止 QQLive 視屏直播設定 189
（4） ARP 病毒攻擊防制 191
附錄三：Qno 技術支援資訊 199

一、簡介

2WAN 4LAN VPN 防火牆（以下簡稱 VPN 防火牆）為一台符合中小 SME 企業等級經濟型,高效能整合之全功能的新一代設計之防火牆系統，除了具備絕大多數寬頻市場適用的對外連線能力外，還內建了 4 Port 10/100Mbps QoS 交換器，滿足多數企業對防火牆的市場需求。

VPN 防火牆提供了使用者自訂原為硬體 DMZ 埠口為防火牆的標準配備使用外，亦可針對寬頻廣域網路線路備援指定此 DMZ 埠口網路介面成為第二個 WAN port ，亦可彈性針對日後網路頻寬不夠、對外線路需求增加而提供高效能。

雙線路負載平衡模式(Intelligent Load Balancing & By Traffic Load Balance)支援 WAN 端的負載平衡，將線路效能發揮極致；配合新一代,多樣化之高安全整合性的防火牆設備需求環境，內建超高速的 Intel IXP 425 整合型 RISC CPU，透過時脈 266Mhz 的高速處理架構下，發揮超高的網路效能，處理速度直逼中，大型企業用戶專用之昂貴防火牆設備；可符合企業界廣泛的應用系統支援，防火牆效能可達 100Mbps 以上，且具備支援目前企業廣泛應用之虛擬私有網路 VPN 硬體加速模式，包含 IPSec DES/3DES 等 VPN 加密，以 3DES 方式運作效能可達 50Mbps 以上，不論式功能面,實用安全性等，十足超越目前大型昂貴設備之規格。

VPN 防火牆獨家研發了 QVM (Qno VPN Management)，跟有 QVM Server / Clinet 功能系列產品搭配使用，可以達到最簡單的 VPN 設定，只需輸入 User Name 及 Password 還有中心端 IP 地址，就可以簡單快速的建立 VPN 通道，並且若您為 QVM Server 端的話，經由中央控管介面輕鬆且加密的方式做遠程登入 QVM 用戶端做控制。

此 QVM 功能的搭配使用，可以做到 VPN 備援，讓您的企業 VPN 線路永遠保持連線，不受 ISP 的線路斷線問題所困擾。當然，為了保有產品優秀的彈性，VPN 防火牆亦提供傳統 IPSec VPN 的設定，讓其他產品只要支援標準 IPSec 的設備，都可以跟 VPN 防火牆於各辦公室，事業夥伴及遠端使用者一個安全便利的網路加密方式。包括 168 bitData Encryption Standard (3DES)，56 bit Data Encryption Standard (DES)，以及 AH/ESP 方式。VPN 功能提供了各分支點間或大多數遠端使用者採 VPN 方式將資料自動加密解密的通訊方式，支援 Gateway ToGateway，Client To Gateway 模式。

VPN 防火牆內建進階型防火牆功能，能夠阻絕大多數的網路攻擊行為, 使用了 SPI 封包主動偵測檢驗技術(Stateful Packet Inspection)，封包檢驗型防火牆主要運作在網路的層級，但是藉由執行對每個連結的動態檢驗，也擁有應用程式的警示功能，讓封包檢驗型防火牆可以拒絕非標準的通訊協定所使用的連結，預設自動偵測並阻擋.。VPN 防火牆亦同時支援使用網路地址轉換 Network Address Translation (NAT)功能以及 Routing 路由模式，使網路環境架構更為彈性，易於規劃管理。

Content Filtering 內容過濾功能允許企業內部自訂網路存取規則，管理頁面內建可新增移除的過濾名單，可讓管理者選擇應該禁止存取或記錄監控哪些種類的網站，如此可對學校或企業的 Internet 管理有明確的策略，自定過濾設定；透過完整的 OS 管理核心，VPN 防火牆提供線上多樣化的日誌(SysLog)

紀錄，支援線上管理設定工具，可清楚易懂的網路設定組態、並加強管理全部的網路安全存取政策、VPN、及其他服務等。

VPN 防火牆能充分保障各型分支機構辦公室及各點間通訊的安全，避免日益趨多的商業機密竊取與攻擊破壞等。專屬的 OS 獨立式作業平台，使用者無須具備專業級的網路知識即可易於安裝使用，透過瀏覽器如：IE、Netscape 等來使用設定與管理 VPN 防火牆。

二、多 WAN VPN 防火牆設定操作流程

本章節介紹用戶整體設定多 WAN VPN 防火牆操作流程，通過對 VPN 防火牆多 WAN 設定流程的瞭解可以很輕鬆的設定我們的網路，來有效的管理我們的網路，使 VPN 防火牆達到應有的功能，使 VPN 防火牆的效能達到最高。

2.1 系統性設定流程的需要

用戶可以通過以下操作流程設定我們的網路，能夠使我們的網路能夠有效利用頻寬，網路效能達到理想的效果，同時可以阻斷一些攻擊與預防一些安全隱患，透過流程設定更加方便用戶的安裝與操作，簡化維護管理的難度，使得用戶的網路設定一次到位。設定主要流程如下：

1、 硬體安裝。

2、 登錄設定視窗。

3、 確定設備規格及進行密碼和時間設定。

4、 進行廣域網連線的設定

5、 進行內部連線的設定：實體線路設定及 IP 位址設定。

6、 進行 QoS 頻寬管理設定：防止頻寬佔用情況。

7、 進行防火牆設定：預防攻擊及不當存取網路資源。

8、 其他特別設定：虛擬伺服器、UPnP、DDNS、MAC Clone。

9、 管理維護的設定：系統日誌、SNMP、及設定參數備份。

10、 VPN 虛擬私有網路、QnoKey、QVM VPN 功能設定。

11、 登出設定視窗。

2.2 設定流程表

下表主要闡述每個設定流程相對應的 VPN 防火牆管理內容以及此設定所達到的目的，如需詳細瞭解每步過程以及後面章節介紹所對應的內容可參考（附錄一、設定介面及使用手冊章節對照）。

#	設定	內容	目的
1	硬體安裝	建構用戶需要的網路	根據用戶實地網路的要求來安裝 VPN 防火牆硬體。
2	登錄設定視窗	從 Web 登入 VPN 防火牆設定視窗，瞭解系統資訊	登錄 VPN 防火牆的 Web 管理頁面。
3	確定設備規格	確定產品軟體版本以及工作情況	確定 VPN 防火牆規格，系統軟體版本，以及 VPN 防火牆工作狀況。
	進行密碼及時間設定	設定時間及修改密碼	安全的考慮修改登錄密碼。 設定 VPN 防火牆時間與廣域網路同步。
4	進行廣域網連線的設定	確定廣域網線路設定、頻寬調配、及協議綁定	連接廣域網路，透過頻寬的設定等能更好的利用頻寬，優化資料轉發能力。
5	進行內部連線的設定：實體線路設定及 IP 位址設定	鏡像埠口及 VLAN 設定。內部用戶 IP 的分配群組及管理	提供埠口鏡像功能，同時以埠口管理及 VLAN 的設定滿足內網相關需求，彈性提供固定 IP/DHCP 自動 IP 位址分配，方便用戶在不同網路環境的需要。IP 群組管理對一組 IP 位址做相同設定，簡化管理工作。
6	進行 QoS 頻寬管理設定，防止頻寬佔用情況的發生	廣域網埠、內部用戶或應用流量及連線數的限制	確保網路重要資訊不致延遲、確保網路重要應用服務連線順暢；進一步針對現有的頻寬進行管理運用，讓有限的頻寬資源發揮最大的效用。
7	進行防火牆設定，預防攻擊及不當存取網路資源	攻擊阻擋、訪問規則及網頁存取限制	當內網用戶使用 BT 影響其他人上網、員工上班時間不正當上網以及使用 MSN、QQ、Skype 影響工作效率；當網路速度因被駭客攻擊而受影響或內網用戶常被蠕蟲及 ARP 攻擊所苦;網管可依據需求設定內外網路存取規則，以進一步管控員工個別上網行為。
8	進階功能設定：虛擬伺服器、UPnP、DDNS、MAC Clone	針對內部設定虛擬伺服器、UPnP、路由模式、多廣域網 IP、DDNS、Mac Clone	進階功能設定完成對網路的更進一步要求，構建內部虛擬伺服器，UPnP 通訊協定的設定，設定動態路由或者靜態路由，一對一 NAT 設定，動態網域名稱解析服務 DDNS 與 Mac 位址 Clone。
9	管理維護的設定：系統日誌、SNMP、及設定參數備份	VPN 防火牆工作情況監測、系統參數的備份	網管可藉此功能查看系統日誌、即時監控系統狀態及內外流量，確保內網運作無誤。

10	VPN 虛擬私有網路、QnoKey、QVM VPN 功能設定	針對 VPN 連線功能進行設定，包括 PPTP、QnoKey 與 QVM VPN	藉由多種而簡便的 VPN 設定，使各類的 VPN 虛擬私有網應用環境，能有效並順利地運作
11	登出設定視窗	離開設定視窗	登出退出 VPN 防火牆 Web 管理頁面。

下面我們就根據這個流程來設定完成我們的網路設定。

三、硬體安裝

本章介紹產品的硬體介面以及實體安裝。

3.1 VPN 防火牆 LED 顯示燈

LED 燈號說明

LED	顏色	意義
Power-電源	綠燈	綠燈亮： 電源開啟連接
DIAG-自我測試	橘燈	橘燈亮： 系統尚未完成開機自我檢測功能。 橘燈熄滅： 系統已經正常完成開機自我檢測功能。
Link/Act-連線/動作 （埠口右側綠燈）	綠燈	綠燈亮： 乙太網路連線正常 綠燈閃爍： 乙太網路埠正在傳送/接收封包資料傳輸
100M-速度 （埠口左側橘黃燈）	橘燈	橘燈亮： 乙太網路連線在 100Mbps 的速度 橘燈熄滅： 乙太網路連線在 10Mbps 的速度
Connect-網際網路	綠燈	綠燈亮： 廣域網埠已經連線並取得 IP 位址

硬體恢復（Reset）按鍵

動作	意義
點選 Reset 按鈕 5 秒	熱開機，重新啟用 VPN 防火牆 DIAG 燈號： 橘色燈號慢慢閃爍
點選 Reset 按鈕 10 秒以上	恢復原出廠預設值 DIAG 燈號： 橘色燈號快閃

系統內建電池

VPN 防火牆內建有系統時間的電池，此電池的壽命約為 1～2 年，當電池已經無法充電或是使用壽命到達後，VPN 防火牆將無法記錄時間或是連接網際網路同步 NTP 時間伺服器。您必須與您的供應商聯繫，以便取得更換電池技術。

注意！

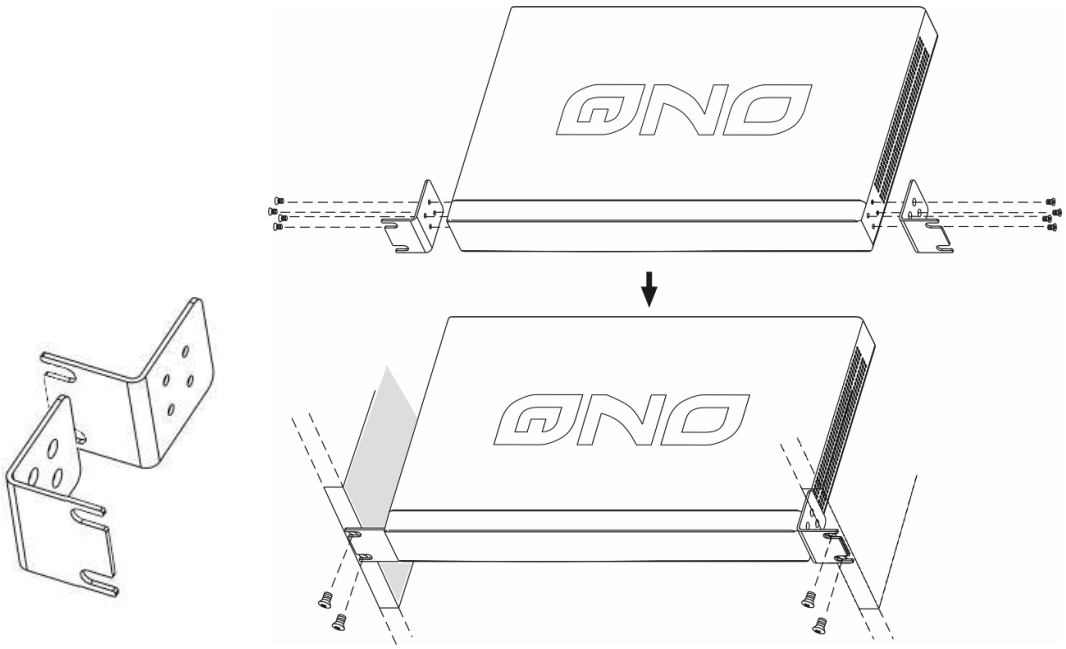
為了產品的正常運行，請勿自行更換電池，以免造成產品無法恢復的損壞！

將 VPN 防火牆安裝在 19”標準機架上

建議您可以將 VPN 防火牆放置於桌上使用，或是您有機房專用 19 吋標準機架的話，可以將 VPN 防火牆安裝於機架上，每一台 VPN 防火牆都有配備專用連接機架配件。當您安裝 VPN 防火牆於機架上的時候，請注

意不要將其他過重的物品堆疊或是放置於機器上，以免因重量過重無法承受而發生危險或是損傷機器本體。

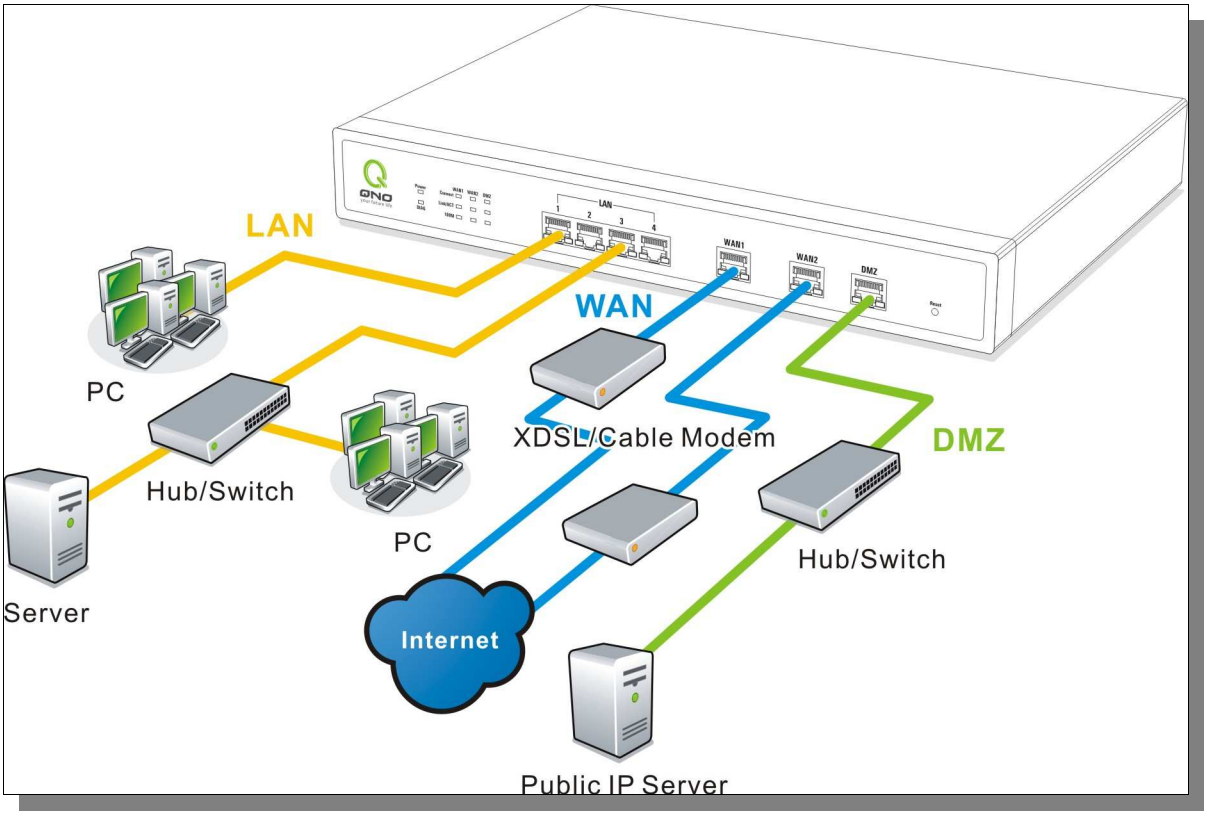
每一台 VPN 防火牆都有配備專用連接機架配件，包含 2 只 L 型鎖附架以及八顆專用螺絲，用來將 VPN 防火牆安裝在機架上使用。安裝於您的 19 吋標準機架上的方法如下圖所示：



注意！

為了產品的穩定運行，無論您是如何放置 VPN 防火牆，請不要阻塞產品兩側通風口的任何一側，並保持通風口有 10mm 以上的通風空間！

3.2 VPN 防火牆的網路連接



廣域網路連線：連接 xDSL Modem 或光纖轉換器來連通網際網路。或是連接交換機或外部路由器、防火牆來連通您現有的網路。

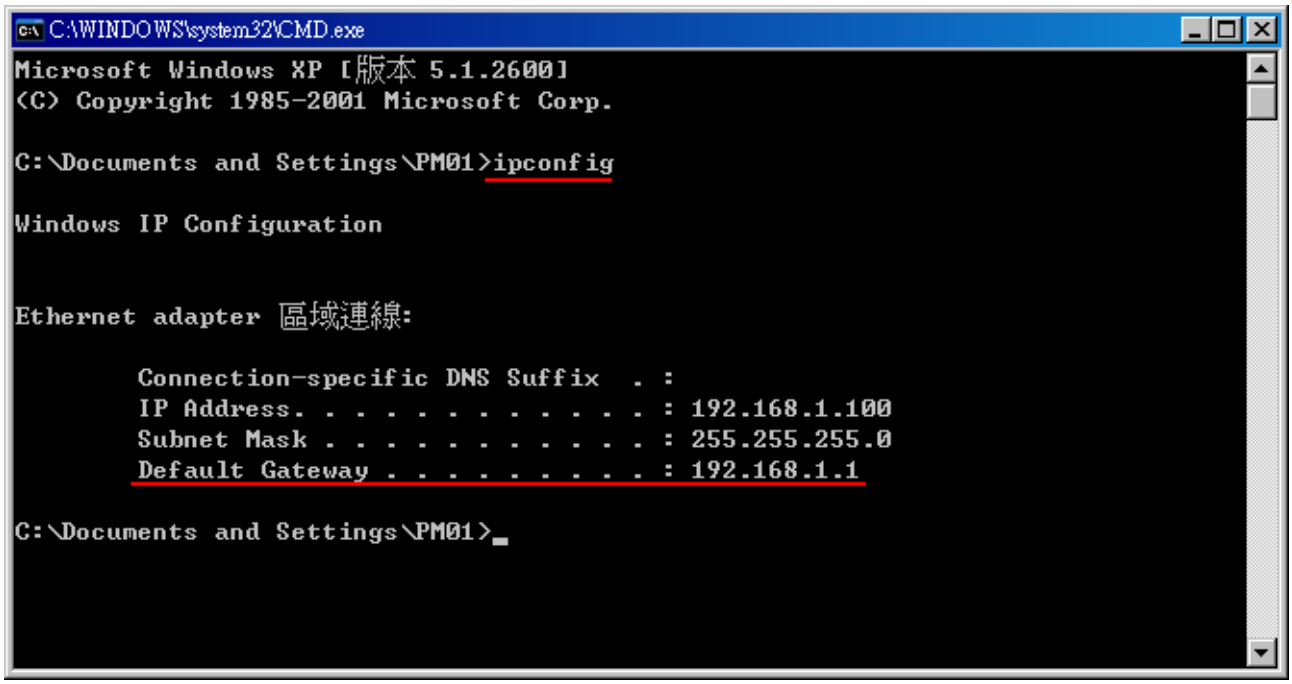
區域網路連線：連接交換機或電腦。若區域網埠口有支援鏡像功能，請在“實體埠口管理”中做設定，設定完成即可直接將監控或過濾伺服器接在此埠口使用

DMZ：此埠口可以連接如 Switch HUB 或是具有外部合法 IP 位址的伺服器，如網頁伺服器以及電子郵件伺服器等。

四、登錄 VPN 防火牆

本章主要是在客戶連接好 VPN 防火牆後，通過連接 VPN 防火牆的電腦登錄 VPN 防火牆的 Web 管理頁。

首先在連接到 VPN 防火牆 LAN 端的電腦（確定電腦是自動獲得 IP 位址）上的 DOS 下查詢 VPN 防火牆的 IP 位址，點開始→執行，輸入 cmd 進入 DOS 操作，再輸入 ipconfig→確認，查到預設閘道（Default Gateway）位址如圖，192.168.1.1。確認預設閘道也就是 VPN 防火牆的預設 IP 位址。



注意！

當 "ipconfig" 不能獲得 IP 位址以及預設閘道的情況，或者獲得的 IP 位址為 0.0.0.0 以及 169.X.X.X 的情況，就是 VPN 防火牆並沒有分配到 IP 位址，建議用戶檢查線路是否有問題，電腦網卡是否接好等。

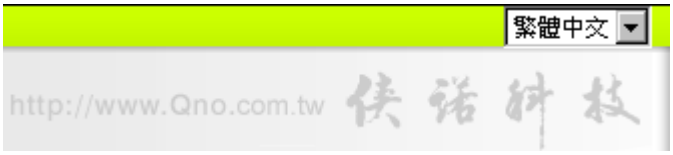
然後開啟網頁流覽器 (如 IE)，在網址欄輸入 192.168.1.1 (VPN 防火牆的預設閘道)，會出現以下的登錄視窗：

VPN 防火牆預設的使用者名稱與使用者密碼皆為"admin"，您可以於稍後設定時更改此登錄密碼。

注意！

為了安全，我們強烈建議您務必在登錄之後更改管理密碼！密碼請牢記，若是密碼忘記，將無法再登錄至 VPN 防火牆的設定視窗，必須點選面板上的 Reset 按鍵十秒以上，恢復到出廠值，其所有設定將需要重新設定。

登錄後，就會顯示 VPN 防火牆的 Web 管理頁面，在其頁面的右上角選擇 VPN 防火牆操作的語言模式，選中的圖示將變成藍色，這裏選擇"繁體"（繁體中文版本），如圖。



五、確定設備規格、狀態顯示以及登錄密碼和時間的設定

本章介紹登錄軟體設定視窗後進入首頁可以瞭解到的設備規格以及設備工作狀態資訊，還有因安全考慮需要用戶即時修改登錄密碼與系統時間設定。

5.1 首頁顯示

首頁顯示 VPN 防火牆目前系統所有參數以及狀態顯示資訊。

5.1.1 廣域網狀態

廣域網狀態

接口位置	廣域網1	廣域網2	廣域網3	廣域網4
IP 位址	0.0.0.0	192.168.3.133	0.0.0.0	0.0.0.0
預設閘道	0.0.0.0	192.168.3.1	0.0.0.0	0.0.0.0
DNS 伺服器	0.0.0.0	192.168.3.10 192.168.3.2	0.0.0.0	0.0.0.0
連線數	0	58	0	0
下載頻寬使用率(%)	0	0	0	0
上傳頻寬使用率(%)	0	0	0	0
動態網域解析服務	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled
QoS頻寬管理	0 條規則	0 條規則	0 條規則	0 條規則
手動連線	釋放 更新	釋放 更新	釋放 更新	釋放 更新

IP 位址： 此為顯示 VPN 防火牆 WAN 端目前的 IP 位址資訊。

預設閘道： 此為顯示 ISP 分配給 VPN 防火牆 WAN 的閘道 IP 位址資訊。

DNS 伺服器： 此為顯示 VPN 防火牆的 DNS 的 IP 位址資訊。

連線數： 此為顯示 VPN 防火牆每個 WAN 目前的連線數目。

下載頻寬使用率： 此為顯示 VPN 防火牆每個 WAN 目前的下載頻寬使用比例。

上傳頻寬使用率： 此為顯示 VPN 防火牆每個 WAN 目前的上傳頻寬使用比例。

動態網域解析服務： 此為顯示 VPN 防火牆的 DDNS 是否啟用的狀態資訊。系統預設此功能為關閉。

QoS 頻寬管理： 此為顯示 VPN 防火牆的網路品質服務(QoS)是否開啟。

手動連線： 當使用者選擇自動取得 IP 位址時，他會顯示二個按鈕分別為釋放與更新。
使用者可以點選釋放按鈕去做釋放 ISP 端所核發的 IP 位址，以及點選更新按鈕去做更新 ISP 端所核發的 IP 位址。

當選擇 WAN 端連線使用如 PPPoE 或是 PPTP 的話，它會變為顯示"連線"與"中斷"。

DMZ IP 位址：　此為顯示 VPN 防火牆 DMZ 目前的 IP 位址設定資訊。

5.1.2 實體埠口設定狀態顯示

實體埠口配置狀態

埠口號	1	2	3	4	5	Internet	Internet	Internet	Internet/DMZ
接口位置	區域網					廣域網1	廣域網2	廣域網3	廣域網4
狀態	連線	連線	啓用	啓用	啓用	啓用	連線	啓用	啓用

此視窗會顯示系統各埠口目前即時狀態：(連線-已經連線，啟用-此埠口處於開啟狀態，關閉-此埠口處於關閉狀態)。您可以點選此狀態按鈕，在彈出的視窗中查看各埠口更詳細的資料顯示。如下圖：

此表會顯示目前該埠設定狀態，如網路連接狀態(10Base-T/100Base-TX/1000Base-T)，接口位置(廣

域網／區域網/DMZ)，線路連線狀態(Up 啟用/Down 關閉)，埠設定狀態(Port Enabled 埠啟用/Port Disabled 埠關閉)，優先順序設定(High 高級/Normal 一般)，網路連接速率(10Mbps/100Mbps/1000Mbps)，工作模式(Half 半雙工/Full 全雙工)，自動偵測功能(Enabled 啟用/Disabled 關閉)。於此表格中，會顯示此埠口的接收和傳送的資料封包以及資料封包傳送 Byte 數及資料封包錯誤率等並計算總數量。

5.1.3 系統資訊

系統訊息

閘道位址/子網路遮罩	192.168.250.1/255.255.255.0	主機序號	
工作模式	NAT模式	韌體版本	
運作時間	0 Days 2 Hours 1 Minutes 44 Seconds	系統時間	Fri Aug 8 2008 12:10:06

區域網閘道位址：此為顯示 VPN 防火牆本身的 LAN 端目前 IP 位址，系統預設為 192.168.1.1。

工作模式： 此為顯示 VPN 防火牆的目前工作模式 (可為 NAT 模式或是路由模式)。

系統預設此功能為 NAT 模式。

運作時間：此為顯示 VPN 防火牆目前已經開機的時間。

主機序號：此為顯示 VPN 防火牆的產品序號。

韌體版本： 此為顯示 VPN 防火牆目前使用的韌體版本。

系統時間：此顯示 VPN 防火牆目前正確時間，但必須注意，您需要正確設定與遠端 NTP 伺服器的時間同步後才會正確顯示。

5.1.4 防火牆狀態

防火牆狀態

防火牆	狀態
SPI封包偵測	開啓
DoS防禦功能	開啓
關閉廣域網回應功能	開啓
防止ARP病毒攻擊	關閉
遠端管理功能	關閉
存取規則設定	5 條規則

SPI 封包偵測：此為顯示 VPN 防火牆的 SPI 主動封包偵測過濾功能選項是否啟用(開啟/關閉)。系統預設此功能為開啟。

DoS 防禦功能：此為顯示 VPN 防火牆的阻斷來自網路上的 DoS 攻擊功能選項是否開啟(開啟/關閉)。系統預設此功能為開啟。

關閉廣域網回應功能：此為顯示 VPN 防火牆的阻斷來自網路上的 ICMP-Ping 的回應功能選項是否啟用(開啟/關閉)。系統預設此功能為開啟。

防止 ARP 病毒攻擊：此為顯示 VPN 防火牆防止 ARP 攻擊的功能選項是否啟用(啟用/關閉)。系統預設此功能為關閉。

遠端管理功能：此為顯示 VPN 防火牆的遠端管理功能選項是否啟用(啟用/關閉)。系統預設此功能為關閉。

存取規則設定：此為顯示 VPN 防火牆的存取規則設定的數目。

5.1.5 VPN 虛擬私有網狀態

VPN配置狀態

VPN設置	狀態
已使用的隧道數目	0
可使用的隧道數目	150
PPTP伺服器	Disabled

VPN 設定狀態： 此為顯示 VPN 防火牆的 VPN 功能選項內容資訊。

已使用的隧道數目：此為顯示 VPN 防火牆的 VPN 功能目前已經設定的隧道數量。

可使用的隧道數目：此為顯示 VPN 防火牆的 VPN 功能目前可使用的隧道數量。

PPTP 伺服器：顯示 PPTP 伺服器是否開啟。

5.1.6 系統日誌設定狀態顯示

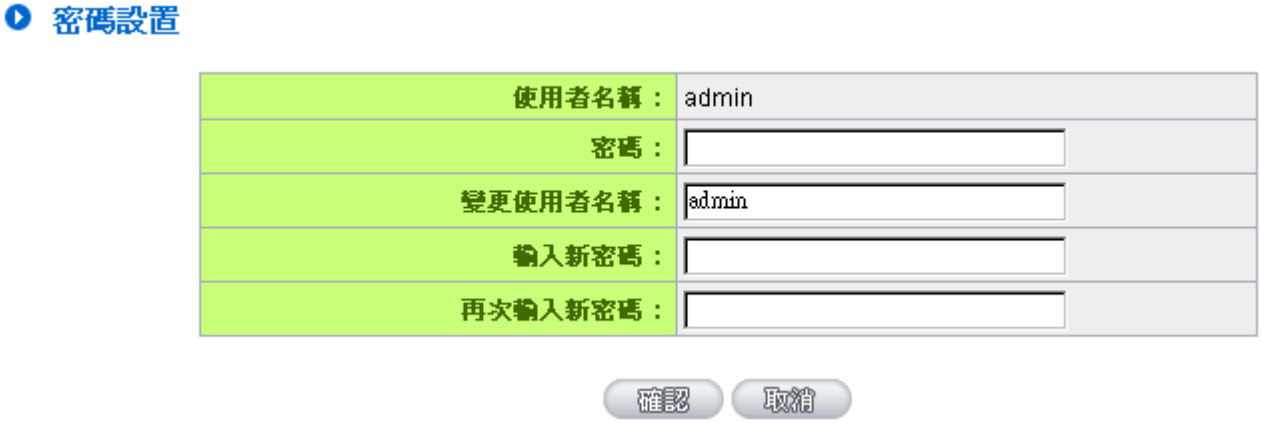
日誌伺服器： 此為顯示您所設定 VPN 防火牆的日誌記錄接收的伺服器。

E-mail 警示功能： 此為顯示您所設定的 E-mail 位址，VPN 防火牆的日誌記錄經由此 E-mail 傳送出去。

5.2 登錄密碼及時間的修改和設定

5.2.1 密碼設定

當您每次登錄 VPN 防火牆的設定視窗時，必須輸入密碼。VPN 防火牆的用戶名和密碼出廠值均為"admin"。考慮安全因素，我們強烈建議您務必在第一次登錄並完成設定之後更改管理密碼！密碼請牢記，若是密碼忘記，將無法再登錄 VPN 防火牆的設定窗口，必須點選 VPN 防火牆前面板上的 Reset 按鍵十秒以上，恢復到出廠值，所有設定值將需要重新設定。



使用者名稱：	出廠初始值預設為 admin。
密碼：	填寫原本舊密碼（出廠初始值預設為"admin"）。
變更使用者名稱：	輸入新用戶名，如 Qno。
輸入新密碼：	填寫要更改的新密碼。
再次輸入新密碼：	再次填寫更改的新密碼以確認。
確定：	點選此按鈕"確定"儲存剛才所修改設定的內容參數。

取消： 點選此按鈕"取消"清除剛才所修改設定的內容參數，此操作必須於"確定" 儲存動作之前才會有效。

5.2.2 系統時間設定

VPN 防火牆可以設定時間，讓您在查看 VPN 防火牆的系統紀錄或設定網路存取的時間設定時，可以瞭解事件發生的正確時間，以及作為關閉存取或是開放存取網路資源的依據條件。您可以選擇與 VPN 防火牆內建的外部時間伺服器(NTP 伺服器)取得時間同步，或自己設定正確時間參數。

與外部時間伺服器同步：VPN 防火牆有內建的網路時間伺服器，會自動同步時間。

選擇時區： 點開下拉功能表選擇您所在地點的時區以正確顯示當地時間。

日光節約時間： 若是您所的地區有實施日光節約時間，可以輸入實施的日期範圍，VPN 防火牆會在此日期範圍自動調整時間。

外部時間伺服器（NTP）位址： 若是您自己有偏愛使用的時間伺服器，可以輸入該伺服器的位址。

確定： 點選此按鈕即會儲存剛才所變動的修改設定內容參數。

取消： 點選此按鈕即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

手動設定時間： 在這輸入正確的時間：小時、分鐘、秒、月份、日與年份。

點選"確認"按鈕即會儲存剛才所修改的設定內容參數，點選按鈕"取消"即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

六、進行廣域網路連線設定

本章節講述基本的廣域網路設定，對大多數的用戶來說，通過本章節完成基本的設定已經足夠連接網路。網路的連接需要一些 ISP 所提供的進一步詳細資訊。其詳細項目設定，請參考以下各節說明：

6.1 網路設定

6.1.1 主機名稱及網域名稱

可輸入 VPN 防火牆的名稱（主機名稱）以及網域名稱，此設定在大多數環境中不需要做任何設定即可使用，除非特殊 ISP 需求！

6.1.2 區域網（LAN）介面設定

此為設定 VPN 防火牆的 LAN 端內部網路的 IP 位址，系統預設為 192.168.1.1，子網路遮罩為 255.255.255.0，您可以依照實際網路架構做變動。

Multiple-Subnet 多重網段設定：

點選“新增/編輯”按鈕彈出多重網段設定的設定視窗。

此功能是將不同於 VPN 防火牆區域網段的其他網段 IP 加入到 VPN 防火牆認可的區域網段中，這樣區域網中的 PC 若是已經設定的 IP 所在的網段不同於 VPN 防火牆的區域網段也可以直接上網。舉例來說，原來內部環境已經有多組不同的 IP 網段，例如 192.168.3.0， 192.168.20.0， 192.168.150.0 等等，將這些網段加入到子網中，則這些網段的內部電腦不需做任何修改就可以上網，這裏可以依照您的實際網路架構運作。

6.1.3 廣域網路 WAN 及非軍事區設定

廣域網網路連接型態設定：

廣域網路設定

接口位置	連線類型	配置
廣域網1	Obtain an IP automatically	編輯
廣域網2	Obtain an IP automatically	編輯
廣域網3	Obtain an IP automatically	編輯
廣域網4	Obtain an IP automatically	編輯

接口位置：廣域網連線所在 WAN 接口位置。

線路連接類型狀態：此項顯示該廣域網埠口目前設定的連線狀態。VPN 防火牆提供五種連線狀態設定：自

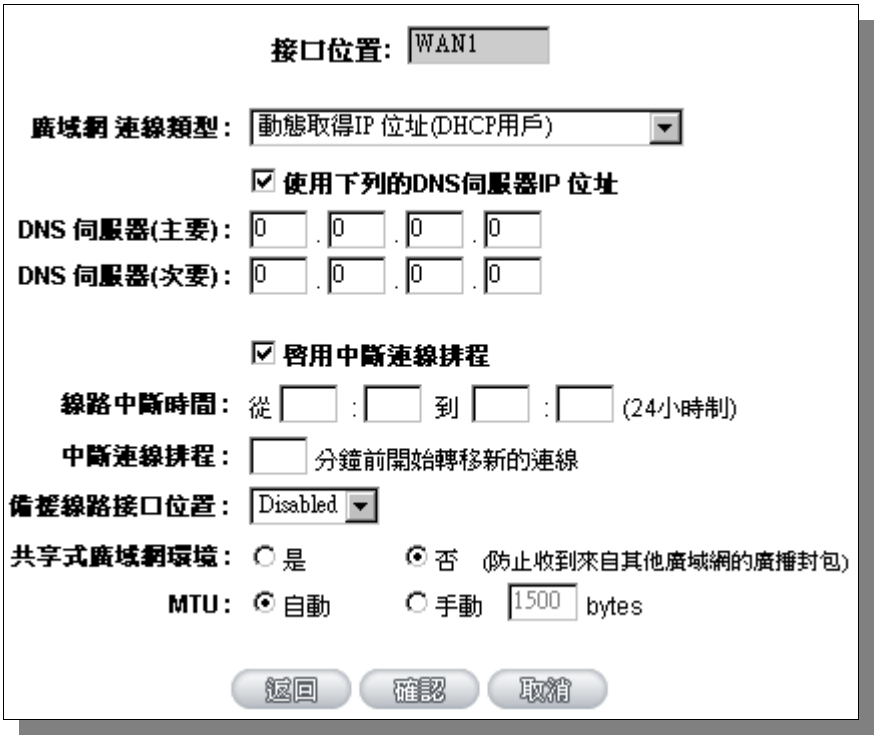
動取得 IP 位址；固定 IP 位址；PPPoE 撥號連線；PPTP 撥號連線以及透通橋接模式。

設定：點選"編輯"按鈕可以進入廣域網連線狀態的設定視窗。各類型的連線狀態設定請參考以下的說明，並選擇配合 ISP 所給您的連線狀態來做設定。

動態取得 IP 位址 (DHCP 用戶)：

此為 VPN 防火牆系統預設的連線方式，此連線方式為 DHCP 用戶端自動取得 IP 模式，多為應用於如線纜數據機或是 DHCP 用戶端連線狀態等連接，若您的連線為其他不同的方式，請選取相關的設定並參考以下的介紹做設定。

在動態取得 IP 模式，您可以使用自定 DNS 的 IP 位址，勾選此選項並填入您要使用的 DNS 伺服器 IP 位址。



使用以下的 DNS 伺服器 IP 位址： 選擇使用自定的 DNS 伺服器 IP 位址。

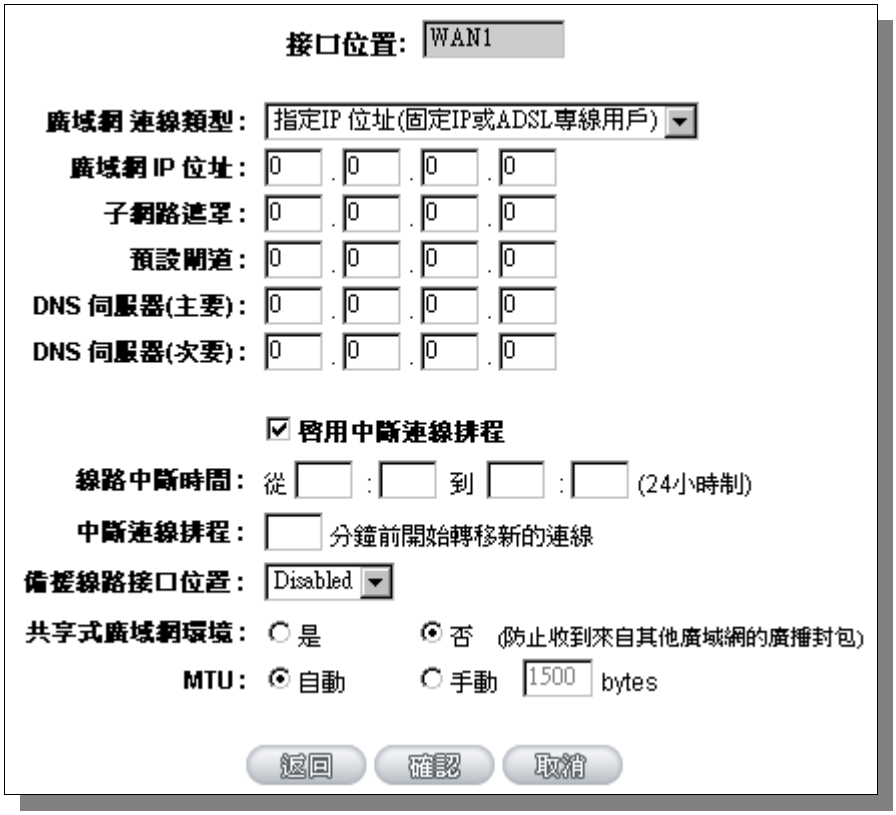
DNS 伺服器： 輸入您的 ISP 所提供的 DNS 伺服器 IP 位址，最少填入一組，最多可填二組。

啟用中斷連線排程：	勾選此功能會啟用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然 VPN 防火牆有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，為了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啟用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
線路中斷時間：	輸入此廣域網中斷連接服務的規則時間。
中斷連線排程：	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
備援線路接口位置：	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。
共用式廣域網環境：	若您的廣域網線路有連接至交換機(Switch)，可以點選「是」將此功能開啟，來屏避掉不需要的廣播封包，增加您網路使用的效能與安全性，預設值「否」則是將此功能關閉。
MTU：	MTU 為 Maximum Transmission Unit 的縮寫，可選自動或手動來控制，一般預設為 1500。 但是在不同的網路環境中，可能會使用不同的數值。尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU 值：1492)。一般使用預設 Auto 即可，不需做任何調整。

點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數，點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

指定 IP 位址（固定 IP 或 ADSL 專線用戶）:

若您的 ISP 有核發固定的 IP 位址給您(如 1 個 IP 或是 8 個 IP 等)，請您選擇此種方式連線，將 ISP 所核發的 IP 資訊分別參照以下介紹填入相關設定參數中。



廣域網 IP 位址：　輸入您的 ISP 所核發的可使用固定 IP 位址的其中一個。

子網路遮罩：　輸入您的 ISP 所核發的可使用固定 IP 位址的子網路遮罩，如：

發放 8 個固定 IP 位址：255.255.255.248

發放 16 個固定 IP 位址：255.255.255.240

預設閘道：　輸入您的 ISP 所核發的可使用固定 IP 位址的預設閘道，若您是使用 ADSL 的話，一般說來都是 ATU-R 的 IP 位址。

DNS 伺服器：　輸入您的 ISP 所規定的 DNS 伺服器 IP 位址，最少填入一組，最多可填二組。

啟用中斷連線排程：　勾選此功能會啟用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然 VPN 防火牆有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，為了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啟用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。

線路中斷時間：　輸入此廣域網中斷連接服務的規則時間。

中斷連線排程：　輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。

備援線路接口位置： 若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。

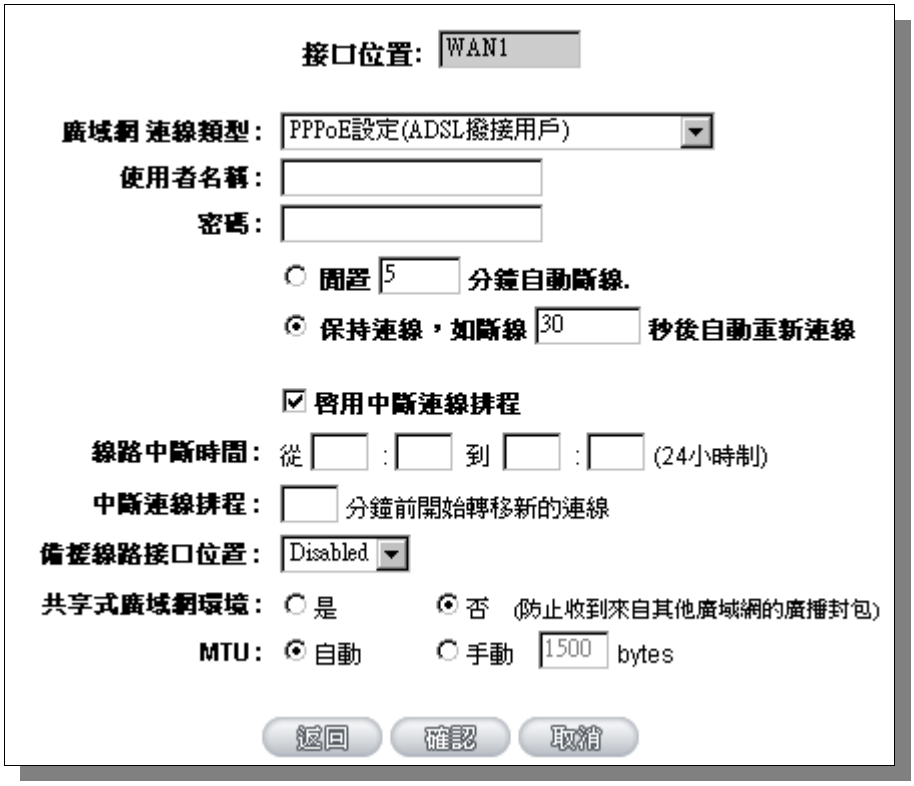
共用式廣域網環境： 若您的廣域網線路有連接至交換機(Switch)，可以點選「是」將此功能開啟，來屏避掉不需要的廣播封包，增加您網路使用的效能與安全性，預設值「否」則是將此功能關閉。

MTU： MTU 為 Maximum Transmission Unit 的縮寫，可選自動或手動來控制，一般預設為 1500。 但是在不同的網路環境中，可能會使用不同的數值。尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU 值：1492)。一般使用預設 Auto 即可，不需做任何調整。

點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數，點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

PPPoE 撥號連線：

此項為 ADSL 虛擬撥號使用(適用於 ADSL PPPoE)，填入 ISP 給予的使用者連線名稱與密碼並以 VPN 防火牆內建的 PPP Over Ethernet 軟體連線，若是您的 PC 之前已經有安裝由 ISP 所給予的 PPPoE 撥號軟體的話，請將其移除，不需要再使用此個別連接網路。



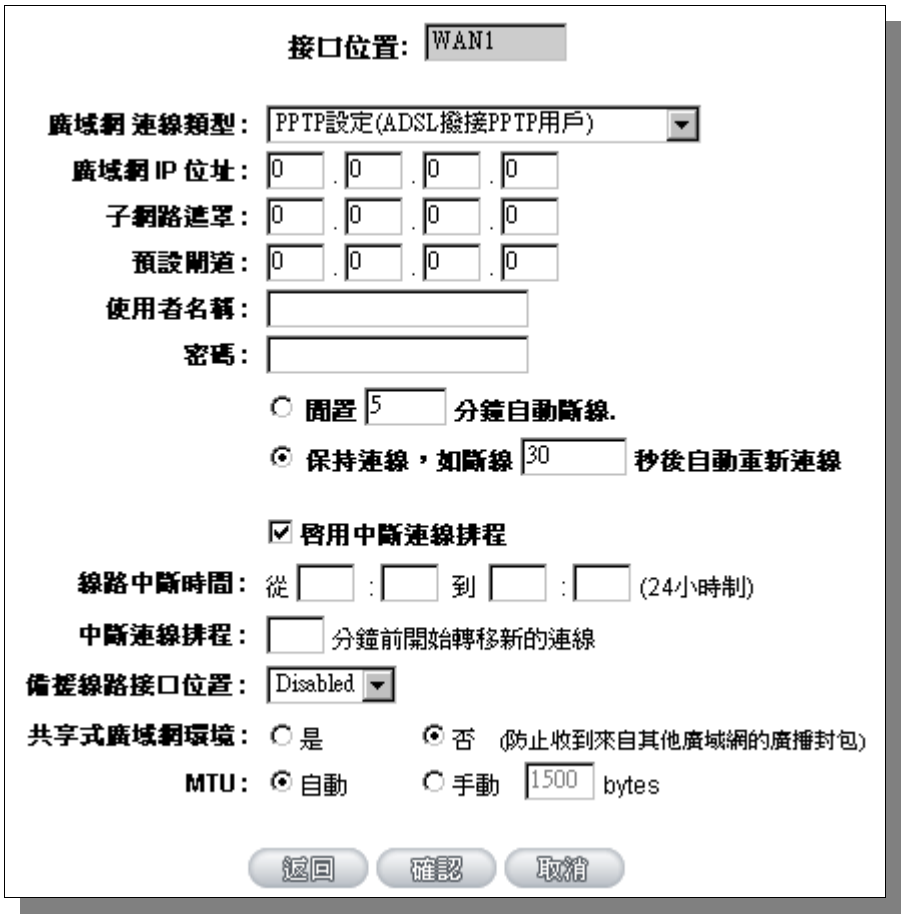
使用者名稱： 輸入您的 ISP 所核發的使用者名稱。

密碼：	輸入您的 ISP 所核發的使用密碼。
閒置( )分鐘自動斷線：	此功能能夠讓您的 PPPoE 撥接連線能夠使用自動撥號功能，當使用端若是有上網需求時，VPN 防火牆 會自動向預設的 ISP 自動撥號連線，當網路一段時間閒置無使用時，則系統會自動離線。您可以自行輸入所需要的無數據包傳送自動離線等待時間，預設為 5 分鐘。
保持連線：	此功能能夠讓您的 PPPoE 撥接連線能夠斷線自動重撥，您可以自行設定重新撥接的時間，預設值為 30 秒。
啟用中斷連線排程：	勾選此功能會啟用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然 VPN 防火牆有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，為了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啟用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
線路中斷時間：	輸入此廣域網中斷連接服務的規則時間。
中斷連線排程：	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
備援線路接口位置：	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。
共用式廣域網環境：	若您的廣域網線路有連接至交換機(Switch)，可以點選「是」將此功能開啟，來屏避掉不需要的廣播封包，增加您網路使用的效能與安全性，預設值「否」則是將此功能關閉。
MTU：	MTU 為 Maximum Transmission Unit 的縮寫，可選自動或手動來控制，一般預設為 1500。 但是在不同的網路環境中，可能會使用不同的數值。尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU 值：1492)。一般使用預設 Auto 即可，不需做任何調整。

點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數，點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

PPTP 撥號連線：

此項為 PPTP (Point to Point Tunneling Protocol) 計時制使用，填入 ISP 給予的使用者連線名稱與密碼並以 VPN 防火牆內建的 PPTP 軟體連線。



廣域網 IP 位址： 輸入您的 ISP 所核發的可使用固定 IP 位址的其中一個。

子網路遮罩： 輸入您的 ISP 所核發的可使用固定 IP 位址的子網路遮罩。

預設閘道： 輸入您的 ISP 所核發的可使用固定 IP 位址的預設閘道，若您是使用 ADSL 的話，一般說來都是 ATU-R 的 IP 位址。

使用者名稱： 輸入您的 ISP 所核發的使用者名稱。

密碼： 輸入您的 ISP 所核發的使用密碼。

閒置( )分鐘自動斷線： 此功能能夠讓您的 PPTP 撥接連線能夠使用自動撥號功能，當使用端若是有上網需求時，VPN 防火牆會自動向預設的 ISP 自動撥號連線，當網路一段時間閒置無使用時，則系統會自動離線。無封包傳送的自動離線時間預設為 5 分鐘，您可以自行輸入所需要的自動離線等待時間。

保持連線： 此功能能夠讓您的 PPTP 撥接連線能夠斷線自動重撥，而且可以自行設定重新撥接的時間，預設值為 30 秒。

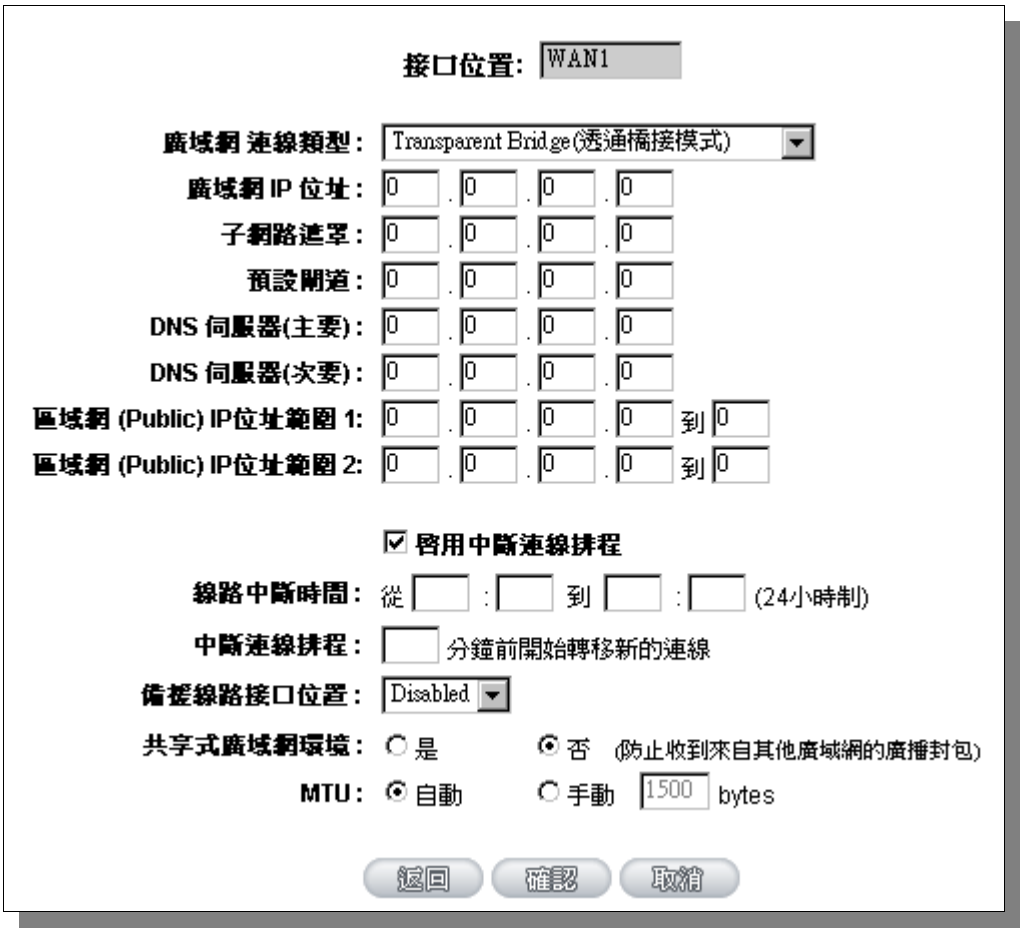
啟用中斷連線排程：	勾選此功能會啟用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然 VPN 防火牆有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，為了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啟用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
線路中斷時間：	輸入此廣域網中斷連接服務的規則時間。
中斷連線排程：	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
備援線路接口位置：	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。
共用式廣域網環境：	若您的廣域網線路有連接至交換機(Switch)，可以點選「是」將此功能開啟，來屏避掉不需要的廣播封包，增加您網路使用的效能與安全性，預設值「否」則是將此功能關閉。
MTU：	MTU 為 Maximum Transmission Unit 的縮寫，可選自動或手動來控制，一般預設為 1500。 但是在不同的網路環境中，可能會使用不同的數值。尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU 值：1492)。一般使用預設 Auto 即可，不需做任何調整。

點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數，點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

透通橋接模式（Transparent Bridge）:

當您內網的電腦 IP 已經都是 Public IP 而不希望將內網都改成 Private IP (例如 192.168.1.X)時，此功能可以讓您不需更動原有架構，立即整合到既有網路中。選擇廣域網連線方式為透通橋接模式，這樣您可以保留內網電腦的 IP 設定為原本的 Public IP 仍然可以正常上網。

當您設定兩個廣域網時，廣域網的連線模式選擇此種透通橋接模式，還是可以做到負載平衡。



廣域網 IP 位址： 輸入您的 ISP 所核發的可使用固定 IP 位址的其中一個。

子網路遮罩： 輸入您的 ISP 所核發的可使用固定 IP 位址的子網路遮罩，如：255.255.255.240

預設閘道： 輸入您的 ISP 所核發的可使用固定 IP 位址的預設閘道，若您是使用 ADSL 的話，一般說來都是 ATU-R 的 IP 位址。

DNS 伺服器： 輸入您的 ISP 所規定的 DNS 伺服器 IP 位址，最少填入一組，最多可填二組。

區域網(Public)IP 位址範圍： 輸入您的 ISP 所核發的可使用固定 IP 範圍。若是您的 ISP 分給您兩個不連續的 IP 位址範圍，您可以分別填入。

啟用中斷連線排程：	勾選此功能會啟用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然 VPN 防火牆有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，為了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啟用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
線路中斷時間：	輸入此廣域網中斷連接服務的規則時間。
中斷連線排程：	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
備援線路接口位置：	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。
共用式廣域網環境：	若您的廣域網線路有連接至交換機(Switch)，可以點選「是」將此功能開啟，來屏避掉不需要的廣播封包，增加您網路使用的效能與安全性，預設值「否」則是將此功能關閉。
MTU：	MTU 為 Maximum Transmission Unit 的縮寫，可選自動或手動來控制，一般預設為 1500。 但是在不同的網路環境中，可能會使用不同的數值。尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU 值：1492)。一般使用預設 Auto 即可，不需做任何調整。

點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數，點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

非軍事區(DMZ)：

對於某些網路環境應用來說，可能會需要用到獨立的 DMZ 非軍事管制區介面來置放對外服務伺服器，如 WWW 網頁伺服器與 Mail 電子郵件伺服器等等。VPN 防火牆提供您獨立的 DMZ 介面來設定連接有合法 IP 位址的伺服器。此 DMZ 介面是從網路或區域網存取對外伺服器內容的溝通橋樑。

IP 位址：此項顯示您給予 DMZ 埠的 IP 位址或範圍。

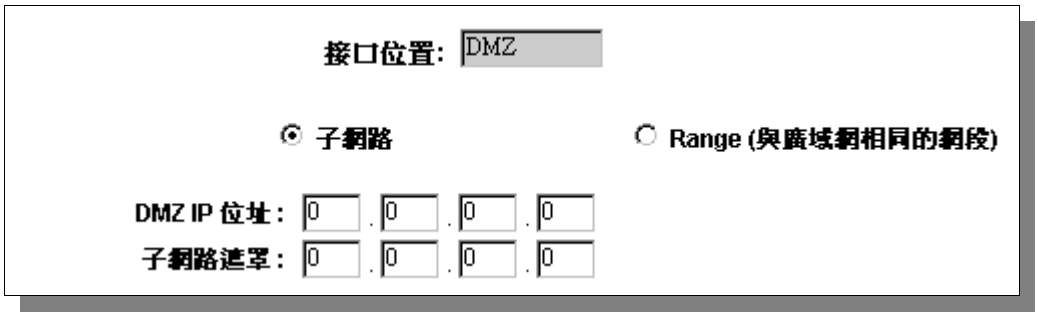
設定：點選"編輯"按鈕可以進入 DMZ 的設定視窗。請參考以下的設定說明。

此 DMZ 的設定可分為 Subnet 及 Range 兩種：

Subnet（子網路）：

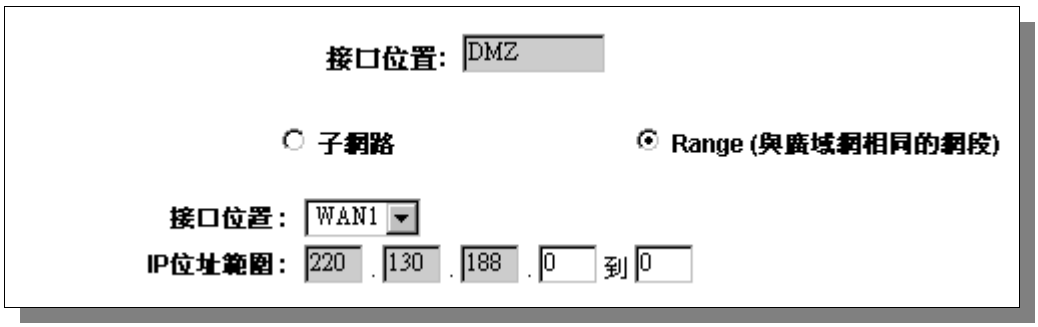
DMZ 與廣域網路 WAN 要在不同的子網路 Subnet 中。

就是若 ISP 端分配給您 16 個合法 IP 如：220.243.230.1-16/子網路遮罩：255.255.255.240 時，您必須將此 16 個 IP 再切兩組變成 220.243.230.1-8 /子網路遮罩：255.255.255.248 及另一組 220.243.230.9-16/子網路遮罩：255.255.255.248，然後 VPN 防火牆及閘道是在同一組，再將另一組設定在 DMZ 中。



Range (與廣域網相同的網段)：

DMZ 與廣域網路 WAN IP 位址在相同的子網路 Subnet。



IP 位址範圍： 輸入在 DMZ 埠的 IP 範圍。

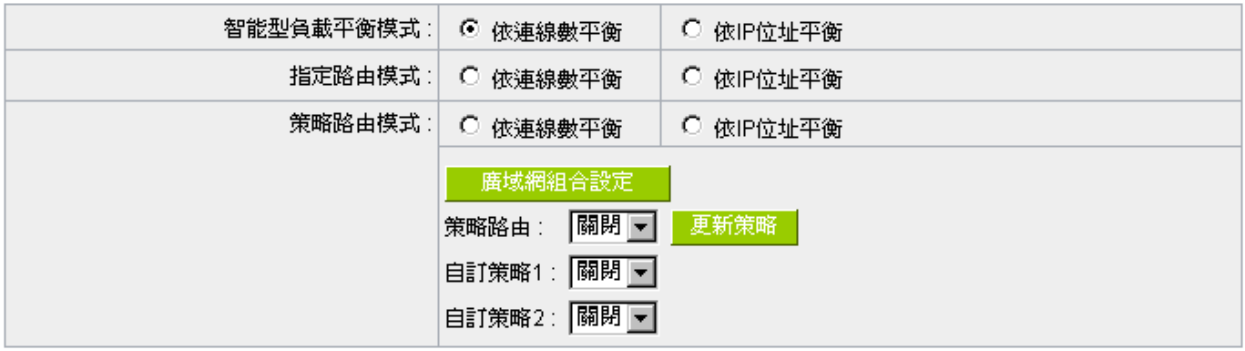
點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數，點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

6.2 多 WAN 設定

當用戶的連線是採用多 WAN 的線路設計，管理人員可以進入基本功能設定的負載平衡設定與協議綁定，對 VPN 防火牆的負載平衡模式等進行設定，使 VPN 防火牆達到最優資料轉發是網路頻寬效能達到最高。

6.2.1 負載平衡模式

模式



智能型負載平衡模式：

當您選用智能型負載平衡模式，VPN 防火牆將以連線數或是 IP 位址連線數為基礎，並依據您廣域網線路的頻寬來自動分配連線，達到對外連線的負載平衡。線路的頻寬是依據您所填入的頻寬設定，例如當兩條廣域網都為上傳 512Kbit/sec 時，其自動負載比例為 1：1，當一條線路的上傳頻寬為 1024kbit/sec 另一條為 512kbit/sec 時，則此自動負載比例為 2：1，所以為了確保您的 VPN 防火牆達到實際線路負載能夠平衡，請填入實際上傳下載頻寬 (請參考下一段 QoS 頻寬管理設定說明)。

依連線數平衡：當您選用連線數平衡模式，VPN 防火牆將以連線數為基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載平衡。

依 IP 位址平衡：當您選用 IP 負載平衡模式，VPN 防火牆將以連線的 IP 數為基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載平衡。

提示！

不論是連線數平衡或是 IP 負載平衡方式，搭配"通訊協議綁定"可以有更彈性運用您的頻寬，您可將特定的內網 IP，使用特定應用通訊埠作訪問，或特定的目的地 IP 經由您指定的廣域網來訪問外網。

譬如您希望指定 IP 192.168.1.100 訪問外網的時候走廣域網 1，或內網所有 IP 去訪問通訊埠 80 時都是經過廣域網 2，或是內網所有 IP 去目的地 IP 211.1.1.1 訪問時要從廣域網 1 去訪問等等，都可

以經由設定此"通訊協議綁定"功能來達到您的需求。請注意，當使智能型負載平衡模式搭配"通訊協議綁定"功能時，除了您指定的訪問會按照您的規則出去訪問外網，其他未被指定的 IP 或通訊埠的訪問還是按照 VPN 防火牆的機制做智能負載平衡。

關於如何設定"通訊協議綁定"功能，以及智能型負載平衡模式搭配"通訊協議綁定"的範例，請參考（6.2.3 節的通訊協定綁定設定說明）。

指定路由模式：

這個模式讓您對特定的內網 IP、特定要訪問的應用通訊埠、或特定目的地 IP 經由您指定的廣域網對外網做訪問。且一經指定後，該廣域網也只能讓這些指定的內網 IP、特定要訪問的應用通訊埠、或特定目的地 IP 使用。其他不在這些指定的內網 IP、特定要訪問的應用通訊埠、或特定目的地 IP 都會從其他的廣域網出去訪問。對於沒有被指定的廣域網，您可以選擇他們的負載平衡模式是以連線數作為負載平衡的基礎，還是以 IP 連線數作為負載平衡的基礎。

未綁定埠平衡模式：若是有部分廣網埠並沒有被指定，例如廣域網 3 與廣域網 4 並沒有指定特定的 IP、通訊埠、或目的 IP 來使用，這些廣域網埠(廣域網 3 與 4)仍然會依據 VPN 防火牆的負載平衡機制來分配連線。平衡機制如下：

依連線數平衡：當您選用連線數平衡模式，VPN 防火牆將以連線數為基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載平衡。

依 IP 位址平衡：當您選用 IP 負載平衡模式，VPN 防火牆將以連線的 IP 數為基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載平衡。

提示！

此指定路由必須配合"通訊協議綁定"功能才能發揮作用。例如指定讓內網去訪問通訊埠 80 時都要從廣域網 1 去訪問，或內網去目的地 IP 211.1.1.1 訪問時要從廣域網 1 去訪問等等，必須要在"通訊協議綁定"功能中做設定。要注意，當使用指定路由模式，以上述的例子來看，除了您指定的訪問必須按照您的規則出去訪問外網都走廣域網 1 以外，其他未被指定的 IP 或通訊埠則經由 VPN 防火牆負載平衡的機制使用其他的廣域網出去。

關於如何設定"通訊協議綁定"功能，以及指定路由模式搭配"通訊協議綁定"的範例，請參考（6.2.3 節的通訊協議綁定設定說明）。

策略路由模式：

當您選用策略路由模式，VPN 防火牆會依照內建的策略(電信網通分流，用在中國的環境)自動分配連線。您只需選擇網通線路接入的廣域網口(或廣域網組合)，VPN 防火牆會自動將該走網通線路去外網訪問的流量都

從網通的廣域網出去，對該走電信線路去外網訪問的流量也都會往電信的廣域網出去，達到"電信走電信，網通走網通"的分流策略。

廣域網組合設定：

當您所接的網通線路不只一條，則需要做廣域網的組合，以便將兩個以上的廣域網口合在一起做相同的策略分流。點選"廣域網組合設定"會彈出以下的對話視窗。

名稱：	在此自定的廣域網組合名稱，如"教育"等，用來辨識廣域網群組。
接口位置：	在此勾選要設在此組合的廣域網口。
加入到對應列表：	增加到廣域網組合列表。
刪除點選的項目：	刪除所選擇的廣域網組合內容。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。
關閉：	關閉並離開此功能設定視窗。

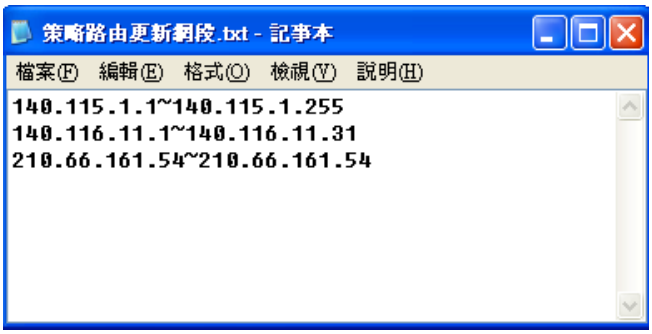
設定完成後，您就可以在網通策略的選擇中選取您的網通介面的廣域網組合。

自定策略：

此外，您也可以自己建立分流策略。在"自定策略"中選擇要指定的廣域網口或廣域網組合(例如廣域網 1)，然後點選"更新策略"的按鍵，會出現匯入策略檔的對話視窗。策略檔是一個可編輯的文字檔案，應含有您指定

的目的 IP 位址。將檔匯入路徑選擇好之後，點選"匯入"，並在設定窗口的最下方點選"確定"，VPN 防火牆就會將要往指定目的 IP 的流量從您指定的廣域網(例如廣域網 1)或廣域網組合出去。

策略檔的建立可以用純文字編輯軟體來撰寫，例如使用 Windows 系統的文字編輯程式"記事本"來建立。將您要指定的目的 IP 位址按照下圖的格式寫入，例如您要指定的目的 IP 位址範圍是從 140.115.1.1 到 140.115.1.255，則在"記事本"中輸入 140.115.1.1～140.115.1.255。下一個目的 IP 位址範圍則要換行輸入。請注意！若是只有一個目的 IP 位址，也需要以同樣的格式來書寫。例如指定的目的 IP 位址是 210.66.161.54，則必須寫成 210.66.161.54～210.66.161.54 格式。儲存檔案後(副檔名應該是.txt)即可匯入自定策略的更新網段。



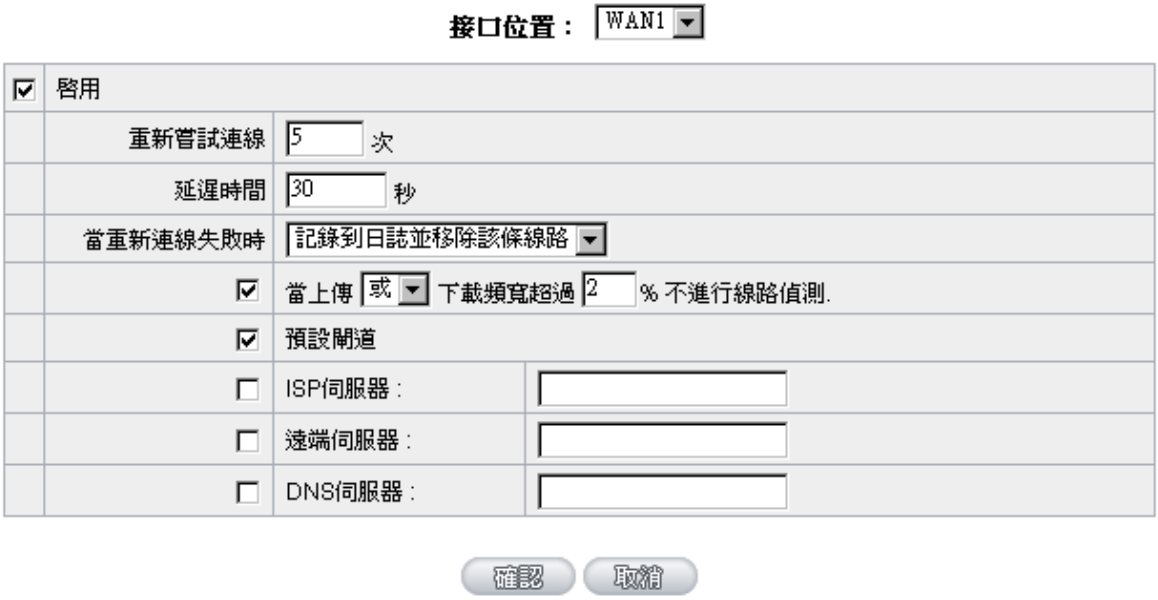
提示！

網通策略與自定策略可以同時存在，但當某一個目的 IP 同時在網通策略以及自定策略中，則會以網通策略優先執行。也就是說要往該目的 IP 的流量會從網通策略的廣域網(或廣域網組合)出去外網。

6.2.2 線路偵測機制

若勾選此項設定，則會顯示出重新發起測試次數，回應延長時間等資訊。當使用兩條廣域網做對外聯結線路時一定將此 NSD 啟用，以避免因為廣域埠流量過大時造成 VPN 防火牆的誤判將此線路判斷為斷線。

線路偵測機制



接口位置：　選擇您要設定線路偵測的廣域網口。

重新嘗試連線：　對外連線偵測重試次數，預設值為五次。如果連線偵測重試次數超過設定次數，網路沒有回應的話，則判斷為對外線路中斷！

延遲時間：　對外連線偵測逾時時間(秒)，預設值為 30 秒。於此設定秒數之後重新測試對外連線。

當重新連線失敗時：　線路連接失敗時的處理方式，有兩種：

（1）僅記錄到日誌：當偵測到與 ISP 連結失敗時，系統就會在系統日誌中將這項錯誤資訊紀錄下來，但保持此線路不會移除，所以會導致有些原來使用此條線路上的用戶無法正常使用。

此選項適用在當某條廣域網連線失敗時，從這個廣域網去訪問的目的地位址是無法從另一條線路去訪問的時候，就可以用此選項。例如若是要訪問 10.0.0.1 到 10.254.254.254 時一定要走廣域網 1 去訪問，而且廣域網 2 是無法訪問到此網段，那就可以使用此選項。因為若廣域網 1 掉線後走廣域網 2 也無法去訪問到 10.0.0.1 到 10.254.254.254，就不需要在廣域網 1 斷線時將此線路移除。

（2）紀錄到日誌並移除該條線路：當偵測到與 ISP 連結失敗時，系統會在系統日誌中將這項錯誤資訊紀錄下來，原本使用此 WAN 端的封包傳遞會自動轉換到另一條廣域埠.等到原本斷線的廣域埠恢復後會自行重新連結，則封包傳遞會自動轉換回來。

此選項適用在當某條廣域網連線失敗時，從這個廣域網去訪問的目的地位置是可以從另一條線路去訪問的時候，就要用此選項。如此可以讓任何一條廣域網斷線的時候，另一條可以做備援，將流量轉移到還在連線的廣域網。

有流量時不進行偵測：　當下載 或 / 與 上傳流量超過頻寬的百分之（ ）時，表示線路仍在連線運作，不必再一直送出 NSD 偵測要求封包

偵測以下可回應的伺服器：

預設閘道：　近端的預設通訊閘道位置，如 ADSL 路由器的 IP 位址，此為自動填入，所以只須打勾選擇是否啟用。

> 注意！
> 有部分的 ADSL 線路的閘道是不會回應偵測封包，或是當您是使用光纖轉換器，或是運營商發給您的是固定的 Public IP，且閘道就是在您這端而不是在運營商那端時，此選項不要啟用。

ISP 伺服器：　ISP 端的偵測位置，如 ISP 的 DNS 伺服器 IP 位址等。在設定此 IP 位址時請確認此 IP 位址是可以且穩定快速的得到回應 (建議填入 ISP 端 DNS IP)。

遠端伺服器：　遠端的網路節點偵測位置，此 Remote Host IP 位址最好也是可以且穩定快速的得到回應(建議填入 ISP 端 DNS IP)。

DNS 伺服器：　網域名稱端 DNS 的偵測位置(此欄位只許填入網址如"www.hinet.net"，請勿填 IP 位址)。另外，兩條 WAN 的此欄位不可以填入相同的網址。

確定：　點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。

取消：　點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

注意！

在"指定路由"的負載平衡模式下，第一個廣域網口會保留給沒有指定到其他廣域網口的 IP 或應用通訊埠(通訊埠)經由此廣域網(WAN1)進出。因此建議您在此模式下將您的其中一條線路接在第一個廣域網口。當您其他的廣域網口斷線時，而您在線路偵測機制下選擇移除有問題線路，流量就會轉移到第一個廣域網口(WAN1)。此外，若是第一個廣域網口(WAN1)斷線，則流量會依次轉移到其他廣域網口，例如轉移到 WAN2，WAN2 也斷線則轉移到 WAN3 等等。

6.2.3 WAN 口協議綁定設定

頻寬設定

VPN 防火牆會依照您實際輸入的上傳頻寬資料作為兩條廣域埠自動負載平衡的比例依據。例如當兩條廣域網都為上傳 512Kbit/sec 時，其自動負載比例為 1：1。當一條線路的上傳頻寬為 1024kbit/sec 另一條為 512kbit/sec 時，則此自動負載比例為 2：1。所以為了確保您的 VPN 防火牆達到實際線路負載能夠平衡，請填入實際上下載頻寬。此段也關係到 QoS 的設定，所以是在 QoS 的頁面做設定，請參考相關 QoS 設定章節。

ISP實際可用頻寬

接口位置	上傳頻寬 (Kbit/sec)	下載頻寬 (Kbit/sec)
廣域網1	10000	10000
廣域網2	10000	10000
廣域網3	10000	10000
廣域網4	10000	10000

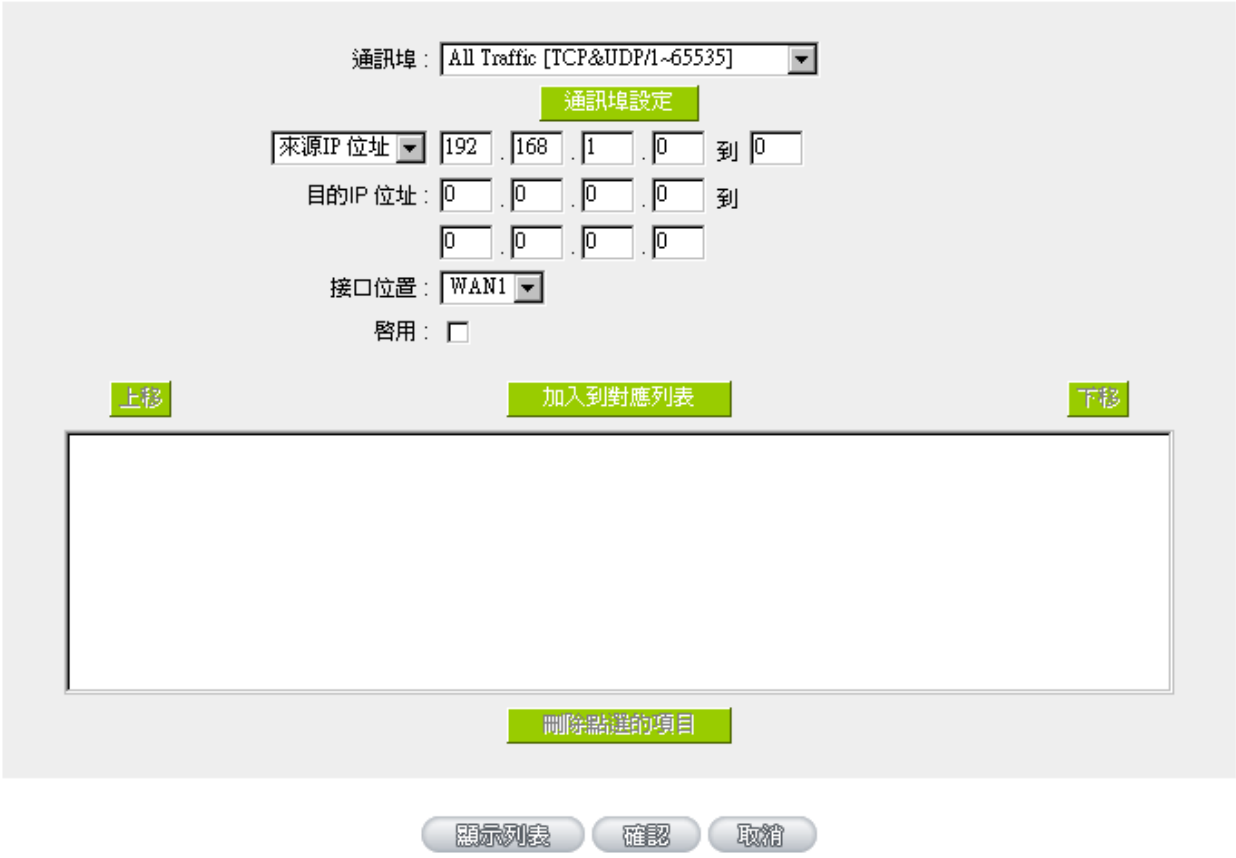
協議綁定

使用者可將特定的 IP 或特定的應用通訊埠(Port)經由您限定的 WAN 出去。其他沒有做綁定的 IP 或伺服器還是會進行廣域網的負載平衡。

注意！

在"指定路由"的負載平衡模式下，第一個廣域網口(WAN1)是不能被指定的，保留給沒有指定到其他廣域網口的 IP 或應用通訊埠(通訊埠)經由此廣域網(WAN1)進出。也就是說第一個廣域網口(WAN1)不能設定通訊協定綁定的規則，以避免所有的廣域網口都被指定有特定的內網 IP、應用通訊埠、目的地 IP，導致其他的 IP 或應用通訊埠沒有廣域網口可以使用。

協議綁定



通訊埠： 在此選擇欲開啟的綁定通訊埠，從下拉式選單中可以選擇預設列表(如 All -TCP&UDP 0～65535， WWW 為 80～80， FTP 為 21～21 等等)，預設的服務為 All 0～65535。

點選"通訊埠設定"按鈕可以進入通訊埠設定視窗，進行新增或刪除選單中預設的通訊埠。

來源 IP 位址： 您可以指定特定的內部虛擬 IP 位址的封包經由特定的廣域埠出去。

在此填上內部虛擬 IP 位址範圍，例如 192.168.1.100 到 150.則 IP 位址 100 到 150 為綁定範圍。如果使用者只需要設定特定的通訊埠而不需指定特定的 IP 位址， 則在 IP 的欄位皆填入 0。您也可以選擇 IP 群組的方式來指定來源 IP。關於 IP 群組的設定，請參考（"7.6 IP 群組管理"的說明）。

目的 IP 位址：	在此填上外部固定 IP 位址，例如若有一目標位址 210.11.1.1，要連接此位址的使用者限定只能從廣域埠 1 到達此目標位址，則在此填上外部固定 IP 位址 210.11.1.1 到 210.11.1.1。如果使用者要設定一個範圍的目的地位置，則填入方式可以為 210.11.1.1 到 210.11.255.254，則表示整組 210.11.x.x 的 Class C 網段都限制走某一條廣域網，若只需要設定特定的應用而不需指定特定的 IP 位址，則在 IP 的欄位皆填入 0.0.0.0。
接口位置：	選擇您所要綁定此條規則在哪一個 WAN 埠。
啟用：	啟用此規則。
加入到對應列表：	增加此條規則到列表。
刪除點選的項目：	刪除在服務列表裏所選擇的規則。
上移 & 下移：	由於每條規則執行的優先順序為由列表的最上面那條往下執行，也就是越後面設定的規則會越後執行，所以您可以自行調整每條規則先後執行順序。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

注意！

通訊綁定協定所設的規則在 VPN 防火牆執行時也有優先順序的，由上到下，在列表上最上方那條會先執行，然後依序往下。

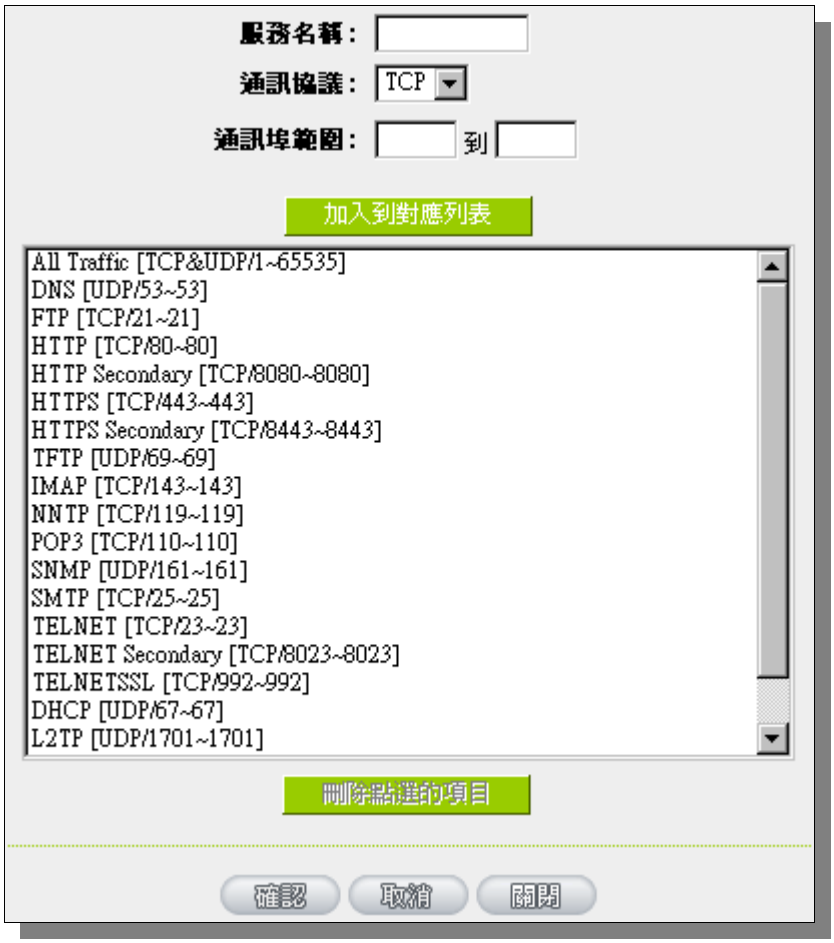
顯示列表：

按下"顯示列表"，會出現以下的對話視窗。您可以選擇以"優先權"來顯示排列的順序，或是以"接口位置"來顯示排列的順序。點選"更新"可以重新顯示視窗，點選"關閉"將結束這個對話視窗。

優先權	接口位置	通訊埠	來源IP 位址	目的IP 位址	啓用	編輯
1	WAN2	FTP [TCP/21~21]	192.168.1.0~192.168.1.0	0.0.0.0~0.0.0.0	Enabled	Edit

新增或刪除管理通訊埠號

若您欲開啟的通訊埠專案沒有在表列中，您可以點選"通訊埠設定"按鈕，新增或刪除管理通訊埠號列表，如以下所述：



服務名稱：	在此自定欲開啟的通訊埠號名稱加入列表中，如 BT 等。
通訊協議：	在此選擇欲開啟的通訊埠號的封包格式為 TCP 或 UDP。
通訊埠範圍：	填入您將新增加的通訊埠範圍。
加入到對應列表：	增加到開啟服務內容列表，最多可新增 100 組。
刪除點選的項目：	刪除所選擇的開啟服務內容。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。
關閉：	離開並關閉此功能設定視窗。

使用"智能型"負載平衡模式時其通訊協議綁定設定方式：

智能負載平衡方式搭配"通訊協議綁定"可以有更彈性運用您的頻寬，您可將特定的內網 IP，使用特定應用通訊埠作訪問，或特定的目的地 IP 經由您指定的廣域網來訪問外網。

範例一：若要指定內網 IP 192.168.1.100 去外網訪問都走廣域網 2，那通訊協議綁定設定方式?

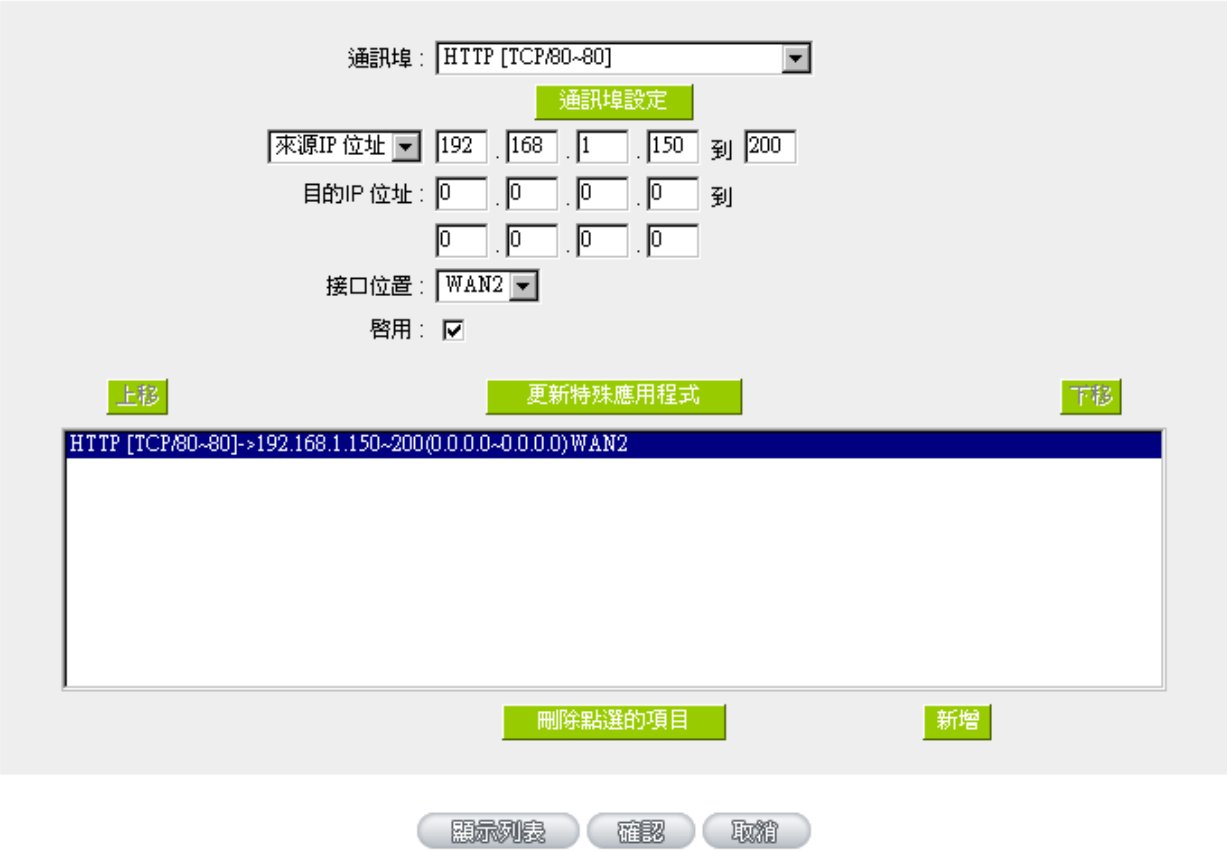
如以下範例所示，通訊埠選擇"All Traffic"，在來源 IP 位址填入 192.168.1.100 到 100，目的 IP 位址保留原本的數值 0.0.0.0 (表示所有的外網位址)。接口位置選則廣域網 2，然後勾選啟用。最後點選"新增"即可將此規則加入。

協議綁定

範例二：若要指定內網 IP192.168.1.150 到 200 去外網訪問 80 埠都走只能走廣域網 2 去訪問，那通訊協定綁定設定方式是怎樣設定?

如以下範例所示，服務端選擇"HTTP[TCP/80~80]"，在來源 IP 位址填入 192.168.1.150 到 200，目的 IP 位址保留原本的數值 0.0.0.0 (表示所有的外網位址)。接口位置選則廣域網 2，然後勾選啟用。最後點選"新增"即可將此規則加入。

協議綁定



範例三：若要指定內網所有 IP 去外網訪問 80 埠都走只能走廣域網 2，但其餘服務都走廣域網 1 時，通訊協定綁定設定方式是怎樣設定?

如以下範例所示，要設定兩條規則：

第一條規則服務端選擇"HTTP[TCP/80~80]"，在來源 IP 位址填入 192.168.1.0 到 0(表示所有的內網位址)，目的 IP 位址保留原本的數值 0.0.0.0 (表示所有的外網位址)。接口位置選則廣域網 2，然後勾選啟用。最後點選"新增"即可將此規則加入。VPN 防火牆會將所有用 80 埠去外網訪問的流量都走廣域網 2，但是不是用 80 埠的流量根據 VPN 防火牆的自動負載平衡演算，還是有可能會走廣域網 2，因此還需要再設第二條規則。

第二條規則，服務端選擇"All Traffic [TCP&UDP/1~65535]"，在來源 IP 位址填入 192.168.1.2 到 254，目的 IP 位址保留原本的數值 0.0.0.0 (表示所有的外網位址)。接口位置選則廣域網 1，然後勾選啟用。最後點選"新增"即可將此規則加入。這時 VPN 防火牆會將不是用 80 埠去外網訪問的流量都走廣域網 1。

協議綁定

使用"指定路由"的負載平衡模式時其通訊協定綁定協定設定方式：

指定路由的模式讓您對特定的內網 IP、特定要訪問的應用通訊埠或特定目的地 IP 經由您指定的廣域網對外網做訪問。且一經指定後，該廣域網也只能讓這些指定的內網 IP、特定要訪問的應用通訊埠、或特定目的地 IP 使用。其他不在這些指定內的內網 IP、特定要訪問的應用通訊埠或特定目的地 IP 都會從另一條廣域網出去訪問。此模式必須配合"通訊協定綁定"功能才能發揮作用。

範例一：若要指定內網所有 IP 去外網訪問 80 埠都走只能走廣域網 2，但其餘服務都走廣域網 1 時，通訊協定綁定設定方式是怎樣設定?

如以下範例所示設定規則，服務端選擇"HTTP[TCP/80~80]"，在來源 IP 位址填入 192.168.1.0 到 0(表示所有的內網位址)，目的 IP 位址保留原本的數值 0.0.0.0 (表示所有的外網位址)。接口位置選則廣域網 2，然後勾選啟用。最後點選"新增"即可將此規則加入。此時廣域網 2 只會有訪問外網 80 埠的流量，其餘流量都只走廣域網 1。

協議綁定

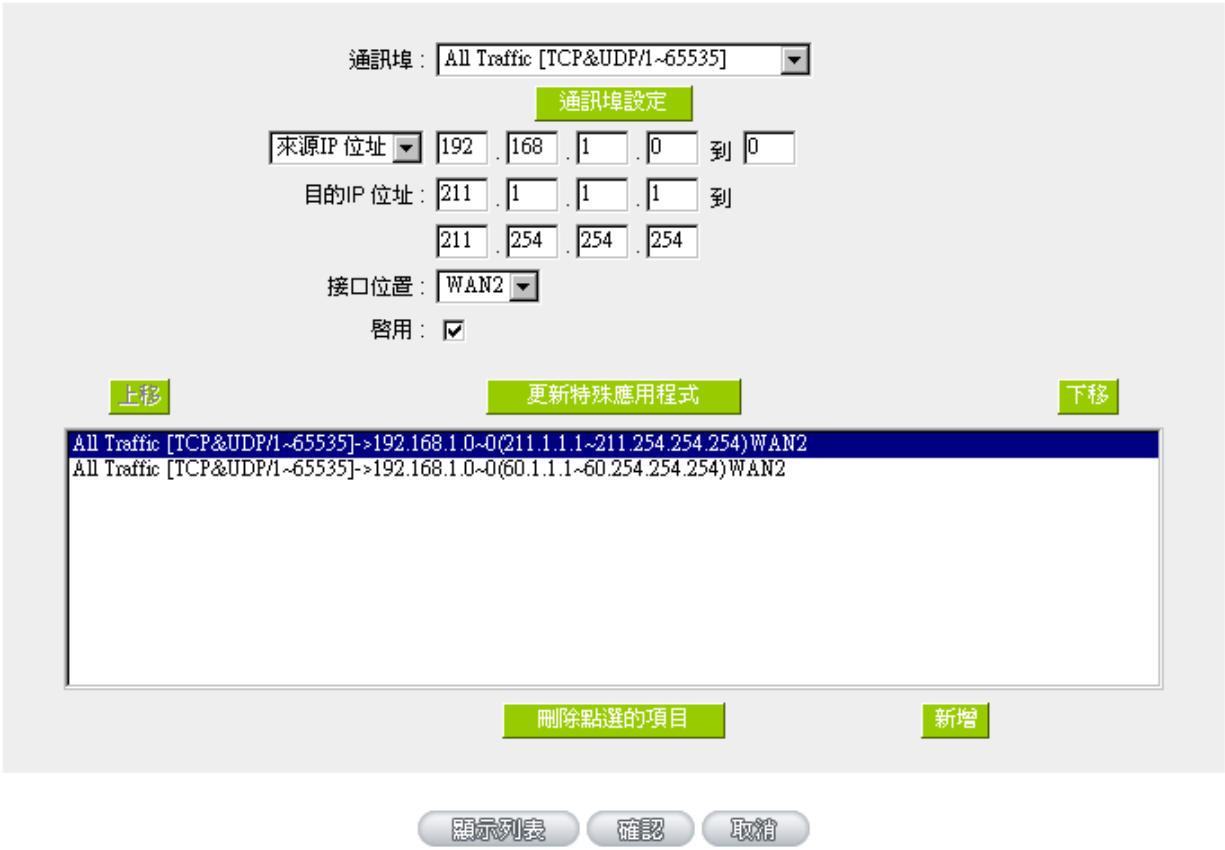
範例二：若要指定內網所有 IP 去外網訪問 IP 211.1.1.1 到 211.254.254.254 還有 60.1.1.1 到 60.254.254.254 整組 A 類段時都走走廣域網 2 去訪問，但去其餘不是這幾個目的地 IP 段時都走廣域網 1 時，那通訊協定綁定設定方式如何設定?

如以下範例所示設定兩條規則：

第一條規則中服務端選擇"All Traffic [TCP&UDP/1~65535]"，在來源 IP 位址填入 192.168.1.0 到 0(表示所有的內網位址)，目的 IP 位址填入 211.1.1.1 到 211.254.254.254。接口位置選則廣域網 2，然後勾選啟用。最後點選"新增"即可將此規則加入。

第二條規則中服務端選擇"All Traffic [TCP&UDP/1~65535]"，在來源 IP 位址填入 192.168.1.0 到 0(表示所有的內網位址)，目的 IP 位址填入 60.1.1.1 到 60.254.254.254。接口位置選則廣域網 2，然後勾選啟用。最後點選"新增"即可將此規則加入。此時，除了上述兩條規則所涵蓋的目的 IP，其餘去外網訪問的流量都只走廣域網 1。

協議綁定


通訊埠 : All Traffic [TCP&UDP/1~65535]
通訊埠設定
來源IP 位址 192 . 168 . 1 . 0 到 0
目的IP 位址 : 211 . 1 . 1 . 1 到
211 . 254 . 254 . 254
接口位置 : WAN2
啓用 :
上移
更新特殊應用程式
下移
All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)WAN2
All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)WAN2
刪除點選的項目
新增
顯示列表
確認
取消

七、內部區域網路設定

通過本章節可以對埠口進行設定管理，瞭解如何設定內部區域網路的 IP 位址。

7.1 實體埠口管理設定（預計未來加入）

VPN 防火牆，管理者可以設定網路實體連線於每一個乙太網路埠，如連接速率，工作模式，優先順序，自動偵測或是 VLAN 等乙太網路埠的功能。

埠口設置

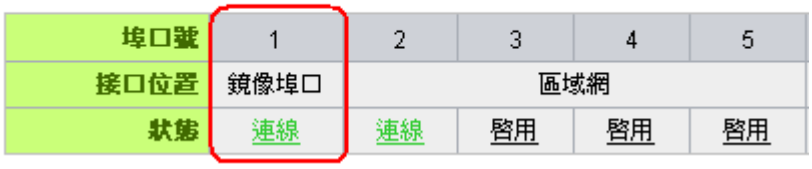
☑ 啓用鏡像埠口(Port 1)

埠口號	接口位置	關閉	優先權	連線速率	半雙/全雙工模式	自動偵測功能	VLAN
1	LAN	☐	Normal	100M	全雙	☑	VLAN1
2	LAN	☐	Normal	100M	全雙	☑	VLAN1
3	LAN	☐	Normal	100M	全雙	☑	VLAN1
4	LAN	☐	Normal	100M	全雙	☑	VLAN1
5	LAN	☐	Normal	100M	全雙	☑	VLAN1
DMZ	DMZ	☐	Normal	100M	全雙	☑	
WAN3	WAN3	☐	Normal	100M	全雙	☑	
WAN2	WAN2	☐	Normal	100M	全雙	☑	
WAN1	WAN1	☐	Normal	100M	全雙	☑	

確認 取消

鏡像埠口：勾選"啟用鏡像埠口（Port 1）"可以將區域網的第一個埠設定為鏡像埠口，所有從內網到外網訪問的流量都會複製到鏡像埠口。因此您可以將監控或是過濾伺服器直接接在鏡像埠口，來達到監控或是過濾網路封包的目的。一旦您啟用這個功能，首頁中的"實體埠口配置狀態"會顯示 LAN Port 1 為"鏡像埠口"。如下圖：

實體埠口配置狀態



埠口號	1	2	3	4	5
接口位置	鏡像埠口	區域網			
狀態	連線	連線	啓用	啓用	啓用

關閉： 此為設定乙太網路的 LAN 埠開啟或是關閉的功能，若是打勾的話，則此乙太網路埠立即被關閉無法連接使用。預設為開啟無打勾。

優先順序設定： 此為設定此乙太網路埠 LAN 端封包傳送優先權設定，若是設定為高的話，則最優先使用傳送封包的權利，預設優先順序為一般。

連線速率： 此為設定此乙太網路埠的網路實體連接速率選項，您可以設定為 10Mbps 或是 100Mbps 連接速度。預設為自動偵測。

半雙/全雙工模式： 此為設定此乙太網路埠的網路實體連接速率工作模式選項，您可以設定為半雙工模式或是全雙工模式運作。預設為自動偵測。

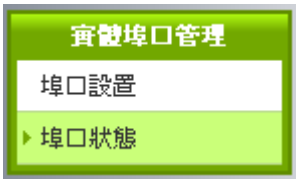
自動偵測功能： 此為設定乙太網路的埠網路實體連接速率自動偵測模式，若是勾選的話，自動偵測所有連接埠的信號與調整。

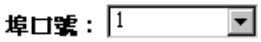
VLAN： 此功能可以讓網管人員在自己的區域網內將每一個區域網埠設定 1 個或多個不同網段且無法互通的區域網埠，但都可以通過 VPN 防火牆上網路。在同一個網段內的成員(在同一個 VLAN 區域網路內)可互相溝通並看得到對方，若不在同一個 VLAN 群組內的成員則無法得知其他成員的存在。使用者可為每一個 LAN 埠選定為哪一個 VLAN 區域網路群組。

VLAN All： 當網管人員在內網設定了多個 VALN 埠，且不在同一個 VLAN 群組內無法互訪，可是內網又需要架設服飾器讓內網所有 VLAN 群組都可以訪問此伺服器。此時可以將某一區域網埠設定為 VLAN All，將此伺服器接入此 VLAN All 的埠，這樣就可以讓所有不同 VLAN 群組的電腦都可以訪問到此伺服器。

7.2 埠口狀態即時顯示（預計未來加入）

此項功能可以讓網路管理者查看每個實體埠口的詳細資訊。





摘要訊息

網路連接型態	10Base-T / 100Base-TX / 1000Base-T
接口位置	LAN
線路連線狀態	Up
實體埠口配置狀態	Port Enabled
優先權設定	Normal
連線速率	100 Mbps
半雙/全雙工模式	Full
自動偵測功能	Enabled
VLAN	VLAN1

流量統計

接收封包數	16051
接收封包流量(Byte)	2226066
傳送封包數	18641
傳送封包流量(Byte)	13695045
錯誤封包統計	0

重新整理

整體資訊項目：

網路連接狀態（10Base-T / 100Base-TX / 1000Base-T），接口位置（區域網/廣域網路/DMZ），線路連線狀態(Up 啟用/Down 關閉)，實體埠口配置狀態（Port Enabled 埠啟用/Port Disabled 埠關閉），優先順序設定（High 高級/Normal 一般），網路連接速率（10Mbps/100Mbps/1000Mbps），半雙/全雙工模式

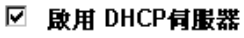
(Half 半雙工/Full 全雙工)，自動偵測功能（Enabled 啟用/Disabled 關閉），VLAN（VLAN Number / VLAN All）。

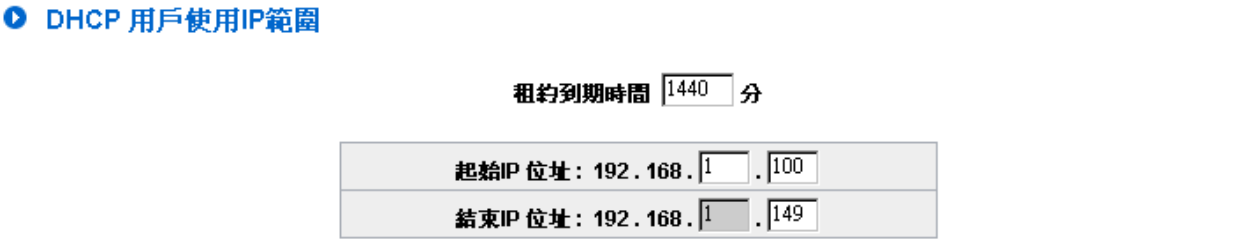
埠口流量統計：

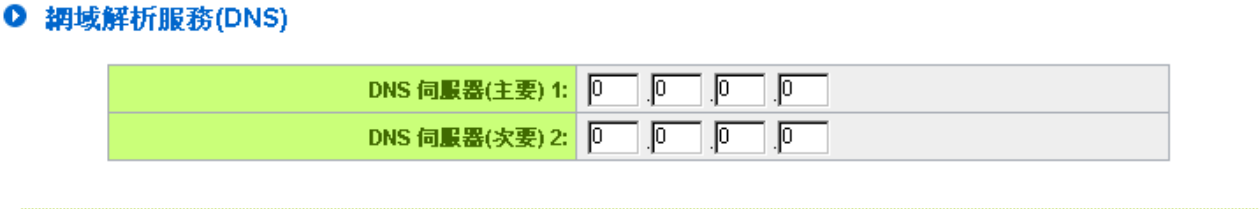
即時顯示 VPN 防火牆工作狀態下的接收和傳送封包計算、封包接收和傳送 Byte 數以及錯誤封包統計實際數值。

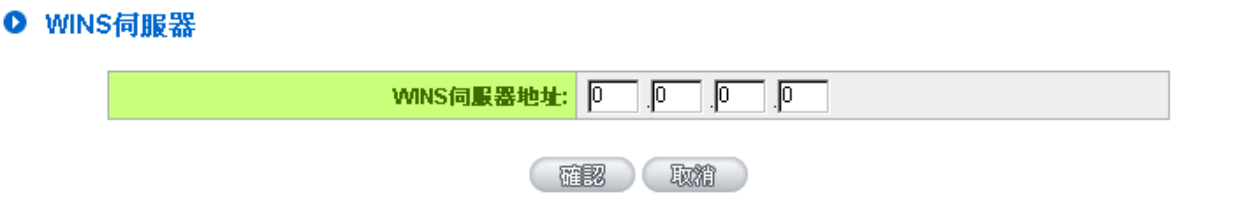
7.3 DHCP 發放 IP 伺服器

VPN 防火牆的 DHCP 伺服器，預設值是啟用，可以提供區域網路內的電腦自動取得 IP 的功能，(如同 NT 伺服器中的 DHCP 服務)，好處是每台 PC 不用去記錄與設定其 IP 位址，當電腦開機後，就可從 VPN 防火牆自動取得 IP 位址，管理方便。









動態 IP 服務：

租約時間：	此設定為發給 PC 端 IP 位址的租約時間，預設為 1440 分鐘(代表時間為一天)，當租約時間到後，PC 端會重新跟 VPN 防火牆申請一次。您可以依照實際需求來設定。
起始 IP 位址：	系統預設為四個網段從 192.168.1.100 的 IP 位址開始發放。您可以依照實際需求來設定。
結束 IP 位址：	系統預設為四個網段 192.168.1.149、IP 位址為最後發放 IP，也就是說出廠設定值每個網段可供 50 台電腦自動取得 IP 位址，您可以依照實際需求來設定。

網域名稱解析伺服器（DNS）位址：

此設定為發給 PC 端 IP 位址的 DNS 網域伺服器查詢位址，若您有特定使用的 DNS 伺服器，可以直接輸入此伺服器的 IP 位址，則 PC 端從 DHCP 取得 IP 位址時，也會一併取得指定的 DNS 伺服器位址。

DNS 伺服器 (主要) 1：	輸入 DNS 網域名稱伺服器的 IP 位置。
DNS 伺服器 (次要) 2：	輸入 DNS 網域名稱伺服器的 IP 位置。

WINS 伺服器：

若您的網路上有解析 Windows 電腦名稱的伺服器，您可以直接輸入此伺服器的 IP 位址。

WINS 伺服器位址：	輸入 WINS 伺服器的 IP 位置。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

7.4 DHCP 狀態顯示

此狀態表為顯示 DHCP 伺服器的目前使用狀態與設定紀錄等，以便提供管理人員需要時做網路設定參考資料。

狀態

DHCP伺服器：	192.168.1.1
已使用的動態IP數量：	4
已發放的固定IP數量：	0
剩餘可用的IP數量：	46
可發放的IP總量：	50

DHCP 用戶連線列表

主機名稱	IP 位址	MAC地址	租約到期時間	刪除
qno-ivan	192.168.1.100	00:20:ed:41:cb:9d	Mon Aug 4 11:10:54 2008	
Compact_QVM_Router	192.168.1.104	00:17:16:01:f7:76	Mon Aug 4 11:00:41 2008	
4_WAN_QVM_Router	192.168.1.105	00:17:16:01:35:d1	Mon Aug 4 10:40:49 2008	
QnoPM001	192.168.1.101	00:1e:8c:c5:b9:69	Mon Aug 4 11:05:45 2008	

重新整理

DHCP 伺服器 IP 位址：　目前 DHCP 伺服器的 IP 位址。

已使用的動態 IP 數量：　目前 DHCP 伺服器已經發放動態 IP 的數量。

已發放的固定 IP 數量：　目前 DHCP 伺服器已經發放固定 IP 的數量。

剩餘可用的 IP 位址：　目前 DHCP 伺服器可以還可發放的 IP 數量。

可發放的 IP 總量：　目前 DHCP 伺服器所設定可發放的 IP 總數量。

主機名稱：　目前此台電腦的電腦名稱。

IP 位址：　目前此台電腦所取得的 IP 位址。

MAC 位址：　目前此台電腦的 MAC 網路實體位置。

租約到期時間：　DHCP 目前核發 IP 位址的租約時間。

刪除：　刪除此筆核發 IP 紀錄。

7.5 IP 與 MAC 位址綁定

在許多的大中型網咖及企業網路中，網管人員可以設定 VPN 防火牆所提供的 IP & MAC 綁定功能，達到用戶不能自行添加電腦來使用對外網路或是私自擅改 IP 上網影響他人。另外通過此功能也可以將每台電腦或伺服器的 MAC 位址綁定，達到電腦或伺服器每次開機或重新要 IP 時，都分配給它相同的一組 IP 位址。

您可以以兩種方式來設定這個功能：

限定可以使用網路的 MAC 位址

此功能主要目的是限制只有在列表裏面的 MAC 位址才可以得到 DHCP 分配的 IP 位址上網，未在此列表的電腦都無法取得 IP 上網；或是限制有在列表但是未啟用綁定功能的電腦。當使用此功能時，切記要將靜態 IP 位址填 0.0.0.0 不可以空白，另外將“封鎖未綁定或綁定列表中未啟用的用戶”選項勾選才可以執行。如下圖中範例所示：

IP 及 MAC 位址綁定

此功能主要目的是讓指定的 MAC 位址電腦在每次開機都會要到同一個指定 IP。此外，若將“封鎖綁定列表中 IP 位址與 MAC 位址不對應的用戶”功能啟用，那麼設定為固定 IP 的電腦或通過此功能已發給特定 IP 的電腦擅自更改 IP 為非指定的 IP 位址時，則會無法上網。

IP與MAC綁定

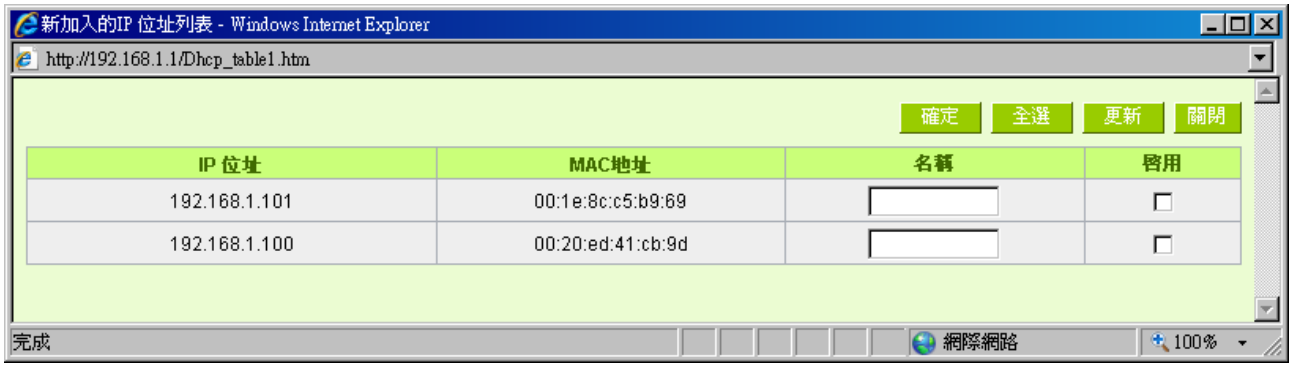
靜態 IP 位址設定：	此欄位有兩種填入方式： 1. 若您只要限制 MAC 位址可以跟 DHCP 要 IP 而不一定是指定的那一個 IP，請在此欄位填 0.0.0.0，不可為空白。 2. 若要求每次此台電腦都要分配到同一個 IP，則將您所要求分配給此台電腦的 IP 位址輸入。這樣所要綁定伺服器或 PC 端每次重啟都會要到固定的同一個虛擬 IP。
所對應的 MAC 位址：	輸入要綁定的伺服器或 PC 端固定實體 MAC (網路卡上的位址)。
名稱：	填入您所綁定此用戶的名字或位址做辨識，可輸入 12 個字元，中英文皆可以。
啟用：	啟用此組設定。
加入到對應列表：	增加或修正此設定到列表中。
刪除點選的項目：	刪除列表中所選擇的綁定。
新增：	當列表中有綁定規則後，右下角會出現此按鈕，可點選增加新的綁定。

封鎖綁定列表中 IP 位址與 MAC 位址不對應的用戶： 此選項打勾後，只要是 User 自行更改電腦的 IP 或不是列表設定的 IP 將無法上網。

封鎖未綁定或綁定列表中未啟用的用戶： 此選項打勾後，只要不在列表中或是在列表中未啟用綁定功能的 MAC 位址都無法上網。

顯示出還未做綁定或新加入的 IP 及其 MAC 位址：

此功能的主要目的是為了減少網管人員需一一查詢每台電腦的 MAC 位址後才能進行綁定，因為會非常耗時且困難。再者，將 MAC 位址手動填入列表也很容易出錯。所以只需要查詢此表格，就可以看到所有進出 VPN 防火牆且還未綁定的 MAC 位址，然後直接在此表格做綁定動作即可。另外，若您發現此表格出現已經綁定的某組 MAC 又出現在此表格，則表示此用戶試圖修改不是您指定的 IP 上網。



名稱： 可以填入您所綁定此用戶的名字或位址做辨識，可輸入 12 個字元。

啟用： 勾選您所要綁定的目標。

確定： 將您所選定好的目標綁定到 IP & MAC 綁定列表。

全選： 選擇所有在此列表中的目標做綁定。

刷新： 更新此列表。

關閉： 關閉此列表。

7.6 IP 群組管理

IP 群組功能可以讓您將數個 IP 位址或 IP 位址範圍組合成一個群組。當您以 IP 位址來管理使用者的網路存取許可權的時候，您可以將具有相同使用權限的使用者設定在同一個 IP 群組裏，並在各個管理功能中選擇以 IP 群組的方式來做設定，可以減少以單一 IP 來做設定的規則數。例如在"通訊協議綁定"的設定，"頻寬管理(QoS)"的設定，以及"訪問規則"的設定中，都可以選擇以 IP 群組的方式來做設定，如此就不需要再以單一 IP 來設定，減少所需要的規則數。

IP 群組：	當您已經有建立好的 IP 群組，您可以在此欄位選擇要修改的群組名稱。
新增群組：	點選此按鈕可以建立新的 IP 群組。
刪除群組：	將您所選定的 IP 群組刪除。
群組名稱：	在此欄位輸入您要建立的 IP 群組名稱，或是修改已經建立過的 IP 群組名稱。
IP 位址：	在此欄位輸入您要建立的 IP 群組的 IP 位址，或是修改已經建立過的 IP 群組的 IP 位址。
加入到對應列表：	加入或修正此設定到列表中。
刪除點選的項目：	刪除列表中所選擇的群組。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於"確定"儲存動作之前才會有效。

八、QoS 頻寬管理功能

頻寬管理 QoS 為 Quality of Service 縮寫，其功能主要為限制某些服務及 IP 的頻寬使用量，以滿足特定應用程式或服務所需要的頻寬或優先權，並讓其餘的使用者共用頻寬，才能有比較穩定、可靠的資料傳送服務。網路管理人員應該針對網咖、企業等的實際需求，對各種不同網路環境、應用程式或服務來進行頻寬管理，才能充分且有效率的達到網路頻寬使用。

8.1 頻寬設定(QoS)

ISP實際可用頻寬

接口位置	上傳頻寬 (Kbit/sec)	下載頻寬 (Kbit/sec)
廣域網1	10000	10000
廣域網2	10000	10000
廣域網3	10000	10000
廣域網4	10000	10000

QoS頻寬管理

8.1.1 頻寬設定

ISP實際可用頻寬

接口位置	上傳頻寬 (Kbit/sec)	下載頻寬 (Kbit/sec)
廣域網1	10000	10000
廣域網2	10000	10000
廣域網3	10000	10000
廣域網4	10000	10000

WAN 的頻寬資料請填入您所申請的寬頻網路實際上傳及下載頻寬，QoS 的頻寬控制會依照您所填入的頻寬作為計算依據。例如每個 IP 及通訊埠可以保障使用的上傳或下載的最小頻寬會依照此 WAN1 及 WAN2 的實際頻寬相加來換算實際可保障的大小。例如上傳頻寬若兩條都為 512Kbit/Sec，那實際上傳頻寬就為 WAN1+WAN2=1024Kbit/Sec，所以若有 50 個 IP 在內部網路，若要保證每人最小可使用的上傳頻寬，則就把 1024Kbit/50=20Kbit，這樣每人可以保證的最小頻寬就可以填 20kbit/Sec，下載同此換算方式。

注意！

這裏的數值單位是 kbit，有些應用軟體顯示下載/上傳速度單位元為 KB，兩個數值之間的換算方式為 1KB=8kbit。

8.1.2 QoS 設定

QoS 可以選擇兩種方式並且同時使用，一為流量控制(頻寬管理)，另一個為優先權控制，設定人員可以依照自己內網需求做兩種模式靈活運用。

頻寬控制 (頻寬管理) - 依使用量做管理：

網管人員可依照您現有的頻寬大小做每一個 IP 或一個範圍的 IP 的使用量限制或保障頻寬。另外也可以針對通訊埠去做頻寬控制。若是內部有架設伺服器的話，也可控制或保障其對外頻寬。

QoS頻寬管理

接口位置：

勾選此條 QoS 設定要控制在哪條 WAN 執行，可單獨或全部勾選。

通訊埠：

選擇此條 QoS 所要設定的頻寬控制為哪個，若您是要針對每個 IP 的所有服務的使用頻寬，則將此選擇在 All(TCP&UDP)1~65535。若您只要針對譬如 FTP 上傳或下載，其餘服務不限制，則選擇 FTP Port21~21，可參考服務號碼預設列表。

IP 位址：

此為選擇您所要限制的使用者為哪些?若您只限制單一 IP，則直接將此 IP 填入，如：192.168.1.100 到 100，則此規則就是針對 192.168.1.100 此 IP 做控制。若是要限制一組 IP 範圍，則填入如 192.168.1.100 到 150，這樣此規則就是針對 192.168.1.100 到 150 做限制。若是此條頻寬限制是針對所有人也就是接在 VPN 防火牆內網的所有 User 則可在 IP 的欄位皆填入 0，也就是 192.168.1.0 到 0，這樣就表示所有 IP 都受此規則限制。另外此 QoS 是可以控制到 Class C 的範圍。

您也可以選擇 IP 群組的方式來指定來源 IP。關於 IP 群組的設定，請參考(“5.4 IP 群組管理”的說明)。

目的：

上傳： 指對內網 IP 的上傳頻寬

下載： 指對內網 IP 的下載頻寬

虛擬伺服器上傳(Server in LAN，上傳)：若您有架設對外的 Server 網站在 VPN 防火牆內部，則此選項為控制外部訪問此 Server 的頻寬控制。

虛擬伺服器下載(Server in LAN，下載)：若您有架設網站在 VPN 防火牆內網，則此選項為控制外部對此伺服器上傳資料時的頻寬控制，例如網咖很多都有架設遊戲伺服器，若外部要來做此遊戲伺服器做資料升級時，可以用此控制做頻寬管理，才不會影響內部使用者上網打遊戲。

保證頻寬 & 最大可用頻寬：
(Kbit/Sec)

保證頻寬：此為限制或保證此條規則的最小可使用頻寬。

最大可用頻寬：此為限制此條規則的最大可使用頻寬，也就是最大不會超過此設定值。

請注意！這裏填入的數值單位是 kbit，有些應用軟體顯示下載/上傳速度單位元為 KB，兩個數值之間的換算方式為 1KB=8kbit。

管制時間：

選擇“所有時間”，此 QoS 設定在所有時間都有效果，如果選擇“從____：____到____：____”填入時間段（24 小時記時制，例如 19：00 到 24：00），以及勾選“每天/周日/週一/週二/週三/週四/週五/週六”的某一天或者幾天，其 QoS 設定只在所勾選設定的特定時間段內有效。

頻寬分配方式：	※此範圍所有 IP 位址共用此設定頻寬： 若選擇此規則的話，其表示所有 IP 或此通訊埠共用這段(保證頻寬到最大可用頻寬)頻寬範圍。 ※此範圍每一 IP 位址獨享此設定頻寬： 若選擇此規則的話，其表示每一個 IP 或這一段通訊埠都可以有此保證頻寬到最大可用頻寬)頻寬範圍，例如若是針對每台電腦 (IP 位址)做的規則設定，則每台電腦(IP 位址)都可以有這麼大的頻寬。 請注意！當您選擇頻寬的共用方式時，要留意實際應用的情況，以避免選擇不恰當的方式而造成頻寬太小無法正常使用網路。例如，內網多人使用 FTP 做檔下載，若是您希望 FTP 不會佔用掉大部分的頻寬，您就可以選擇共用頻寬，不論內網有多少人使用 FTP 做檔下載，總和所佔用的頻寬是固定的。
啟用：	啟用此規則。
加入到對應列表：	增加此條規則到列表。
上移 &下移：	由於 QoS 的每條規則執行的優先順序為由列表的最下面那條往上執行，也就是越後面設定的規則會優先執行，所以您可以自行調整每條規則先後執行順序。通常將要限制頻寬的通訊埠移至最下方如 BT，e-mule 等，然後將針對限制 IP 頻寬的規則往上移。
刪所選中的項目：	刪除在服務列表裏所選擇的內容。
顯示列表：	可以顯示出您所有在頻寬管理設定的規則，並可直接點選"編輯"做修改（見表後詳解）。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

顯示列表：

點選左下方的"顯示列表"按鈕，會出現以下的對話視窗。您可以選擇以"規則"來顯示已設定的規則，或是以"接口位置"來顯示已設定的規則。點選"刷新"可以重新顯示視窗，點選"關閉"將結束這個對話視窗。可直接點選"編輯"做修改。

通訊埠	IP 位址	目的	保證頻寬 (Kbit/sec)	最大可用頻寬 (Kbit/sec)	頻寬分配方式	啓用	接口位置	編輯
FTP [TCP/21~21]	192.168.1.0 ~ 192.168.1.0	Upstream	10	100	Each	Enabled	WAN1,WAN2,WAN3,WAN4	Edit

範例一：若希望內網去做 ftp 下載都只能共同使用 50kbit 下載頻寬要如何設定?

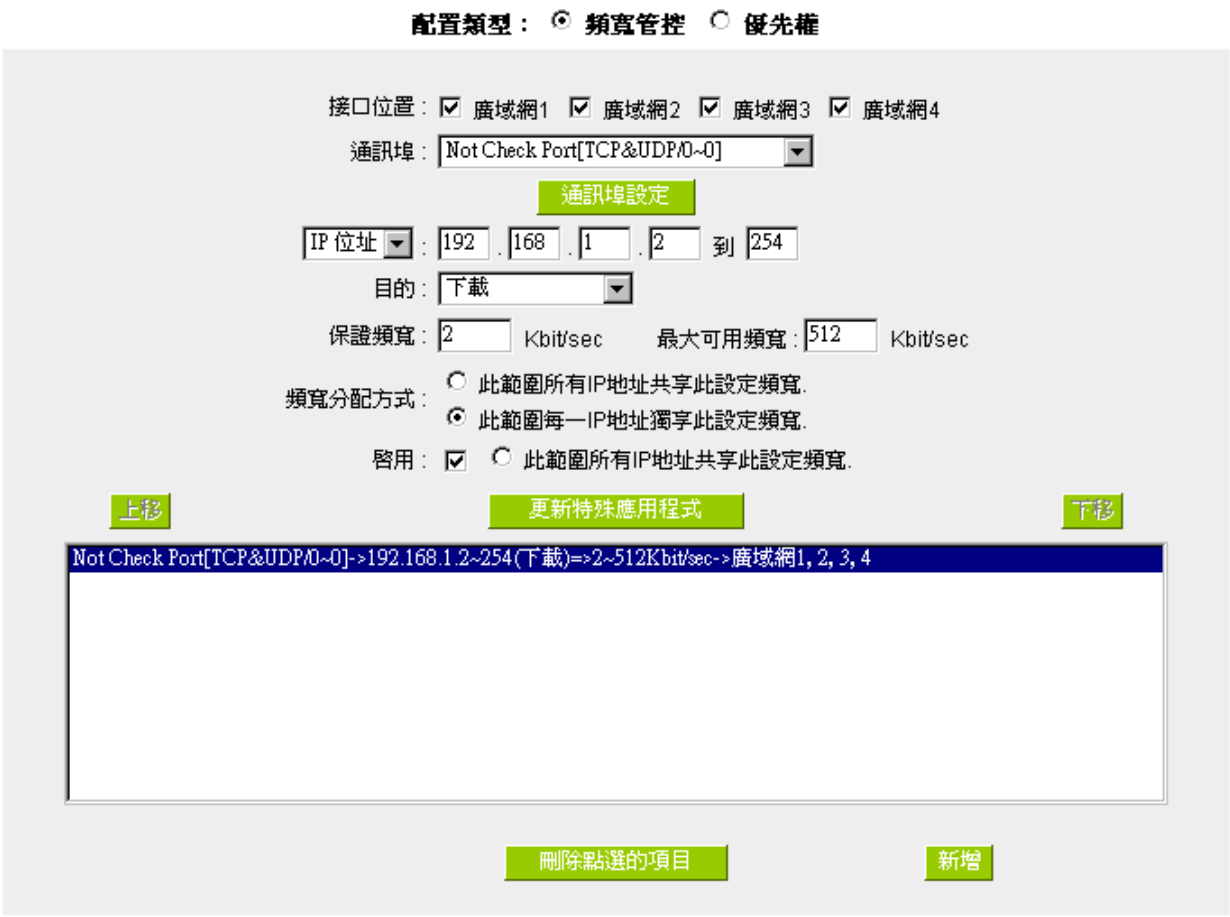
如以下範例所示設定規則，接口位置勾選廣域網 1、2、3、4，服務端選擇"FTP[TCP /21~21"，在 IP 位址填入 0.0.0.0 到 0(表示所有的位址)，目的選擇下載。最小頻寬填入 2 kbit/sec，表示 FTP 下載保證有 2kbit/sec 的頻寬。最大頻寬填入 50kbit/sec，表示 FTP 下載最多只能使用到 50kbit/sec 的頻寬。頻寬共用方式選擇"此 IP 位址共用此設定頻寬"，如此不論內網有多少人使用 FTP，所有 FTP 下載的頻寬總和最多只能使用 50kbit/sec。勾選啟用，最後點選"新增"即可將此規則加入。

QoS頻寬管理

範例二：若希望內網所有 IP 每人最大下載使用頻寬只能有 512Kbit，需要一個 IP 一個 IP 設定嗎?

不需要一個 IP 一個 IP 設定。如以下範例所示設定規則，接口位置勾選廣域網 1、2、3、4，服務端選擇"No Check Port[TCP&UDP /0~0"，在 IP 位址填入 192.168.1.2 到 254(要作限制的位址範圍)，目的選擇下載。最小頻寬填入 2 kbit/sec，表示每個 IP 保證有 2kbit/sec 的頻寬。最大頻寬填入 512kbit/sec，表示每個 IP 最多只能使用到 512kbit/sec 的頻寬。頻寬共用方式選擇"此範圍每一 IP 位址最大及最小可用頻寬"，如此每一個 IP 最小一定有 2kbit/sec 的保證。勾選啟用，最後點選"新增"即可將此規則加入。

QoS頻寬管理



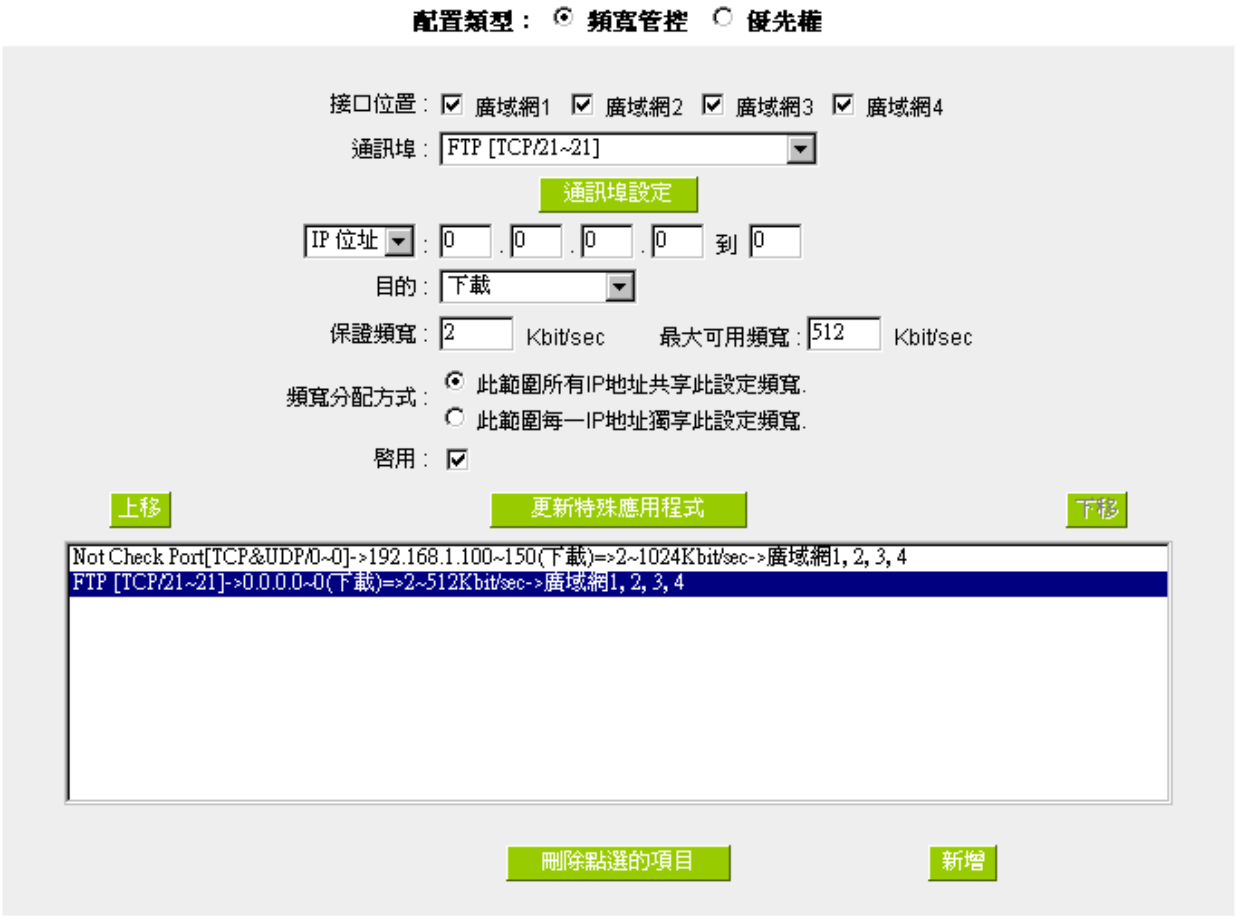
範例三：若希望內網所有 IP192.168.1.100-150 每人最大下載使用頻寬只能有 1M，但當使用 ftp 下載時都只能共用 512Kbit 時要如何設定?

如以下範例所示設定兩條規則，第一條規則接口位置勾選廣域網 1、2、3、4，服務端選擇"No Check Port[TCP&UDP /0~0"，在 IP 位址填入 192.168.1.100 到 150(要作限制的位址範圍)，目的選擇下載。最小頻寬填入 2 kbit/sec，表示每個 IP 保證有 2kbit/sec 的頻寬。最大頻寬填入 1024kbit/sec，表示每個 IP 最多只能使用到 1M/sec 的頻寬。頻寬共用方式選擇"此範圍每一 IP 位址最大及最小可用頻寬"，如此每一個 IP 最小一定有 2kbit/sec 的保證。勾選啟用，最後點選"新增"即可將此規則加入。

第二條規則接口位置勾選廣域網 1、2、3、4，服務端選擇"FTP[TCP /21~21"，在 IP 位址填入 0.0.0.0 到 0(表示所有的位址)，目的選擇下載。最小頻寬填入 2 kbit/sec，表示 FTP 下載保證有 2kbit/sec 的頻寬。最大頻寬填入 512kbit/sec，表示 FTP 下載最多只能使用到 512kbit/sec 的頻寬。頻寬共用方式選擇"此 IP 位址共用此設定頻寬"，如此不論內網有多少人使用 FTP，所有 FTP 下載的頻寬總和最多只能使用 50kbit/sec。勾選啟用，最後點選"新增"即可將此規則加入。

請注意！QoS 頻寬管理的執行順序為由列表最下麵那一條往上做執行動作，所以要將先執行的規則往最下麵移。以這個範例來說，先執行 FTP 的共用頻寬，在執行每個 IP 的保證以及最大可用頻寬。因此若是內網有人使用 FTP 下載，就會先受到第一條規則的限制，最大只能用到 512kbit/sec。若是將規則反過來，將上述的第一條規則移到最下方來先執行，則每個 IP 最大可用到 1M 的頻寬，此時用 FTP 下載也就可以用到 1M 的頻寬，那麼後執行的 FTP 頻寬限制在 512kbit 就不會執行，也就沒有意義了！

QoS頻寬管理



優先順序- 依優先順序做管理：

優先順序顧名思義就是可以將您選定想要的服務做先後順序的調配，也就是可以直接選擇通訊埠將其優先順序做一分配。

VPN 防火牆會將頻寬做 60%(最高)、10%(最低)的頻寬分配，也就是若您將 80 埠選擇為高級，那麼 VPN 防火牆只要遇到 80 埠的封包就會給予 60%的頻寬出去，若您將 FTP 埠 21 設定為低級，那當有人使用 Port 21 時，VPN 防火牆只會給它 10%的頻寬使用，其餘未做分配的服務端就使用 30%頻寬。

接口位置： 勾選此條選擇優先權的設定要控制在哪條 WAN 執行。

通訊埠： 在此選擇此條優先權所要設定的通訊埠為哪個，要針對譬如 FTP 上傳或下載，則選擇 FTP Port21~21，可參考下拉功能表服務號碼預設列表。

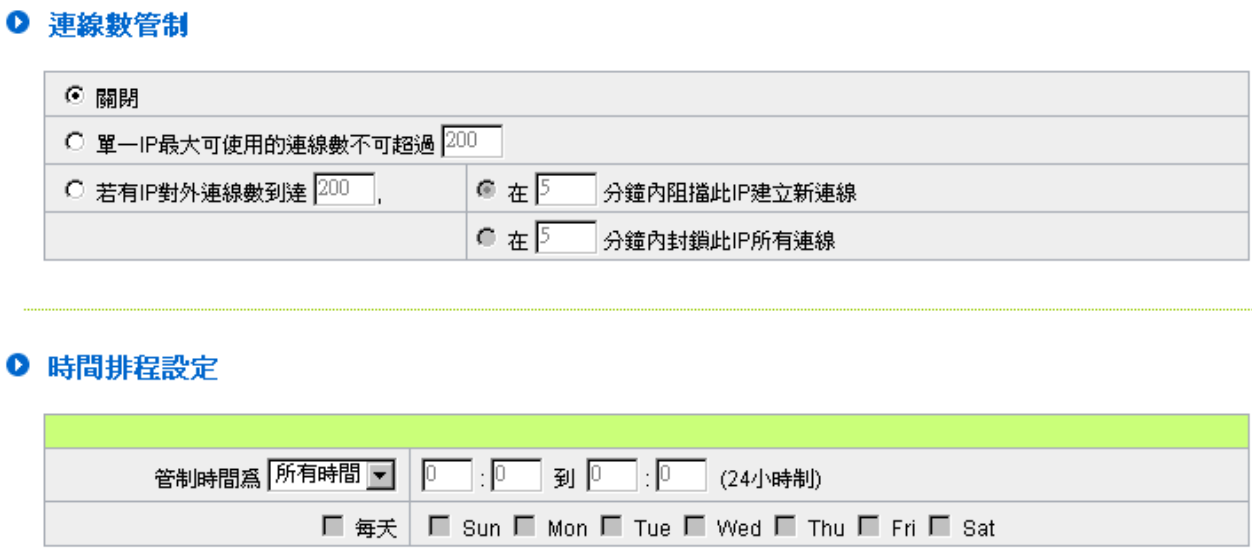
目的：	上傳： 指標對此通訊埠的上傳做優先權控制。 下載： 指標對此通訊埠的下載做優先權控制。 虛擬伺服器上傳(Server in LAN，上傳)：若您有架設對外的 Server 網站在 VPN 防火牆內部，則此選項為控制外部訪問此 Server 的頻寬控制。 虛擬伺服器下載(Server in LAN，下載)：若您有架設網站在 VPN 防火牆內網，則此選項為控制外部對此伺服器上傳資料時的頻寬控制，例如網咖很多都有架設遊戲伺服器，若外部要來做此遊戲伺服器做資料升級時，可以用此控制做頻寬管理，才不會影響內部使用者上網打遊戲。
優先權順序：	高： 此為保證 60%的頻寬給此通訊埠使用。 低： 此為只給 10%的頻寬給此通訊埠使用。
啟用：	啟用此規則。
加入到對應列表：	增加此條規則到列表。
刪除所選中的項目：	刪除所選擇在服務列表裏的內容。
顯示列表：	可以顯示出您所有在優先權設定的規則，並可直接點選"編輯"做修改。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

8.2 連線數管制

連線數管制可以控制內網的電腦最多能同時建立的連線數。這個功能對網管人員在控制內網使用 P2P 軟體如 BT、迅雷、emule 等會造成大量發出連線數的軟體提供了非常有效的管理。設定恰當的容許連線數可以有效控制 P2P 軟體時所能產生的連線數，相對也使頻寬使用量達到一定的限制。

另外，若電腦中了類似衝擊波的病毒而產生大量對外發連線請求時，也可以達到抑制作用。

連線數管制設定以及時間排程設定：



關閉：	不使用此連線數管控功能。
單一 IP 最大可使用的連線數不可超過：	此選項為限制每一台內網的電腦最大可建立的對外連線數，當用戶電腦使用連線數到達此限制值時，要建立新的連線必須等到之前的連線結束後才能再建立。例如，當用戶使用 BT 或 P2P 等下載時且連線數超過此設定值後，當用戶又要再開其他服務時會無法使用，除非將使用中的 BT 或 P2P 軟體關閉。
若有 IP 對外連線數到達___時：	在____分鐘內阻止此 IP 建立新連線：此選項為當用戶端電腦使用連線數到達您的設定數值時，此用戶在 5 分鐘之內將不能再增加新連線，就算舊連線已經結束，也必須等到設定時間過後才能再建立新的連線。 在____分鐘內封鎖此 IP 所有連線：此選項為當用戶端電腦使用的連線數到達您的設定數值時，此用戶正在使用的所有連線都將被清除，且在 5 分鐘之內將不能建立任何連線(不能上網)，必須等到設定時間過後才能再建立新的連線。

時間排程設定：	選擇"所有時間"，此連線數管制設定在所有時間都有效果，如果選擇"從____：____到____：____"填入時間段（24 小時記時制，例如 19：00 到 24：00）， 以及勾選"每天/周日/週一/週二/週三/週四/週五/週六"的某一天或者幾天，其設定在所勾選設定的特定時間段內有效。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

不受限制的通訊埠或 IP 位址

當有的用戶以及 IP（比如公司管理層等），或者是特定需要不受限制的服務通訊埠（公司財務資料的傳輸，郵件的傳輸等），管理人員可以設定這些服務通訊埠或者 IP 不受連線管制。

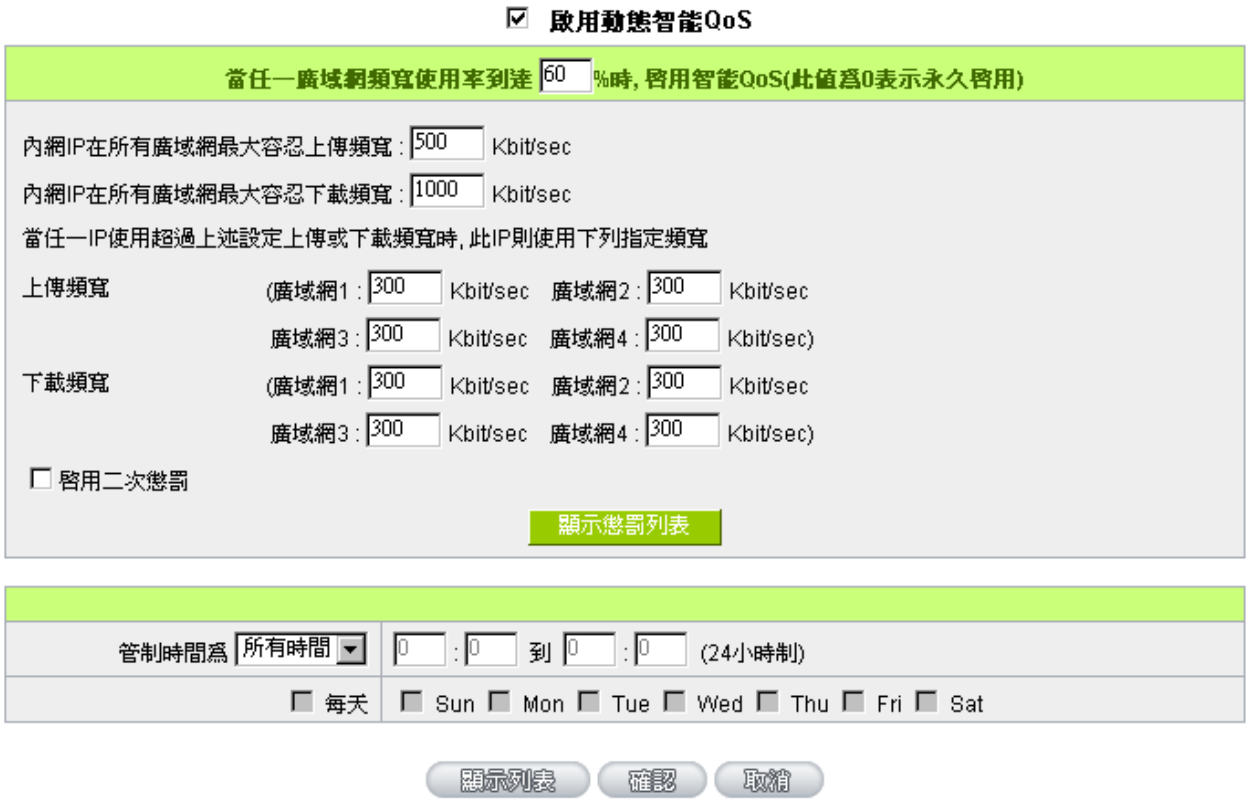
不受限制的通訊埠或IP 位址

通訊埠：	選擇不受限制的通訊埠。
IP 位址：	輸入不受限制的 IP 位址範圍，或者選擇不受限制的 IP 群組。
啟用：	啟用此規則。
加入到對應列表：	將添加的規則增加到列表中。
刪除點選的項目：	選擇列表中的規則，刪除選中的規則。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。

取消： 點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

8.3 動態智慧頻寬管理（Smart QoS）

無需網管進行設定的智慧型頻寬管理 Smart QoS 功能，自動壓抑佔用頻寬用戶，來解決內網 QoS 管理簡化網管的管理工作。



啟用動態智能 QoS：	勾選啟用動態智慧 QoS。
當任一廣域網頻寬使用率到達____%時，啟用智慧 QoS	當頻寬使用率到達實際頻寬的一個%比時，將啟用活智慧 QoS，您可輸入需要的數值，系統預設是 60%。
內網 IP 在所有廣域網最大容忍上傳頻寬 ：	填入內網 IP 上行最大容忍使用頻寬。
內網 IP 在所有廣域網最大容忍下載頻寬 ：	填入內網 IP 下載最大容忍使用頻寬。
當任一 IP 使用超過上述設定上傳或下載頻寬時, 此 IP 則使用下列指定頻寬：	當任一 IP 使用超過上述設定上傳或下載頻寬時，就實行懲罰措施，並以各個廣域網路的上傳 / 下載分別設定，懲罰後允許使用的頻寬是多少
啟用二次性懲罰：	點選勾選"啟用二次性懲罰："後，VPN 防火牆內部設定好二次懲罰條件，當內部網路上網用戶上網過程中的上傳與下載達到內部條件將執行二次懲罰。
顯示處罰列表：	點選後，在彈出的對話方塊中將會顯示 VPN 防火牆罰中的 IP，上行限制中，下載限制中以及二次懲罰資訊。

管制時間：	選擇"所有時間"，此 QoS 設定在所有時間都有效果，如果選擇"從____：____到____：____"填入時間段（24 小時記時制，例如 19：00 到 24：00）， 以及勾選"每天/周日/週一/週二/週三/週四/週五/週六"的某一天或者幾天，其 QoS 設定在所勾選設定的特定時間段內有效。

九、防火牆設定

本章節介紹防火牆設定的選項，以及網路存取控制的設定，保證網路的安全性。

9.1 基本設定

從防火牆功能的一般設定選項當中， 您可以控制開啟或是關閉這些選項功能。出廠預設值是將防火牆開啟，並關閉不必要的回應。

防火牆功能： 此為選擇開啟或關閉防火牆功能。預設啟用。

SPI 封包檢測： 此為封包主動偵測檢驗技術，防火牆主要運作在網路層，但是藉由執行對每個連結的動態檢驗，也擁有應用程式的警示功能。同時，封包檢驗型防火牆可以拒絕非標準的通訊協定所使用的連結。預設啟用。

防止 DoS 攻擊功能：	此為保護 DoS 攻擊，如 SYN Flooding， Smurf， LAND， Ping of Death， IP Spoofing 等。預設啟用。
關閉廣域網回應功能：	若是選擇啟用的話，則 VPN 防火牆會關閉對外的 ICMP 與不正常連線的封包回應，所以若是您從外部去 ping 此台 VPN 防火牆的 WAN IP 是無法 ping 通的，預設值為開啟拒絕對外回應的功能。
遠端管理功能：	遠端管理功能，若您要通過遠端網路 直接連線進入 VPN 防火牆的設定視窗，必需將此功能開啟，並於遠端於流覽器網址填入 VPN 防火牆的外部合法 IP 位址(WAN IP)，並加上預設可修改的控制埠(預設為 80，可更改)。
允許 Multicast 封包穿透:	網路上有許多影音串流媒體，使用廣播方式可以讓用戶端接收此類封包訊息格式。預設為關閉
防止 ARP 病毒攻擊：	此功能為防止內網遭受 ARP 欺騙攻擊而造成電腦無法上網，此 ARP 病毒欺騙大多在網咖環境發生，會讓所有上網電腦一瞬間掉線或部份電腦無法上網。開啟此功能可以避免此種病毒攻擊。

進階設定

封包類型： VPN 防火牆提供三種資料封包傳輸類型，包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood。

廣域網限定值設定：防止來自外部網路的攻擊。設定"所有封包限定值"（即外部攻擊的所有封包資料），當其達到一個最大值（預設 15000pakets/Sec），VPN 防火牆將只允許通過所設定最大值的封包數。

當單一 IP 的封包限定值（外部單一一個 IP 位址攻擊的封包資料）達到一個最大值（預設 2000pakets/Sec），就會阻擋此 IP 上網 5 分鐘（預設是 5 分鐘），禁止其訪問伺服器，限制其流量和連接數，從而有效保證網路的安全。這裏您可以根據需要調整你的限定值以及阻擋時間來達到對外網攻擊的有效防護，建議其限定值從大到小來調節，避免限定值過小影響正常網路的運行。

區域網限定值設定：防止來自內部網路的攻擊。同樣，當所有封包限定值（即外部攻擊的所有封包資料）達到一個最大值（預設 15000pakets/Sec），VPN 防火牆將只允許通過所設定最大值的封包數。

當單一封包限定值（內部單一一個 IP 位址攻擊的封包資料）達到一個最大值（預設 2000pakets/Sec），就會阻擋此 IP 上網 5 分鐘（預設是 5 分鐘），禁止其訪問伺服器，限制其流量和連接數，從而有效保證網路的安全。您可以根據需要調整你的閥值以及阻擋時間來達到對內網攻擊的有效防護，建議其閥值從大到小來調節，避免閥值過小影響正常網路的運行。

不受限制的來源IP位址: 輸入不要被 DOS 防禦設定限定值所限制的區域網來源 IP 位址或是範圍

不受限制的目的IP位址: 輸入不要被 DOS 防禦設定限定值所限制的目的 IP 位址

(從區域網發出的封包)

顯示被阻擋的 IP：

顯示被 DOS 防禦功能所阻擋的 IP 位址，以及該 IP 位址還剩餘多少時間解除阻擋

禁止特殊應用： VPN 防火牆支援封鎖下列幾種的方式連結：Java，Cookies，Active X，HTTP 代理伺服器存取。

不受限制的信任網域名稱： 若啟用這項功能，使用者可以將信任的網站或者 IP 位址加入可信任的網域中，則 VPN 防火牆就不會去阻擋可信任網域的網頁中所帶有的 Java/ActiveX/Cookies 等。

確定： 點選此按鈕"確定"即會儲存剛才所變動的修改設定內容參數。

取消： 點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於"確定"儲存動作之前才會有效。

9.2 阻擋特定服務

VPN 防火牆提供一指封特定的服務功能，可以通過設定將特殊服務 MSN、Skype、QQ、BT 下載這些服務擋住，以方便用戶的管理設定。

如下圖可以看出 MSN 服務被關閉，內部網路 192.168.1.2～100 的 IP 則設為例外允許的 IP 範圍，此範圍內仍將提供 MSN 資訊服務功能，您可以按照需要對內網 IP 的這幾個服務做阻擋設定。

另外，若啟用封鎖 QQ 服務，也可以針對某些 QQ 號碼能夠不受封鎖做設定，按下"不受限制的 QQ 號碼"，跳出以下視窗即可將不受封鎖限制的 QQ 號碼輸入，增加到下方清單以內：

使用者名稱：　　輸入能識別此 QQ 號碼的資訊，例如 Qno Sales。

不受限制的 QQ 號碼：　　輸入不受限制的 QQ 號碼。

加入到對應列表：　　將添加的規則增加到列表中。

刪除點選的項目：　　選擇列表中的規則，刪除選中的規則。

9.3 存取規則設定

VPN 防火牆設計有簡而易懂的網路存取規則條例工具，管理者可以用來對不同的使用者設定不同的存取規則條件，來管理使用者對網路的存取許可權。存取規則可以依據不同的條件來過濾，例如可以設定封包要管制的進出方向是從內部到外部還是從外部到內部，或是設定以使 IP 位址、目地端 IP 位址、IP 通訊協定狀態等條件來做管制，管理者可以依照實際的需求調性設定。

9.3.1 預設管制規則

管理者定訂的網路存取規則條例，可以選擇關閉或是允許來調整使用者對網路的存取。以下就針對 VPN 防火牆的網路存取規則條例做一說明：

VPN 防火牆預設的網路存取規則條例：

*從 LAN 端到 WAN 端的所有封包可以通過-All traffic from the LAN to the WAN is allowed

*從 WAN 端到 LAN 端的所有封包不可以通過-All traffic from the WAN to the LAN is denied

*從 LAN 端到 DMZ 端的所有封包不可以通過-All traffic from the LAN to the DMZ is denied

*從 DMZ 端到 LAN 端的所有封包不可以通過-All traffic from the DMZ to the LAN is denied

*從 WAN 端到 DMZ 端的所有封包不可以通過-All traffic from the WAN to the DMZ is denied

*從 DMZ 端到 WAN 端的所有封包不可以通過-All traffic from the DMZ to the WAN is denied

管理者可以自定存取規則並且超越 VPN 防火牆的預設存取條件規則，但是以下的四種額外服務項目為永遠開啟，不受其他自定規則所影響：

* HTTP 的服務從 LAN 端到 VPN 防火牆 預設為開啟的 (為了管理 VPN 防火牆使用)。

* DHCP 的服務從 LAN 端到 VPN 防火牆 預設為開啟的 (為了從 VPN 防火牆自動取得 IP 位址使用)。

* DNS 的服務從 LAN 端到 VPN 防火牆 預設為開啟的 (為了解析 DNS 服務使用)。

* Ping 的服務從 LAN 端到 VPN 防火牆 預設為開啟的 (為了連通測試 VPN 防火牆使用)。

跳到 1 / 1 頁　　每頁顯示 5 筆

優先權	啓用	管制動作	通訊埠	接口位置	來源IP 位址	目的IP 位址	管制時間	日	編輯	刪除
	☑	Allow	All Traffic [*]	LAN	Any	Any	Always			
	☑	Deny	All Traffic [*]	WAN1	Any	Any	Always			
	☑	Deny	All Traffic [*]	WAN2	Any	Any	Always			
	☑	Deny	All Traffic [*]	WAN3	Any	Any	Always			
	☑	Deny	All Traffic [*]	WAN4	Any	Any	Always			

加入新規則　回復出廠預設值

除了預設規則以外， 所有的網路存取規則都會顯示於此規則列表中，您可以自己選擇高低優先權於每一個網路存取規則項目中。VPN 防火牆在做規則確認時是依照優先權 1-2-3…。依序做規則判斷，所以優先權是讓您在做存取規則的設定規劃中必須要考慮的，以避免您想開啟或關閉的功能失效。

編輯：　可以設定網路存取規則項目。

垃圾桶圖像：　可以刪除網路存取規則項目。

加入新規則：　新增新的網路存取規則按鈕可以新增一項新的存取規則。

回復出廠預設值：　可以恢復到出廠原有預設存取規則項目並刪除所有的自定規則內容。

9.3.2 增加新的存取規則

管制動作： 允許： 允許符合此管制條例行為的封包通過。
關閉： 不允許符合此管制條例行為的封包通過。

通訊埠： 從下拉式選單中選擇您所要允許或不允許的通訊埠服務項目內容。

通訊埠設定： 若是您想要管制的通訊埠服務內容沒有存在於預設列表內的話，您可以點選右方的服務端新增或刪除表來新增一個服務內容。於彈出視窗中輸入一個服務名稱以及通訊協定與埠，點選"新增"按鈕即可新增一個管制服務項目內容。

日誌： 允許： 依據此規則發生的相關事件將在日誌中記錄。
關閉： 依據此規則發生的相關事件不會日誌中記錄。

接口位置： 選擇您所要允許或不允許的來源封包接口(例如是從 LAN， WAN1，WAN2 還是任何的)，可以從下拉式選單中選擇。

來源 IP 位址： 選擇來源封包的 IP 範圍(如任何的，單獨或者範圍)，若是選擇單獨是範圍的話，請輸入此單一或是一區段範圍的 IP 位址。
您也可以選擇 IP 群組的方式來指定來源 IP。關於 IP 群組的設定，請參考（"7.6 IP 群組管理"說明）。

目的 IP 位址： 選擇目的端封包的 IP 範圍(如任何的，單獨或者範圍)，若是選擇單獨是範圍的話，請輸入此單一或是一區段範圍的 IP 位址。

時間排程設定：	您可以將此條規則依照您所需要的執行時間來做控管。例如您可以設定此規則每天上午 8：00 開始執行下午 17：00 結束，或 24 小時都執行管制。
應用此存取規則：	選擇"所有時間"表示都 24 小時都執行此規則(預設)，或是可以選擇從幾點到幾點，以及設定是每天還是某幾天做管制。
…到…：	…到…： 此管制規則有時間限制，設定方式為 24 小時制，如 08：00 到 18：00 (早上 8 點到下午 6 點)。
管制天數：	勾選"每天"是表示每一天的這段時間都受控管，若是只針對一星期特定星期幾，可以直接選擇星期。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

範例 1：若要將病毒埠 TCP 135-139 封鎖要如何設定?

首先在通訊埠新增部份加入 TCP 135-139 埠(請參考如何新增通訊埠的章節)，然後進行以下的設定：

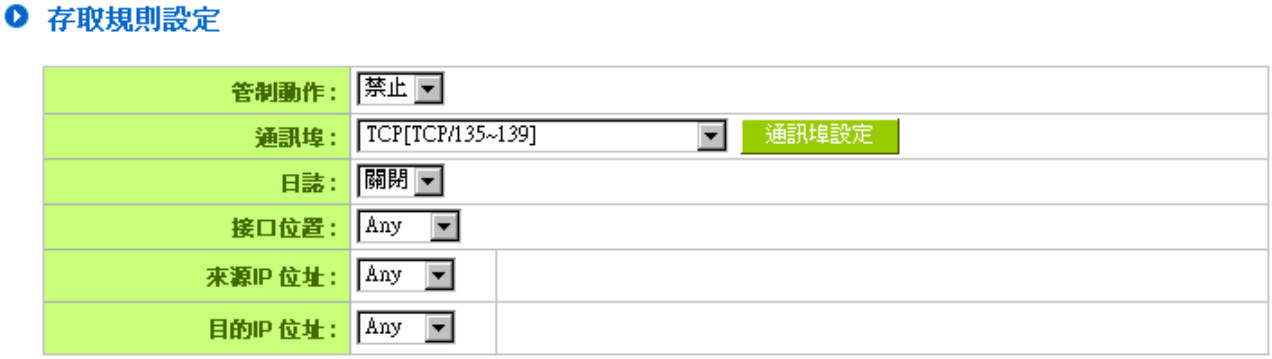
管制動作：禁止

通訊埠：TCP135-139

來源接口：任何的(此意思為封鎖由內網往外網以及從外網攻擊內網的任何此埠)

來源 IP 位址：任何的(此意思為封鎖由內網往外網以及從外網攻擊內網的任何此埠)

目的 IP 位址：任何的(此意思為封鎖由內網往外網以及從外網攻擊內網的任何此埠)



範例 2：若要禁止內網 IP 段 192.168.1.200 到 192.168.1.230 禁止訪問 80 埠要如何設定?

管制動作：：禁止

通訊埠：TCP 80

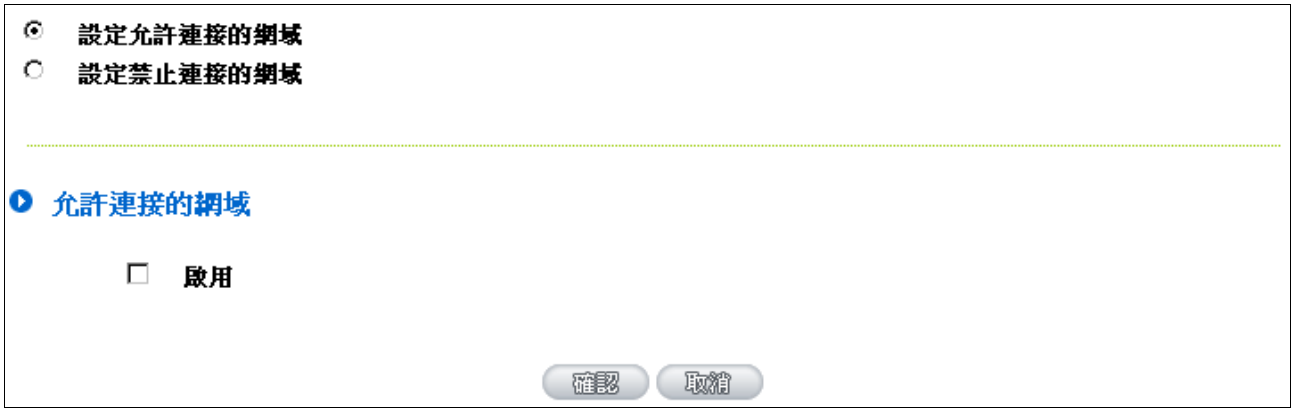
來源接口：區域網(此意思為封鎖由內網往外網的 80 埠)

來源 IP 位址：範圍 192.168.1.200 到 192.168.1.230

目的 IP 位址：任何的(此意思為封鎖由 192.168.1.200 到 192.168.1.230 內網往外網任何 80 埠)

9.4 網頁內容管制

VPN 防火牆的網頁內容管制可支援兩種模式的網頁管制，一為封鎖禁止訪問的網域名稱，另一個為允許訪問的網域名稱，此兩種模式只能使用一種。



封鎖禁止訪問的網域名稱

此功能需將完整的網域名稱如 www.sex.com 填入，即可封鎖此網站。

設定禁止連接的網域：	設定那些是受管制禁止訪問的網域名稱。
啟用禁止連接的網域名稱功能：	開啟網頁管制內容項目。
網域名稱：	填寫欲管制的網址，如 www.playboy.com。
加入到對應列表：	點選"增加到對應表"按鈕新增此一欲管制的網址。
刪除點選的項目：	可以使用滑鼠點選一個或多個管制的網址，然後點選即可刪除。

網頁內容過濾(關鍵字)：

啟用網頁內容過濾（關鍵字）功能：	當此項功能啟用後，當輸入網址有存在"sex"關鍵字時，則 VPN 防火牆會將所有有"sex"的網頁封鎖。
關鍵字（僅支援英文關鍵字）:	輸入關鍵字。
加入到對應列表：	增加此新增的服務項目內容到服務表列內。
刪除選中的的項目：	選擇刪除服務項目內容從服務表列內。
確定：	點選此按鈕"確定"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於"確定" 儲存動作之前才會有效。

允許訪問的網域名稱

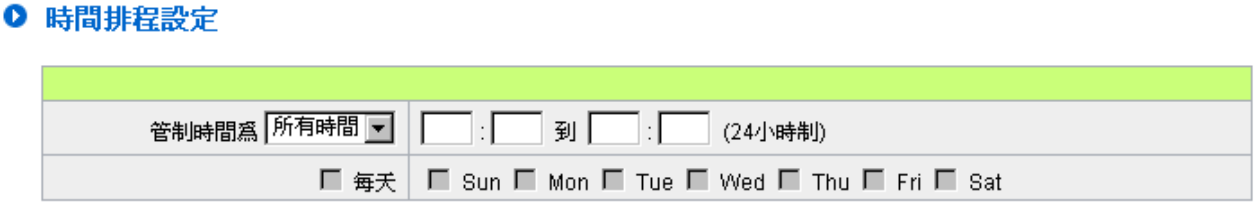
此功能的目的是設定只能去訪問的網址，在有些公司或學校中，會只允許員工或學生只能去哪些網站，就

可以用此功能來達成。

啟用允許連接的網域功能：	選擇打勾開啟允許網址管制功能，預設為關閉。
網域名稱：	填寫欲管制的允許網址，如 www.google.com。
加入到對應列表：	點選此按鈕新增此欲管制的允許網址。
刪除點選的項目：	可以使用滑鼠點選一個或多個管制的允許網址，然後點選即可刪除。

管制內容時間排程設定

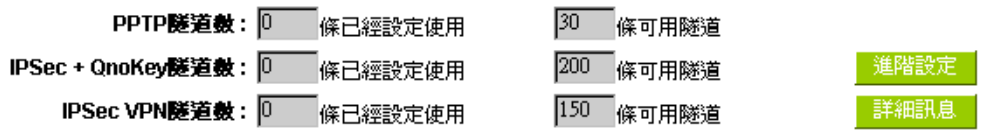
當選擇為"所有時間"時，表示此條規則 24 小時執行。若選擇"...到..."時，此管制條例會依據所設定的生效時間去執行此條規則，如管制時間為週一到週五，早上八點到下午六點，您可以參考以下圖例來管制。

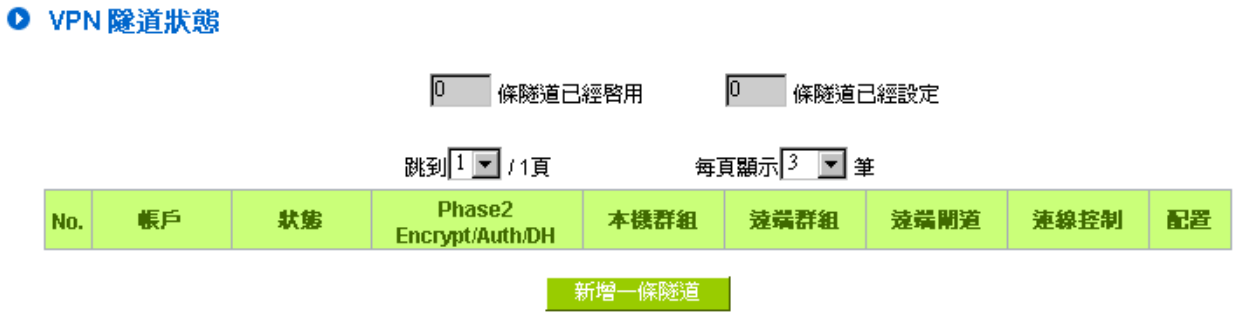


所有時間：	表示此管制規則 24 小時開啟。
…到…：	此管制規則有時間限制，設定方式為 24 小時制，如 08：00 到 18：00 (早上 8 點到下午 6 點)。
管制天數：	勾選"每天"是表示每一天的這段時間都受控管，若是只針對一星期特定星期幾，可以直接選擇星期。

十、VPN 虛擬私有網路設定

10.1. VPN 虛擬私有網路（VPN）

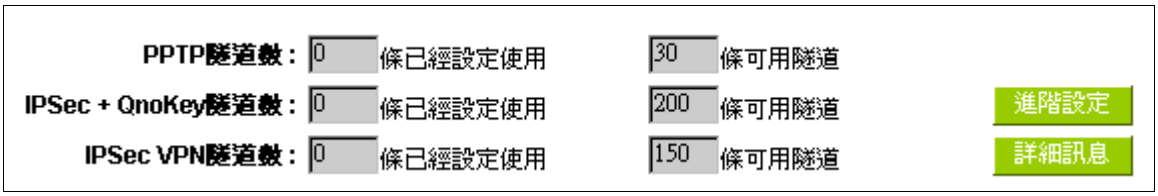




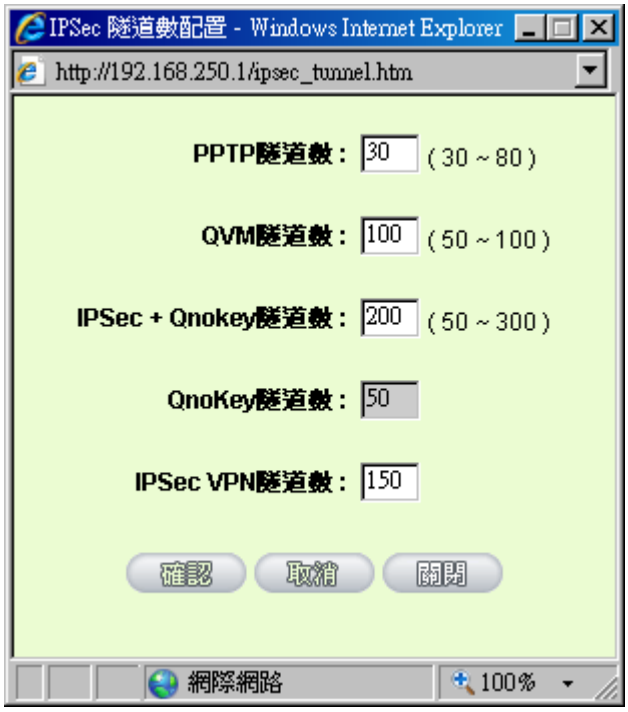
10.1.1. 目前所有的 VPN 狀態顯示

此 VPN 狀態可以顯示目前有關 VPN 方面的即時狀態，包含：所有的隧道數(PPTP/IPSec+QnoKey 、與 IPSec VPN 隧道數)，設定參數以及 GroupVPN-VPN 群組狀態等資訊。

進階設定： 使用者可以透過進階設定自行調整 IPSec 與 QnoKey 隧道數。



此為顯示目前有多少 VPN 隧道已經設定使用，還剩下多少隧道可以提供設

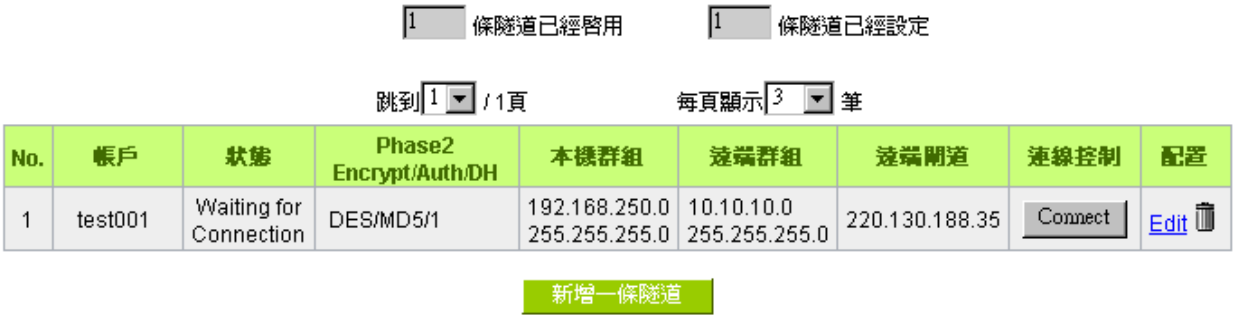


詳細資訊： 按下此詳細資訊按鈕可以顯示如以下畫面的目前所有 VPN 組態，讓用戶清楚的管理所有 VPN 連接資訊。

VPN 隧道目前狀態顯示（Tunnel Status）：

以下就針對”VPN 隧道狀態” VPN 隧道目前狀態顯示做完整解說：

VPN 隧道狀態



上一頁/下一頁、跳到 ___/___頁、每頁顯示的欄位	您可以按下上一頁與下一頁按鈕跳到您想監看的 VPN 隧道畫面上，或者您可以直接選擇每一次所顯示的頁次，來監看您的所有 VPN 隧道狀態，如(3，5，10，20，All)
Tunnel No.	當您設定 VPN 防火牆內建之 VPN 功能時，請選擇您要設定的隧道編號
狀態：	於此狀態顯示 已經連線成功-（Connected）
	電腦名稱解析失敗-（Hostname Resolution Failed）
	解析電腦名稱（Resolving Hostname）
	等待連線-（Waiting for Connection）等資訊
	若是用戶選擇手動-Manual 設定 IPSec 隧道，則此狀態會顯示手動-Manual 設定與沒有測試此項手動設定功能狀態模式
帳戶名稱：	目前連線 VPN 隧道連接名稱，如 XXX Office，建議您若是有一個以上的隧道設定的話，務必將每一個隧道名稱都設為不同，以免混淆
	注意： 此隧道名稱若是您需要連接其他 VPN 設備(非 VPN 防火牆)時，有一些設備規定此隧道名稱要與主控端為相同名稱並做驗證，此隧道才會順利連線開啟
Phase2 Encrypt/Auth/Group ：	於此顯示加密(DES/3DES)以及驗證(MD5/SHA1)以及群組 Group (1/2/5)等設定模式 若是您選擇手動(Manual)設定 IPSec 的話，於此將不會顯示 Phase 2 DH 群組

本機群組： 此為顯示本地區域端的 VPN 連線安全群組設定

遠端群組： 此為顯示遠端的 VPN 連線安全群組設定

遠端閘道： 此為設定為欲與遠端 VPN 設備連線的 IP 位址，請設定為遠端的 VPN 防火牆的對外合法 IP 位址或是網域名稱等

連線控制： 可以按下"連接"按鈕去驗證此隧道的狀態，測試結果將會更新於此狀態上，在聯通的情況下顯示"中斷"，你可以點"中斷"按鈕中斷 VPN 連接

配置： 設定項目包含編輯(Edit)以及刪除圖示

若您按下編輯(Edit) 按鈕， 將會連接到此設定的項目當中，您可以修改其中的設定。 若您選擇按下垃圾桶圖示的話， 所有此隧道的設定將會被刪除

__條隧道已經啟用、__條隧道已經設定 於此顯示已有多少條隧道已被啟用開啟以及有多少條隧道已經被設定過

群組 VPN 狀態顯示：

若您無選擇並設定群組 VPN 模式(GroupVPNs)， 此將顯示出會群組 VPN 狀態。

VPN 群組隧道狀態

群組名稱	已連線隧道	Phase2 Encrypt/Auth/DH	本機群組	遠端用戶	用戶狀態	連線控制	配置
TEST002	0	DES/MD5/1	192.168.250.0 255.255.255.0	www.qqoo.com.tw	Detail List	N/A	Edit

群組名稱： 目前設定連線 GroupVPNs 隧道連接名稱

已連線隧道： 於此顯示已經連線的 VPNGroups 隧道

Phase2 Encrypt/Auth/DH： 於此顯示加密 Encrypt(DES/3DES)以及 Auth 驗證(MD5/SHA1)以及 DH 群組(Group 1/2/5)等設定模式
若是您選擇手動(Manual)設定 IPSec 的話，於此將不會顯示 Phase 2 DH 群組

本機群組： 此為顯示本地區域端的群組 VPN 連線安全群組設定

遠端用戶端：	此為顯示此群組名稱遠端的 VPN 連線安全群組設定
用戶狀態：	若您按下更多資訊列表(Detail List) 按鈕， 此將會顯示更多有關資訊，包含群組名稱，IP 位址以及連線時間資訊等
連線控制：	可以按下連接按鈕-Connect 去驗證此隧道的狀態，測試結果將會更新於此狀態上
配置：	如下圖所示，設定項目包含編輯(Edit)以及刪除圖示 若您按下編輯(Edit)按鈕， 將會連接到此設定的項目當中，您可以修改其中的設定。 若您選擇按下垃圾桶圖示的話 ， 所有此隧道的設定將會被刪除

10.1.2. 新增一條 VPN 隧道

VPN 防火牆支持閘道對閘道隧道或用戶端對閘道隧道。

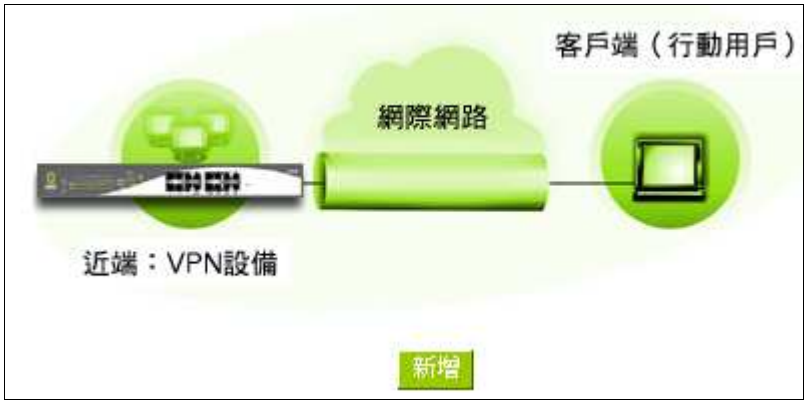
VPN 隧道連接為 2 台 VPN 防火牆，分別通過網際網路 Internet 所組成，當您按下新增一條隧道的話， 將會直接導引到 VPN 閘道對 VPN 閘道的設定或用戶端對 VPN 閘道的設定的頁面上。

閘道對閘道設定（Gateway to Gateway）：

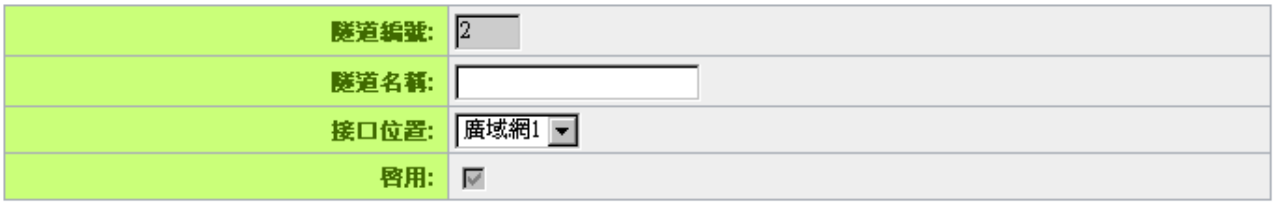
當您按下新增"新增" 的話，將會直接導引到 VPN 閘道對 VPN 閘道的設定頁面上。

用戶端對閘道(Client to Gateway)：

當您按下"新增" 的話， 將會直接導引到用戶端對 VPN 閘道的設定頁面上。



10.1.2.1. 閘道對閘道的設定



透過以下的設定說明，使用者就可以在兩台 VPN 防火牆之間建立一條 VPN 隧道。

隧道編號： 當您設定 VPN 防火牆內建之 VPN 功能時，請選擇您要設定的 Tunnel 隧道編號

隧道名稱： 設定此隧道連接名稱，如 XXX Office，建議您若是有一個以上的隧道設定的話，務必將每一個隧道名稱都設為不同，以免混淆

請注意： 此隧道名稱若是您需要連接其他 VPN 設備(非 VPN 防火牆)時，有一些設備規定此隧道名稱要與主控端為相同名稱並做驗證,此隧道才會順利連線開啟！。

VPN 接口位置： 您可以選擇哪一個接口位置做為此 VPN 隧道的節點

啟用： 勾選啟用選項，將此 VPN 隧道開啟。此項目為預設為啟用，當設定完成後，可以再選擇是否啟用隧道設定

本機用戶群組設定(Local Group Setup) ：

此項目的本機閘道認證類型(Local Security Gateway Type)必須與連接遠端的閘道認證類型(Remote Security Gateway Type)相同。

本機閘道認證類型：

本機閘道認證類型，有五種操作模式項目選擇，分別為：

僅用 IP

IP + 網域名稱(FQDN) 認證

IP + E-mail (USER FQDN) 認證

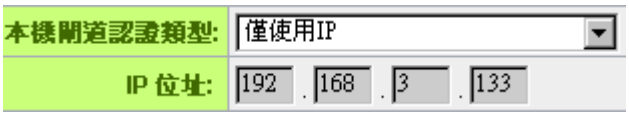
動態 IP + 網域名稱(FQDN) 認證

動態 IP + E-mail (USER FQDN) 認證

此項目的本機閘道認證類型(Local Security Gateway Type)必須與連接遠端的閘道認證類型(Remote Security Gateway Type)相同。

(1) 僅用 IP：

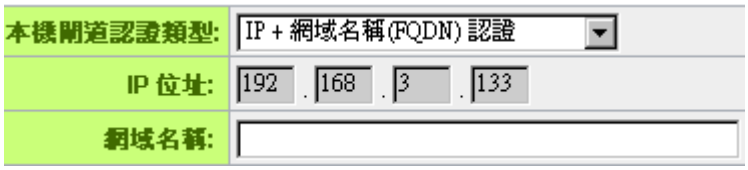
若您選擇僅用 IP 類型的話， 只有固定填入此 IP 位址可以存取此隧道，然後 VPN 防火牆的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。



(2) IP + 網域名稱(FQDN) 認證：

若您選擇 IP+網域名稱類型的話，請輸入您所驗證的網域名稱以及 IP 位址然後 VPN 防火牆的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。

FQDN 是指主機名稱以及網域名稱的結合，也必須存在於 Internet 上可以查詢的到，如 vpn.server.com。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。

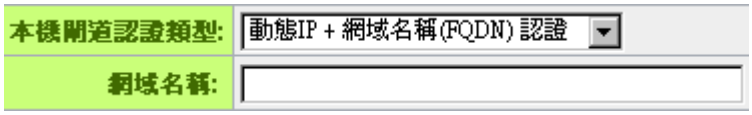


(3) IP + E-mail (USER FQDN) 認證：

若您選擇 IP 位址加上電子郵件類型的話， 只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，然後 VPN 防火牆的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。

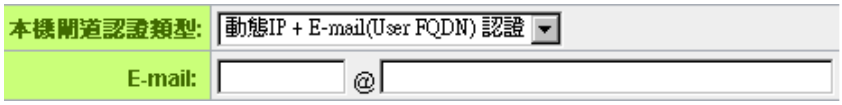
(4) 動態 IP + 網域名稱(FQDN) 認證：

若是您使用動態 IP 位址連接 VPN 防火牆時， 您可以選擇此類型連接 VPN，，當遠端的 VPN 閘道要求與 VPN 防火牆作為 VPN 連線時，VPN 防火牆將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入網域名稱即可。



(5) 動態 IP + E-mail (USER FQDN) 認證：

若是您使用動態 IP 位址連接 VPN 防火牆時， 您可以選擇此類型連接 VPN，使用者不必輸入 IP 位址，當遠端的 VPN 閘道要求與 VPN 防火牆作為 VPN 連線時， VPN 防火牆 將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入電子郵件認證到 E-Mail 位置空格欄位中即可。

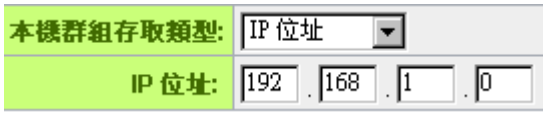


本機群組存取類型：

此為設定本地區域端的 VPN 連線存取類型，以下有幾個關於本地區域端設定的項目，請您選擇並設定適當參數：

(1) IP 位址

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 位址的本地端電腦可以連線。



以上的設定參考為：當此 VPN 隧道連線後，於 192.168.1.0 的此 IP 位址的電腦可以連線。

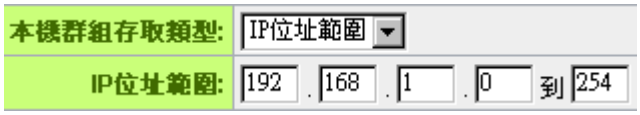
(2) 子網域

此項目為允許此 VPN 隧道連線後，每一台于此網段的本地端電腦都可以連線。

以上的設定參考為：當此 VPN 隧道連線後，只有 192.168.1.0，子網路遮罩為 255.255.255.0 的此網段電腦可以與遠端 VPN 連線。

(3) IP 位址範圍

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 範圍的本地端電腦可以連線。



以上的設定參考為：當此 VPN 隧道連線後，於 192.168.1.0~254 的此網段的 IP 位址範圍的電腦可以連線。

遠端用戶群組設定（Remote Group Setup） ：

此項目的遠端的閘道認證類型(Remote Security Gateway Type)必須與連接遠端的近端本地閘道認證類型(Local Security Gateway Type)相同。

遠程閘道認證類型：　　遠端的閘道認證類型，有五種操作模式項目選擇，分別為：

僅用 IP

IP + 網域名稱(FQDN) 認證

IP + E-mail (USER FQDN) 認證

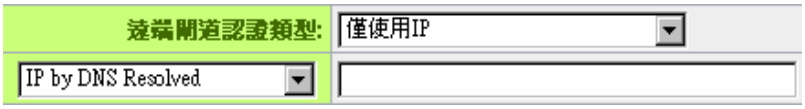
動態 IP + 網域名稱(FQDN) 認證

動態 IP + E-mail (USER FQDN) 認證

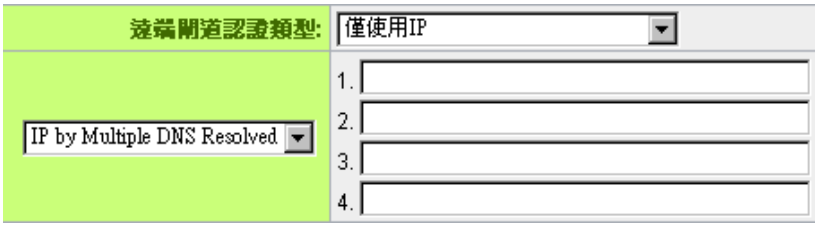
(1) 僅用 IP：

若您選擇僅用 IP 類型的話，只有固定填入此 IP 位址可以存取此隧道，

若是使用者不知道遠端客戶的 IP 位址，則可以通過名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

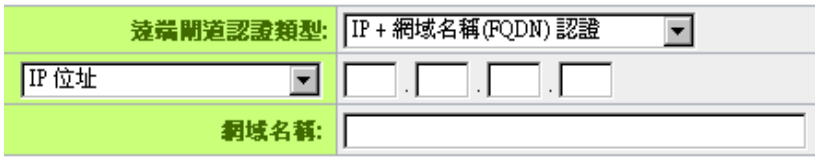


或者也可以通過 Multiple DNS Resolved 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

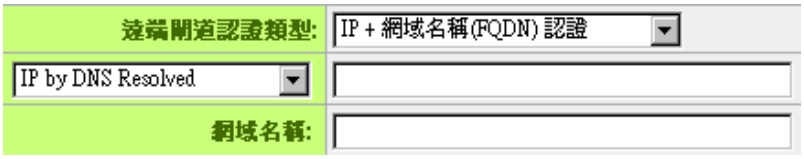


(2) IP + 網域名稱(FQDN) 認證：

若您選擇 IP+網域名稱類型的話，請輸入 IP 位址以及您所驗證的網域名稱 FQDN 是指主機名稱以及網域名稱的結合，使用者可以輸入一個符合 FQDN 的網域名稱即可。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。



若是使用者不知道遠端的 IP 位址，則可以通過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。此網域名稱必須存在 Internet 上可以查詢的到。並且在設定完成後在 Summary 的遠端閘道下面自動顯示出相對應的 IP 位址



或者也可以通過 Multiple DNS Resolved 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址

(3) IP + E-mail(USER FQDN) 認證：

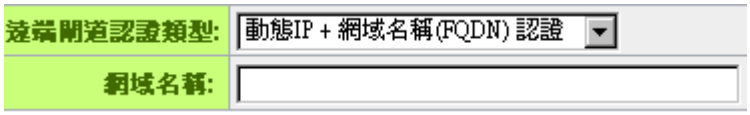
若您選擇 IP 位址加上電子郵件類型的話，只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，

若是使用者不知道遠端客戶的 IP 位址，則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

或者也可以通過 Multiple DNS Resolved 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

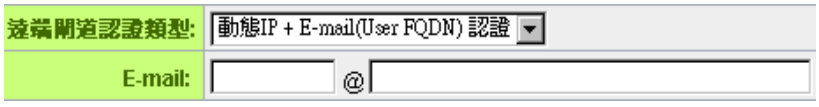
(4) 動態 IP + 網域名稱(FQDN) 認證：

若是您使用動態 IP 位址連接 VPN 防火牆時，您可以選擇動態 IP 位址加上主機名稱以及網域名稱的結合。



(5) 動態 IP + E-mail (USER FQDN) 認證：

若是您使用動態 IP 位址連接 VPN 防火牆時， 您可以選擇此類型連接 VPN，當遠端的 VPN 閘道要求與 VPN 防火牆作為 VPN 連線時，VPN 防火牆 將會開始驗證並回應此 VPN 隧道連線; 請輸入電子郵件認證到 E-Mail 位置空格欄位中。

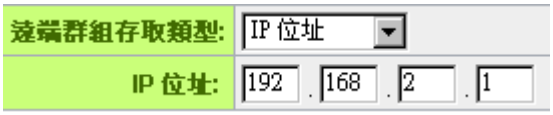


遠端群組存取類型：

此為設定遠端端的 VPN 連線存取類型，以下有幾個關於遠端端設定的項目，請您選擇並設定適當參數：

(1) IP 位址

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 位址的本地端電腦可以連線。



以上的設定參考為：當此 VPN 隧道連線後，於 192.168.2.1 的此 IP 位址範圍的電腦可以連線。

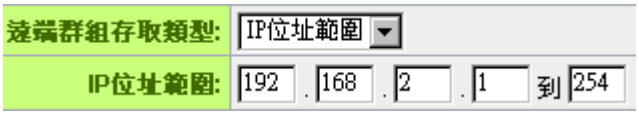
(2)子網域

此項目為允許此 VPN 隧道連線後，每一台于此網段的本地端電腦都可以連線。

以上的設定參考為：當此 VPN 隧道連線後，只有 192.168.2.0，子網路遮罩為 255.255.255.0 的此網段電腦可以與遠端 VPN 連線

(3)IP 位址範圍

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 位址範圍的本地端電腦可以連線



以上的設定參考為：當此 VPN 隧道連線後，只有 192.168.2.1 到 192.168.2.254 的 IP 位址範圍的電腦可以連線。

IPSec Setup

若是任何加密機制存在的話，此兩個 VPN 隧道的加密機制必須要相同才可以將此隧道連接，並於傳輸資料中加上標準的 IPSec 密鑰，我們稱為加密密鑰 "key"。VPN 防火牆提供了以下二種加密管理模式 Key Management，分別為手動(Manual) 以及 IKE 協議自動加密模式- IKE with Preshared Key

(automatic)，你可以通過下拉功能表選擇需要的加密模式如下圖所示。

密鑰管理協議：

此選項設定為當您設定此 VPN 隧道使用何種加密模式以及驗證模式後，必須設定一組交換密碼，並請注意此參數必須與遠端的交換密碼參數相同;設定的方式有自動 Auto (IKE)或是手動 Manual 設定二種，於設定時請您選擇其中一種設定方式即可！

IPSec 設定

密鑰管理協議:	使用IKE協議
階段1 DH協議群組:	群組1
階段1 加密演算法:	DES
階段1 認證演算法:	MD5
階段1 SA有效時間:	28800 秒
完全順向密鑰(PFS)	☑
階段2 DH協議群組:	群組1
階段2 加密演算法:	DES
階段2 認證演算法:	MD5
階段2 SA有效時間:	3600 秒
共用密鑰:	

進階設定 -

使用 IKE 協定：

透過 IKE 產生共用的金鑰來加密與驗證遠端的使用者。若將完全順向密鑰 PFS(Perfect Forward Secrecy)啟用後，則會再第二階段的 IKE 協調過程產生的第二把共同金鑰做進一步加密與驗證。當 PFS 啟用後，透過 brute force 來擷取金鑰的駭客(hacker)無法在此短時間內，進一步得到第二把金鑰。

- 完全順向密鑰(Perfect Forward Secrecy)：若您將 PFS 選項勾選後，記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啟。
- 階段 1/階段 2 DH 協議群組：於此選項可以選擇採用 Diffie-Hellman 群組方式： Group1 或是 Group2/Group5。
- 階段 1/階段 2 加密演算法：此加密選項設定為設定此 VPN 隧道使用何種加密模式，並請注意設定此參數必須與遠端的加密參數相同：DES：64-位元元加密模式、3DES：128-位元元加密模式、AES：用安全碼進行資訊加密的標準，它支持 128 位、192 位和 256 位的密匙。
- 階段 1/階段 2 認證演算法：此驗證選項設定為設定此 VPN 隧道使用何種驗證模式，並請注意設定此參數必須與遠端的驗證模式參數相同："MD5"或"SHA1"。
- 階段 1 SA 有效時間：為此交換密碼的有效時間，系統預設值為 28800 秒(8 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全。
- 階段 2 SA 有效時間：為此交換密碼的有效時間，系統預設值為 3600 秒(1 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全
- 共用密鑰：於 Auto (IKE) 選項中，您必須輸入一組交換密碼於 "Pre-shared Key" 的欄位中，

在此的範例設定為 test，您可以輸入數位元或是文字的交換密碼，系統將會自動的將您輸入的數位元或是文字的交換密碼自動轉成 VPN 隧道連接時的交換密碼與驗證機制;此數位元或是文字的交換密碼最高可輸入 30 個文字組合。

Manual-手動輸入

IPSec 設定

密鑰管理協議:	手動輸入
Incoming SPI:	
Outgoing SPI:	
加密演算法:	DES
認證演算法:	MD5
加密密鑰:	
認證密鑰:	

若您選擇手動模式 Manual 的話，此提供您自定加密密鑰，而此密鑰不需經過任何交握。

- 於此分成加密密鑰"Encryption KEY"以及認證密鑰"Authentication KEY"二種，您可以輸入數位元或是文字的交換密碼，系統將會自動的將您輸入的數位元或是文字的交換密碼自動轉成 VPN 隧道連接時的交換密碼與驗證機制;此數位元或是文字的交換密碼最高可輸入 23 個文字組合。
- 另外還需要設定"Incoming SPI"的交換字串以及"Outgoing SPI" 交換字串，此字串必須與遠端 VPN 設備連接時相同;於此的 Incoming SPI 設定參數，您必須在遠端的 VPN 設備的 Outgoing SPI 設定相同字串，而於本地端的 Outgoing SPI 設定字串，也必須與在遠端的 VPN 設備的 Incoming SPI 設定相同字串！

進階設定-只供給使用 IKE 協定使用

在 VPN 防火牆的進階設定項目中，分別有 Main 以及 Aggressive 模式，Main mode 是 VPN 防火牆的預設 VPN 作業模式，而且與大多數的其他 VPN 設備使用連接方式為相同。

- Aggressive Mode：大多為遠端的設備採用，如使用動態 IP 連接時，是為了加強其安全控管機制。
- 使用 IP Header 壓縮協定：若選擇此項目勾選，則連接的 VPN 隧道中 VPN 防火牆 支援 IP 表頭形態的壓縮(IP Payload compression Protocol)。
- 持續保持連線：若選擇此項目勾選，則連接的 VPN 隧道中會持續保持此條 VPN 連接不會中斷，此使用多為分公司遠端節點對總部的連接使用，或是無固定 IP 位址的遠端使用。
- AH 雜湊演算法：AH (Authentication Header) 驗證表頭封包格式，可選擇 MD5/DSHA-1。
- 允許 NetBIOS 廣播封包通過：若選擇此項目勾選，則連接的 VPN 隧道中會讓 NetBIOS 廣播封包通過。，有助於微軟的網路鄰居等連接容易，但是相對的佔用此 VPN 隧道的流量就會加大！
- 允許穿越 NAT：允許 VPN 可以穿透位於路由器前方的 NAT 機制
- 掉線偵測功能(DPD)：若選擇此項目勾選，則連接的 VPN 隧道中會定期的傳送 HELLO/ACK 訊息封包來偵測是否 VPN 隧道的兩端仍有連線存在。當有一端斷線則 VPN 防火牆會自動斷線，然後再建立新連線。使用者可以選擇每一次 DPD 訊息封包傳遞的時間，預設值為 10 秒。

10.1.2.2. 用戶端對閘道的設定

透過以下的設定說明，管理人員就可以在用戶端與 VPN 防火牆之間建立一條 VPN 隧道。

用戶可以選擇這一條 VPN 隧道在用戶端是只供一個客戶所使用(Tunnel)或者是由一群客戶所使用(Group VPN)。若由一群客戶所使用則可以節省個別設定遠端的客戶，只需設定的一條隧道供一組客戶所使用，以節省設定時的麻煩。

（1） 在隧道模式（Tunnel）的情況：

隧道編號： 當您設定 VPN 防火牆內建之 VPN 功能時，請選擇您要設定的 Tunnel 隧道編號。

隧道名稱： 設定此隧道連接名稱，如 XXX Office，建議您若是有一個以上的隧道設定的話，務必將每一個隧道名稱都設為不同，以免混淆

請注意： 此隧道名稱若是您需要連接其他 VPN 設備時，有一些設備規定此隧道名稱要與主控端為相同名稱並做驗證，此隧道才會順利連線開啟！。

VPN 接口位置： 您可以選擇哪一個接口位置做為此 VPN 隧道的節點

啟用： 勾選啟用 選項，將此 VPN 隧道開啟。 此項目為預設為啟用，當設定完成後可以再選擇是否啟用隧道設定。

本機用戶群組設定(Local Group Setup)

此項目的本機閘道認證類型(Local Security Gateway Type)必須與連接遠端的閘道認證類型(Remote Security Gateway Type)相同。

本機閘道認證類型：

本機閘道認證類型，有五種操作模式項目選擇，分別為：
僅用 IP

IP + 網域名稱(FQDN) 認證
IP + E-mail (USER FQDN) 認證

動態 IP + 網域名稱(FQDN) 認證

動態 IP + E-mail(USER FQDN) 認證

此項目的本機閘道認證類型(Local Security Gateway Type)必須與連接遠端的閘道認證類型(Remote Security Gateway Type)相同。

(1) 僅用 IP：

若您選擇僅用 IP 類型的話， 只有固定填入此 IP 位址可以存取此隧道，然後 VPN 防火牆的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。

(2) IP + 網域名稱(FQDN) 認證：

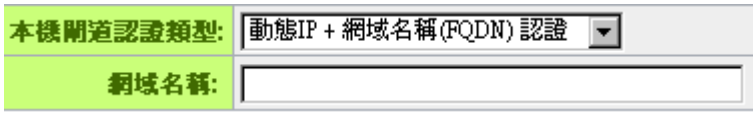
若您選擇 IP+網域名稱類型的話，請輸入您所驗證的網域名稱以及 IP 位址然後 VPN 防火牆的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。 FQDN 是指主機名稱以及網域名稱的結合，也必須存在於 Internet 上可以查詢的到，如 vpn.server.com。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。

(3) IP + E-mail(USER FQDN) 認證：

若您選擇 IP 位址加上電子郵件類型的話， 只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，然後 VPN 防火牆的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。

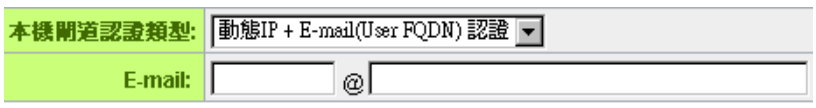
(4) 動態 IP + 網域名稱(FQDN) 認證：

若是您使用動態 IP 位址連接 VPN 防火牆時， 您可以選擇此類型連接 VPN， ，當遠端的 VPN 閘道要求與 VPN 防火牆作為 VPN 連線時， VPN 防火牆 將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入網域名稱即可。



(5) 動態 IP + E-mail (USER FQDN) 認證：

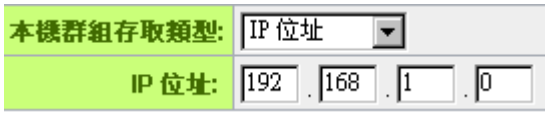
若是您使用動態 IP 位址連接 VPN 防火牆時， 您可以選擇此類型連接 VPN，使用者不必輸入 IP 位址，當遠端的 VPN 閘道要求與 VPN 防火牆作為 VPN 連線時， VPN 防火牆 將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入電子郵件認證到 E-Mail 位置空格欄位中即可。



本機群組存取類型： 此為設定本地區域端的 VPN 連線存取類型，以下有幾個關於本地區域端設定的項目，請您選擇並設定適當參數：

(1)IP 位址

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 位址的本地端電腦可以連線。



以上的設定參考為：當此 VPN 隧道連線後，於 192.168.1.0 的此 IP 位址的電腦可以連線。

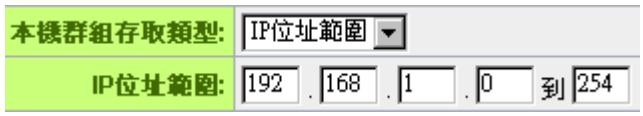
(2)子網域

此項目為允許此 VPN 隧道連線後，每一台于此網段的本地端電腦都可以連線。

以上的設定參考為：當此 VPN 隧道連線後，只有 192.168.1.0，子網路遮罩為 255.255.255.0 的此網段電腦可以與遠端 VPN 連線。

(3)IP 位址範圍

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 範圍的本地端電腦可以連線。



以上的設定參考為:當此 VPN 隧道連線後,於 192.168.1.0~254 的此網段的 IP 位址範圍的電腦可以連線。

遠端用戶群組設定（Remote Group Setup）：

此項目的遠端的閘道認證類型(Remote Security Gateway Type)必須與連接遠端的近端本地閘道認證類型(Local Security Gateway Type)相同。

遠程的閘道認證類型：

遠端的閘道認證類型，有五種操作模式項目選擇，分別為：

僅用 IP

IP + 網域名稱(FQDN) 認證

IP + E-mail (USER FQDN) 認證

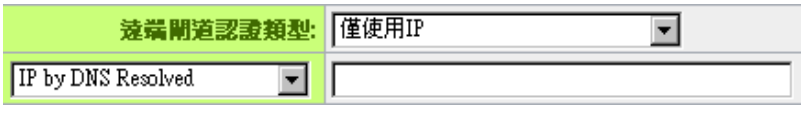
動態 IP + 網域名稱(FQDN) 認證

動態 IP + E-mail (USER FQDN) 認證

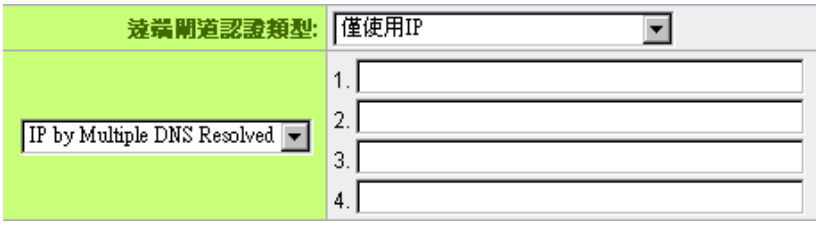
(1) 僅用 IP：

若您選擇僅用 IP 類型的話，只有固定填入此 IP 位址可以存取此隧道，

若是使用者不知道遠端客戶的 IP 位址，則可以通過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

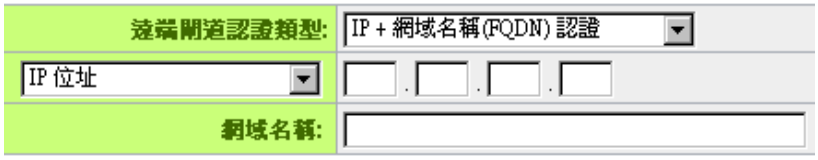


或者也可以通過 Multiple DNS Resolved 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

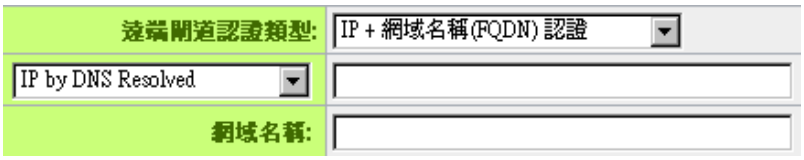


(2) IP + 網域名稱(FQDN) 認證：

若您選擇 IP+網域名稱類型的話，請輸入 IP 位址以及您所驗證的網域名稱 FQDN 是指主機名稱以及網域名稱的結合，使用者可以輸入一個符合 FQDN 的網域名稱即可。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。



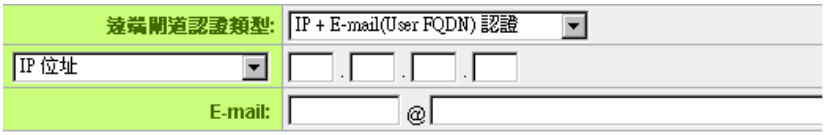
若是使用者不知道遠端的 IP 位址，則可以通過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。此網域名稱必須存在 Internet 上可以查詢的到。並且在設定完成後在 Summary 的遠端閘道下面自動顯示出相對應的 IP 位址。



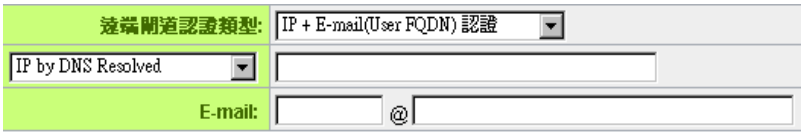
或者也可以通過 Multiple DNS Resolved 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

(3) IP + E-mail (USER FQDN) 認證：

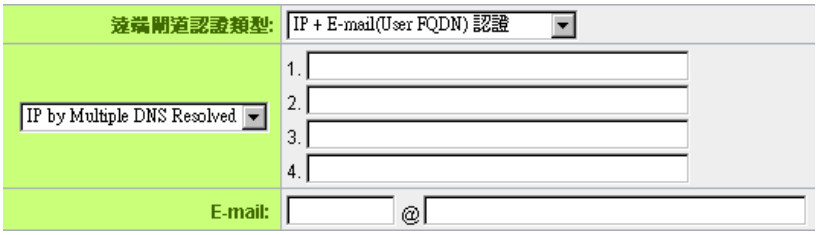
若您選擇 IP 位址加上電子郵件類型的話，只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，



若是使用者不知道遠端客戶的 IP 位址，則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

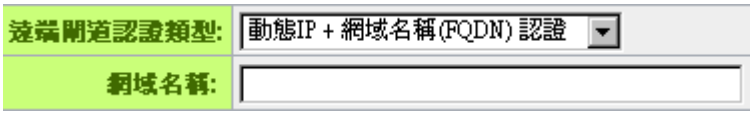


或者也可以通過 Multiple DNS Resolved 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。



(4) 動態 IP + 網域名稱(FQDN) 認證：

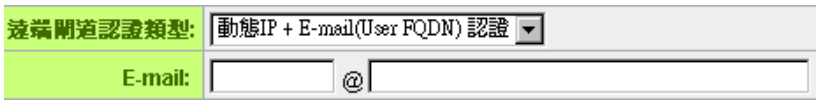
若是您使用動態 IP 位址連接 VPN 防火牆時，您可以選擇動態 IP 位址加上主機名稱以及網域名稱的結合。



(5) 動態 IP + E-mail (USER FQDN) 認證：

若是您使用動態 IP 位址連接 VPN 防火牆時， 您可以選擇此類型連接 VPN，當遠端的 VPN 閘道要求與 VPN 防火牆作為 VPN 連線時，VPN 防火牆 將會開始驗證並回應此 VPN 隧道連線; 請輸入電子郵

件認證到 E-Mail 位置空格欄位中。



IPSec Setup

IPSec 設定

若是任何加密機制存在的話，此兩個 VPN 隧道的加密機制必須要相同才可以將此隧道連接，並於傳輸資料中加上標準的 IPSec 密鑰，於此我們稱為加密密鑰 "key"。VPN 防火牆提供了以下二種加密管理模式，分別為手動(Manual) 以及 IKE 協議自動加密模式- IKE with Preshared Key (automatic) 如下圖所示。

密鑰管理協議：

此選項設定為當您設定此 VPN 隧道使用何種加密模式以及驗證模式後，必須設定一組交換密碼，並請注意此參數必須與遠端的交換密碼參數相同;設定的方式有自動 Auto (IKE)或是手動 Manual 設定二種，於設定時請您選擇其中一種設定方式即可！

IPSec 設定

密鑰管理協議:	使用IKE協議
階段1 DH協議群組:	群組1
階段1 加密演算法:	DES
階段1 認證演算法:	MD5
階段1 SA有效時間:	28800 秒
完全順向密鑰(PFS)	☑
階段2 DH協議群組:	群組1
階段2 加密演算法:	DES
階段2 認證演算法:	MD5
階段2 SA有效時間:	3600 秒
共用密鑰:	

進階設定 +

使用 IKE 協定：

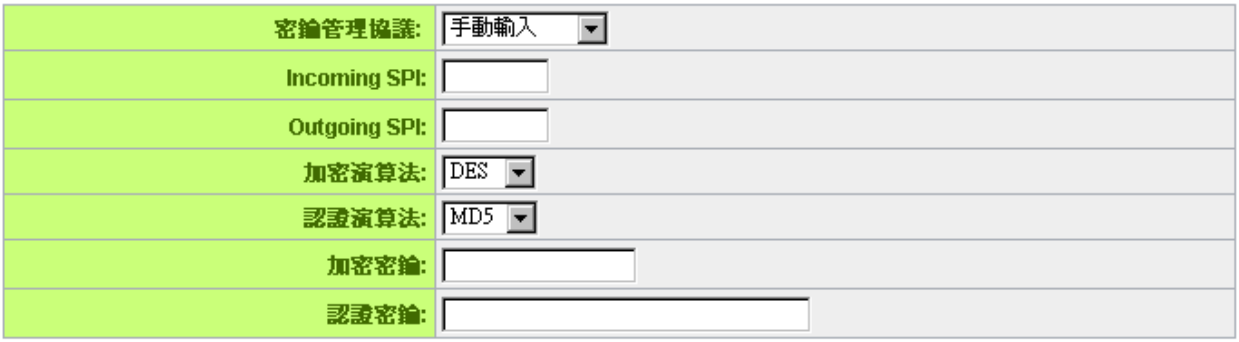
透過 IKE 產生共用的金鑰來加密與驗證遠端的使用者。若將完全順向密鑰 PFS(Perfect Forward Secrecy)啟用後，則會再第二階段的 IKE 協調過程產生的第二把共同金鑰做進一步加密與驗證。當 PFS 啟用後，透過 brute force 來擷取金鑰的駭客(hacker)無法在此短時間內，進一步得到第二把金鑰。

- 完全順向密鑰(Perfect Forward Secrecy)：若您將 PFS 選項勾選後，記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啟。
- 階段 1/階段 2 DH 協議群組：於此選項可以選擇採用 Diffie-Hellman 群組方式： Group1 或是 Group2/Group5。
- 階段 1/階段 2 加密演算法：此加密選項設定為設定此 VPN 隧道使用何種加密模式，並請注意設定此參數必須與遠端的加密參數相同：DES：64-位元元加密模式、3DES：128-位元元加密模式、AES：用安全碼進行資訊加密的標準，它支持 128 位、192 位和 256 位的密匙。
- 階段 1/階段 2 認證演算法：此驗證選項設定為設定此 VPN 隧道使用何種驗證模式，並請注意設定此參數必須與遠端的驗證模式參數相同："MD5"或"SHA1"。
- 階段 1 SA 有效時間：為此交換密碼的有效時間，系統預設值為 28800 秒(8 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全。
- 階段 2 SA 有效時間：為此交換密碼的有效時間，系統預設值為 3600 秒(1 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全

- 共用密鑰：於 Auto (IKE) 選項中，您必須輸入一組交換密碼於 "Pre-shared Key" 的欄位中，在此的範例設定為 test，您可以輸入數位元或是文字的交換密碼，系統將會自動的將您輸入的數位元或是文字的交換密碼自動轉成 VPN 隧道連接時的交換密碼與驗證機制;此數位元或是文字的交換密碼最高可輸入 30 個文字組合。

Manual-手動輸入

IPSec 設定



若您選擇手動模式 Manual 的話，此提供您自定加密密鑰，而此密鑰不需經過任何交握。

- 於此分成加密密鑰"Encryption KEY"以及認證密鑰"Authentication KEY"二種，您可以輸入數位元或是文字的交換密碼，系統將會自動的將您輸入的數位元或是文字的交換密碼自動轉成 VPN 隧道連接時的交換密碼與驗證機制;此數位元或是文字的交換密碼最高可輸入 23 個文字組合。
- 另外還需要設定"Incoming SPI"的交換字串以及"Outgoing SPI" 交換字串，此字串必須與遠端 VPN 設備連接時相同;於此的 Incoming SPI 設定參數，您必須在遠端的 VPN 設備的 Outgoing SPI 設定相同字串，而於本地端的 Outgoing SPI 設定字串，也必須與在遠端的 VPN 設備的 Incoming SPI 設定相同字串！

Advanced(進階作業模式)-只供給使用自動交換密鑰模式使用(IKE Preshareed Key Only)

在 VPN 防火牆 的進階設定項目中，分別有 Main 以及 Aggressive。模式，Main mode 是 VPN 防火牆的預設 VPN 作業模式，而且與大多數的其他 VPN 設備使用連接方式為相同。

- Aggressive Mode：大多為遠端的設備採用，如使用動態 IP 連接時，是為了加強其安全控管機制。
- 使用 IP Header 壓縮協定：若選擇此項目勾選，則連接的 VPN 隧道中 VPN 防火牆 支援 IP 表頭形態的壓縮(IP Payload compression Protocol)。
- 持續保持連線：若選擇此項目勾選，則連接的 VPN 隧道中會持續保持此條 VPN 連接不會中斷，此使用多為分公司遠端節點對總部的連接使用，或是無固定 IP 位址的遠端使用。
- AH 雜湊演算法：AH (Authentication Header) 驗證表頭封包格式，可選擇 MD5/DSHA-1。
- 允許 NetBIOS 廣播封包通過：若選擇此項目勾選，則連接的 VPN 隧道中會讓 NetBIOS 廣播封包通過。，有助於微軟的網路鄰居等連接容易，但是相對的佔用此 VPN 隧道的流量就會加大！
- 允許穿越 NAT：允許 VPN 可以穿透位於路由器前方的 NAT 機制
- 掉線偵測功能(DPD)：若選擇此項目勾選，則連接的 VPN 隧道中會定期的傳送 HELLO/ACK 訊息封包來偵測是否 VPN 隧道的兩端仍有連線存在。當有一端斷線則 VPN 防火牆會自動斷線，然後再建立新連線。使用者可以選擇每一次 DPD 訊息封包傳遞的時間，預設值為 10 秒。

（2） 在 Group VPN 的情況：

群組編號： 最多可以設定兩組 Group VPN。

群組名稱： 設定此隧道連接名稱，如 XXX Office，建議您若是有一個以上的隧道設定的話，務必將每一個隧道名稱都設為不同，以免混淆。

請注意： 此隧道名稱若是您需要連接其他 VPN 設備(非 VPN 防火牆)時，有一些設備規定此隧道名稱要與主控端為相同名稱並做驗證，此隧道才會順利連線開啟！。

接口位置： 您可以選擇哪一個接口位置做為此 VPN 隧道的節點

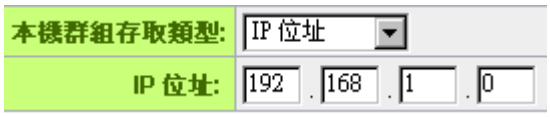
啟用： 勾選啟用 選項，將此 VPN 隧道開啟。 此項目為預設為啟用 Eanble，當設定完成後可以再選擇是否啟用隧道設定。

本機用戶群組設定：

本機群組存取類型： 此為設定本地區域端的 VPN 用戶群組類型，以下有幾個關於本地區域端設定的項目，請您選擇並設定適當參數：

(1) IP 位址

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 位址的本地端電腦可以連線。



以上的設定參考為：當此 VPN 隧道連線後，於 192.168.1.0 的 IP 位址範圍的電腦可以連線。

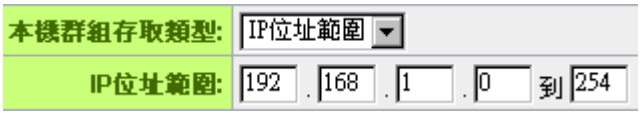
(2) 子網域

此項目為允許此 VPN 隧道連線後，每一台于此網段的本地端電腦都可以連線。

以上的設定參考為：當此 VPN 隧道連線後，只有 192.168.1.0，子網路遮罩為 255.255.255.0 的此網段電腦可以與遠端 VPN 連線。

(3) IP 位址範圍

此項目為允許此 VPN 隧道連線後，只有輸入此 IP 範圍的本地端電腦可以連線。



以上的設定參考為:當此 VPN 隧道連線後,於 192.168.1.0~254 的此網段的 IP 位址範圍的電腦可以連線。

遠端用戶群組設定

遠端用戶認證類型：　遠端用戶端設定，有三種操作模式項目選擇，分別為：

Domain Name(FQDN)：網域名稱

E-mail Address(USER FQDN)：電子郵件名稱

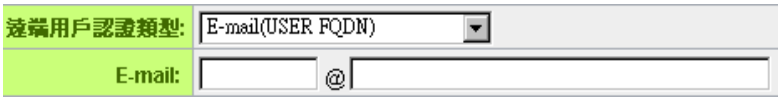
Microsoft XP/2000 VPN Client：微軟 XP/2000 VPN 用戶端

(1) Domain Name(FQDN)：網域名稱

若您選擇網域名稱類型的話，請輸入您所驗證的網域名稱。FQDN 是指主機名稱以及網域名稱的結合，也必須存在於 Internet 上可以查詢的到，如 vpn.Server.com。此網域名稱必須與用戶端的近端設定形態相同才可以正確連接。

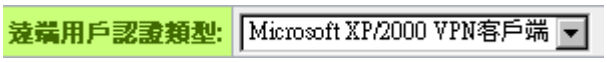
(2) E-mail (USER FQDN)： 電子郵件名稱

若您選擇電子郵件類型的話， 只有固定填入此電子郵件位置可以存取此隧道。



(3) Microsoft XP/2000 VPN Client： 微軟 XP/2000 VPN 用戶端

若您選擇微軟 XP/2000 VPN 用戶端形態的話，您不需要在進行額外設定。



IPSec Setup

若是任何加密機制存在的話，此兩個 VPN 隧道的加密機制必須要相同才可以將此隧道連接，並於傳輸資料中加上標準的 IPSec 密鑰，於此我們稱為加密密鑰 “key”。VPN 防火牆提供了以下二種加密管理模式，分別為手動(Manual) 以及 IKE 自動加密模式- IKE with Preshared Key (automatic)。

在選擇 Group VPN 的情況之下或者是在遠端閘道安全形態 Remote Security Gateway Type 中使用動態位置 IP 時，Aggressive Mode 會自動啟用，沒有手動 Manual 模式。

密鑰管理協定：

IPSec 設定

密鑰管理協議:	使用IKE協議
階段1 DH協議群組:	群組1
階段1 加密演算法:	DES
階段1 認證演算法:	MD5
階段1 SA有效時間:	28800 秒
完全順向密鑰(PFS)	☑
階段2 DH協議群組:	群組1
階段2 加密演算法:	DES
階段2 認證演算法:	MD5
階段2 SA有效時間:	3600 秒
共用密鑰:	

進階設定 +

- 完全順向密鑰(Perfect Forward Secrecy)：若您將 PFS 選項勾選後，記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啟。
- 階段 1/階段 2 DH 協議群組：於此選項可以選擇採用 Diffie-Hellman 群組方式： Group1 或是 Group2/Group5。
- 階段 1/階段 2 加密演算法：此加密選項設定為設定此 VPN 隧道使用何種加密模式，並請注意設定此參數必須與遠端的加密參數相同：DES：64-位元元加密模式、3DES：128-位元元加密模式、AES：用安全碼進行資訊加密的標準，它支持 128 位、192 位和 256 位的密匙。
- 階段 1/階段 2 認證演算法：此驗證選項設定為設定此 VPN 隧道使用何種驗證模式，並請注意設定此參數必須與遠端的驗證模式參數相同："MD5"或"SHA1"。
- 階段 1 SA 有效時間：為此交換密碼的有效時間，系統預設值為 28800 秒(8 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全。
- 階段 2 SA 有效時間：為此交換密碼的有效時間，系統預設值為 3600 秒(1 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全
- 共用密鑰：於 Auto (IKE) 選項中，您必須輸入一組交換密碼於 "Pre-shared Key" 的欄位中，在此的範例設定為 test，您可以輸入數位元或是文字的交換密碼，系統將會自動的將您輸入的數位元或是文字的交換密碼自動轉成 VPN 隧道連接時的交換密碼與驗證機制;此數位元或是文字的交換密碼最高可輸入 30 個文字組合。

進階設定-只供給使用 IKE 協定使用(IKE Preshareed Key Only)

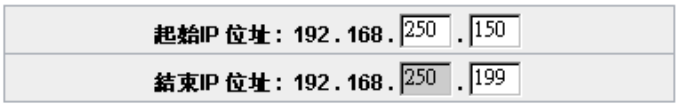
在 VPN 防火牆的進階設定項目中，分別有 Main 以及 Aggressive 模式，Main mode 是 VPN 防火牆的預設 VPN 作業模式，而且與大多數的其他 VPN 設備使用連接方式為相同。

- Aggressive Mode：大多為遠端的設備採用，如使用動態 IP 連接時，是為了加強其安全控管機制。
- 使用 IP Header 壓縮協定：若選擇此項目勾選，則連接的 VPN 隧道中 VPN 防火牆支援 IP 表頭形態的壓縮(IP Payload compression Protocol)。
- 持續保持連線：若選擇此項目勾選，則連接的 VPN 隧道中會持續保持此條 VPN 連接不會中斷，此使用多為分公司遠端節點對總部的連接使用，或是無固定 IP 位址的遠端使用。
- AH 雜湊演算法：AH (Authentication Header) 驗證表頭封包格式，可選擇 MD5/DSHA-1。
- 允許 NetBIOS 廣播封包通過：若選擇此項目勾選，則連接的 VPN 隧道中會讓 NetBIOS 廣播封包通過。，有助於微軟的網路鄰居等連接容易，但是相對的佔用此 VPN 隧道的流量就會加大！
- 允許穿越 NAT：允許 VPN 可以穿透位於路由器前方的 NAT 機制
- 掉線偵測功能(DPD)：若選擇此項目勾選，則連接的 VPN 隧道中會定期的傳送 HELLO/ACK 訊息封包來偵測是否 VPN 隧道的兩端仍有連線存在。當有一端斷線則 VPN 防火牆會自動斷線，然後再建立新連線。使用者可以選擇每一次 DPD 訊息封包傳遞的時間，預設值為 10 秒

10.1.3. PPTP 設定

提供支援 Window XP/2000 的 PPTP 對我們 VPN 防火牆做點對點隧道協議，讓遠端單機用戶使用此種協定建立 VPN 連線。

PPTP 用戶使用IP範圍



遠端用戶設定

啟用 PPTP 伺服器： 當使用者勾選後即可以啟用點對點隧道協定 PPTP 伺服器

PPTP 用戶使用 IP 範圍： 請輸入近端 PPTP IP 位址的範圍，其目的是要給遠端的使用者一個可進入近端網路的入口 IP。輸入起始範圍 Range Start：請在最後一欄

輸入數值。輸入結束範圍 Range End： 請在最後一欄數入數值

使用者名稱： 請輸入遠端使用者的名稱

密碼的輸入與確認： 輸入使用者帳號密碼及請再次確認輸入遠端使用者新的帳號密碼

加入到對應列表： 新增輸入的帳號與密碼

刪除點選的項目： 刪除用戶

所有的 PPTP 通道狀態：顯示所有連接成功的用戶，包括使用者名稱、遠端 IP 位址和 PPTP 發放的位址

PPTP 用戶連線列表

使用者名稱	遠端用戶的IP 位址	本機對映的IP 位址
PM001	192.168.250.100	192.168.250.150

重新整理

10.1.4. 封包穿透路由器功能（VPN Pass Through）

IPSec 封包穿透功能：	若是選擇啟用的話，則允許 PC 端使用 VPN- IPSec 封包穿透 VPN 防火牆以便與外部 VPN 設備連線
固定來源埠 或 變更來源埠：	在 VPN 連線是以 Cisco VPN Server 與 Cisco VPN Client 的狀況下才有需要用的此選項，因為 VPN Server 不接受先後兩筆用同一個 IP 位址以及同一個 Source Port 的第二筆連線，所以第二筆連線需要變更 Source Port，此時就需要選擇 Change Source Port 將原來以 UDP 500 的 Source Port 改成另外隨機的 Source Port 連線，選擇 Fixed 代表不變更 Source Port 仍以 UDP 500 連線
PPTP 封包穿透 VPN 防火牆功能：	若是選擇啟用 的話，則允許 PC 端使用 VPN-PPTP 封包穿透 VPN 防火牆以便與外部 VPN 設備連線。
L2TP 封包穿透 VPN 防火牆功能：	若是選擇啟用 的話，則允許 PC 端使用 VPN-L2TP 封包穿透 VPN 防火牆以便與外部 VPN 設備連線。

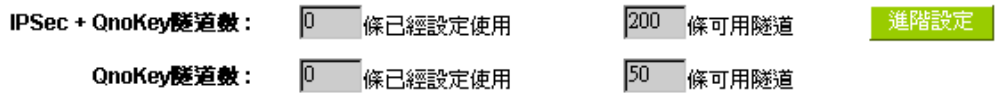
設定修改完成請按下“確定”按鈕儲存網路設定變更或是按下“取消”按鈕不做任何設定變更。

10.2. QnoKey

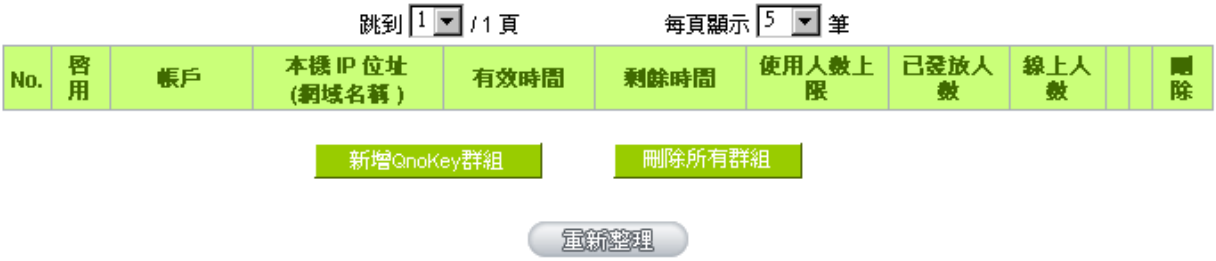
介紹 Qno VPN 防火牆進行用戶端資料的初始設定以及配合 QnoKey 管理軟體如何設定 QnoKey 用戶端，成功燒制 QnoKey。

10.2.1. QnoKey 總表頁面

登錄 VPN 防火牆後，點開 QnoKey 功能表選項，將出現目前 QnoKey 狀態資訊摘要總表頁面，如下圖所示：



QnoKey 用戶連線列表



IPSec+QnoKey 隧道數	顯示 IPsec+QnoKey 總共隧道數。表示有幾條已經設定使用，以及目前總隧道數。
QnoKey 隧道數	表示有幾條已經設定使用，以及目前總隧道數。使用者可以透過進階設定自行調整 IPSec 與 QnoKey 隧道數。
啟用：	表示 QnoKey 用戶名稱是否啟用狀態
帳戶：	顯示 QnoKey 的用戶名稱群組
本機 IP 位址(網域名稱)	伺服器 IP 位址或所使用的網域名稱
有效時間：	所設定的 QnoKey 的使用期限,永久使用則會在此顯示永久
剩餘時間：	如設定 QnoKey 使用天數，則在此顯示設定後還可使用的有效剩餘時間
使用人數上限：	表示此用戶名稱群組設定可以允許燒制的 QnoKey 數
已發放人數	顯示已經燒制的 QnoKey 數
線上人數：	顯示當前線上連線使用 QnoKey 數
顯示用戶：	顯示已經設定的 QnoKey 所有使用者列表
刪除	刪除一條使用名稱群組設定規則

跳到 1 頁	選擇跳至資訊摘要第幾頁
5 每頁顯示的欄位	總表頁面每頁顯示幾條群組資訊
新增 Qnokey 群組：	增加新的群組設定
刪除所有群組：	清除所有群組設定。

10.2.2 群組設定頁面

按下“新增 Qnokey 群組”按鈕後，將進入“群組參數設定”頁面，如下圖所示。

這個頁面主要用來設定 QnoKey 群組。在這裏，通過廣域網埠口、有效時間、使用者上限人數、遺失保護措施等，對 QnoKey 的群組參數進行設定，以便對 QnoKey 使用者分類管理，提高其安全性。

啟用此群組：	勾選此選項，啟用這條設定群組。
群組帳戶名稱：	在此填寫想要建立的 QnoKey 群組名稱。
接口位置：	勾選設定廣域網埠口，並填寫各廣域網埠口相對應的正確的 IP 位址或網域名稱(經 DDNS 解析)。如有廣域網埠口為空則不需

要填寫 IP，以免造成 VPN 連接不成功。此操作設定允許用戶從哪一廣域網埠連進來，便於管理工作。

當選定廣域網 1，則此 QnoKey 群組用戶只能通過廣域網埠 1 連進來。若同時勾選廣域網 1，廣域網 2，則允許此 QnoKey 群組用戶通過廣域網 1 或廣域網 2 連接 VPN，當廣域網 1 斷線則會自動轉向廣域網 2，作為 VPN 連接備援。

請注意：

- 若勾選的廣域網埠口，在網路連接類型為靜態 IP 的話，系統會自動顯示出此廣域網 IP，管理端不需自己再輸入。
- 若勾選的廣域網埠口，在網路連接類型為 DHCP/PPPoE 等其他類型的話,管理端則需要輸入正確的 IP 位址或網域名稱(經 DDNS 解析)。

有效時間：

在這裏設定此 QnoKey 群組的有效使用時間。

當用戶端 QnoKey 使用比較固定，可點選"永久"選項，設定用戶端有效使用時間為永久使用。

如果用戶端使用情況比較複雜，或提供給出差移動用戶使用，為確保 VPN 資料安全，可設定 QnoKey 使用有效期限為幾天，這裏允許設定"1~99"天，可根據實際需要填寫想設定的天數。

使用人數上限：

這裏填寫此群組設定規則所允許燒制 QnoKey 的最大數

Key 遺失保護措施：

在下拉功能表中選擇 QnoKey 遺失後所進行的操作選項。

如果 QnoKey 不小心意外遺失，可採取三種操作 "不做任何防護"、"清除 Key 內容"和"封鎖連線"。

對 QnoKey 進行此項設定，可以進一步提高 VPN 的安全性。選擇"不做任何防護"操作選項，則當這把 Key 遺失後，不做任何操作。

選擇"清除 Key 內容"操作選項，會在這把 QnoKey 遺失後再

建立 VPN 連線時，將這把 QnoKey 裏的資料清除。

選擇"封鎖連線"操作選項，則會在這把 Key 遺失後，不能再連上 VPN，將其鎖定。

按下“確定”按鈕應用此群組設定規則，按“取消”取消剛才的設定操作。按“返回上一頁”返回上一頁。

當按下“確定”按鈕，會彈出一個對話方塊，詢問您是否繼續增加設定群組，點選“確定”繼續增加另一個群組設定規則，點選“取消”返回到 QnoKey 總表。如下圖所示。

這時在 QnoKey 群組資訊總表頁面就會顯示出剛設定好的群組。如下圖所示。

當新增規則後，每一條規則後面都會出現“顯示用戶”和“編輯”按鈕。點選“顯示使用者”按鈕，則會顯示應用這條群組規則的用戶列表。點選“編輯”按鈕編輯修改設定。點選垃圾桶圖示，刪除這條設定。

10.2.3 群組用戶列表頁面

點選“顯示用戶”按鈕後，將顯示應用這條群組規則的群組用戶列表頁面。

群組用戶列表

群組帳戶： test

No.	啓用	QnoKey序列號	使用者名稱	狀態	Key遺失保護措施	硬件綁定	MAC地址	刪除

返回 確認 取消

群組帳戶名稱：	顯示此用戶所在群組的名稱。
啟用：	勾選此選項，啟用此 QnoKey 用戶。
QnoKey 序列號：	顯示此 QnoKey 的序列號。
使用者名稱：	顯示此 QnoKey 的用戶名。
狀態：	顯示此 QnoKey 的連線狀態，“連線”表示用戶已經連線線上；“不線上”表示沒有線上連線使用。
Key 遺失保護措施：	勾選表示此 QnoKey 遺失，則應用所設定 QnoKey 遺失後的操作。
硬件綁定：	若啟硬體綁定，QnoKey 只能在所設定綁定 MAC 位址的電腦上使用執行，不是該 MAC 位址資料的電腦，無法使用 QnoKey
MAC 位址：	若有啟用硬體綁定功能，會顯示 QnoKey 所綁定的電腦 MAC 位址資料，不是該 MAC 位址資料的電腦，無法使用 QnoKey
刪除：	刪除該單一用戶的 QnoKey 連線資料

10.3. QVM VPN 功能設定

搭配 QVM 系列 VPN 防火牆提供了三大便利性功能：

1. SmartLink IPSec VPN：簡單建立 VPN，取代傳統 VPN 建立的複雜缺點，只需要伺服器 IP、用戶名及密碼就可以完成。
2. 中央控管功能：讓所有外點或分公司的 VPN 連線狀態清楚且可直接在 VPN 防火牆中控畫面，遠端進入外點用戶端做設定。
3. VPN 斷線備援機制：讓 ISP 斷線困擾造成外點或分公司資料無法對總公司傳送問題順利解決。

10.3.1. QVM 中心伺服器端設定

選擇 QVM 功能為伺服器模式：

帳戶名稱：　　需要跟遠端用戶端名稱一致，請輸入遠端用戶端使用者的名稱，中英文皆可

密碼：/再次輸入密碼： 需要跟遠端用戶端密碼一致，請輸入使用者密碼及再次確認使用者密碼

IP 位址/子網路遮罩： 此為 VPN 防火牆內部哪一個網段 IP 位址以及子網路遮罩，需要跟遠端用戶端做 QVM 連線

VPN Hub 功能： 分點與總部連通後，可以讓分點之間實現互聯互通，不用再去各分點的設備之間建立通道，方便管理，更能節省資源。不同運營商電信網通線路可透過總部中央點進行轉換，讓連線速度不延遲，解決跨網 VPN 連線壅塞的問題。同時還能結合俠諾專長的頻寬管理功能，讓總部的網管人員可以控制不同分支援點間的互相連線，達到更嚴密控管的功能。

啟用： 啟用此帳號

加入到對應列表： 新增輸入的帳號與密碼

刪除點選的項目： 刪除所選擇的使用者

設定修改完成請按下“確定”按鈕儲存網路設定變更或是按下“取消”按鈕不做任何設定變更。

10.3.2. QVM 中央控管（QVM 連接狀態查詢）

用戶可以通過點選遠端用戶的名稱登錄遠端用戶端 VPN 防火牆對遠端網路進行相關設定。

QVM 用戶連線列表

No.	帳戶	狀態	接口位置	啓動時間	結束時間	持續時間	連線控制	配置
1	test			---	---	---	Waiting...	Edit

重新整理

帳戶： 此為用戶的外點用戶端所顯示的用戶名稱。綠色表示已經連通，藍色表示等待連線，紅色表示此條 QVM 關畢

狀態： 此為顯示此條 QVM VPN 的連線狀態。紅色線表示斷線，綠色線表示已經連通

接口位置： 此為遠端此條 QVM 現在經由 VPN 防火牆的哪一條 WAN 口進來做 QVM 連線

啟動時間： 表示此條 QVM 的起用時間

結束時間： 表示此條 QVM 最後的結束時間

持續時間： 表示此條 QVM 啟用至結束的總時間

連接控制： 表示現在此條 QVM 所處於的狀態：等待連線-Waiting，斷開-Disconnect 將此條 QVM 斷線並關畢-Disable 此功能，啟用開啟此條 QVM 至等待連線狀態

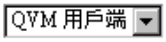
配置： 若您按下 Edit 按鈕， 將會連線到此設定的項目當中，您可以修改其中的設定

10.3.3. QVM 用戶端設定

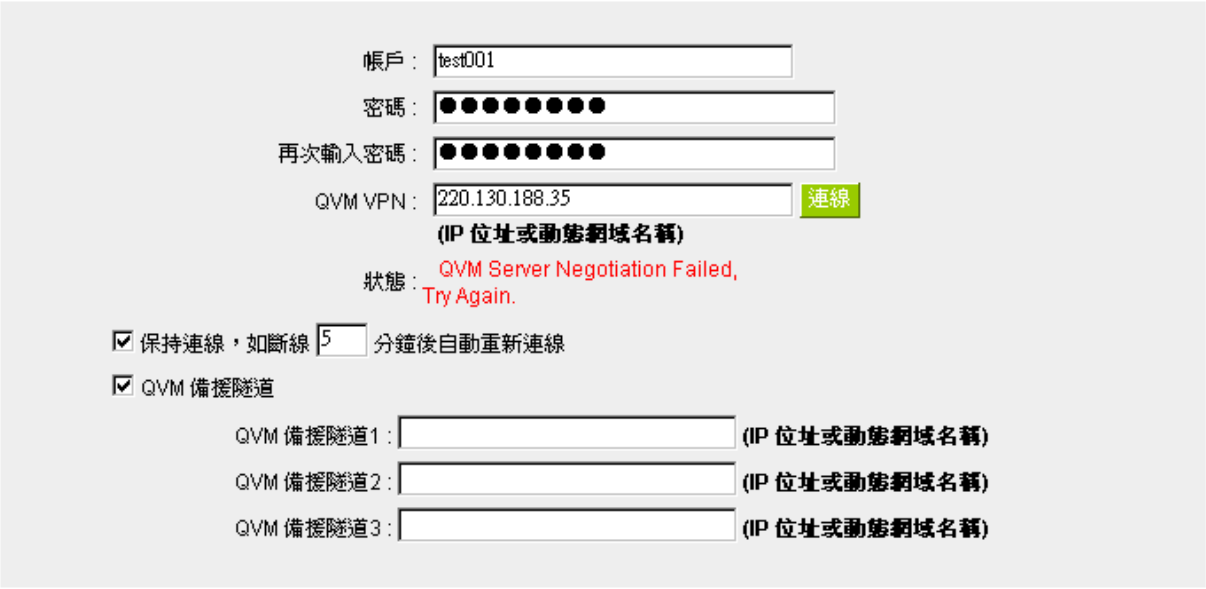
選擇 QVM 功能為用戶端模式：

選擇進行 VPN 連接的 VPN 防火牆為 QVM 用戶端。

QVM 配置模式



QVM 用戶端配置



進階功能配置

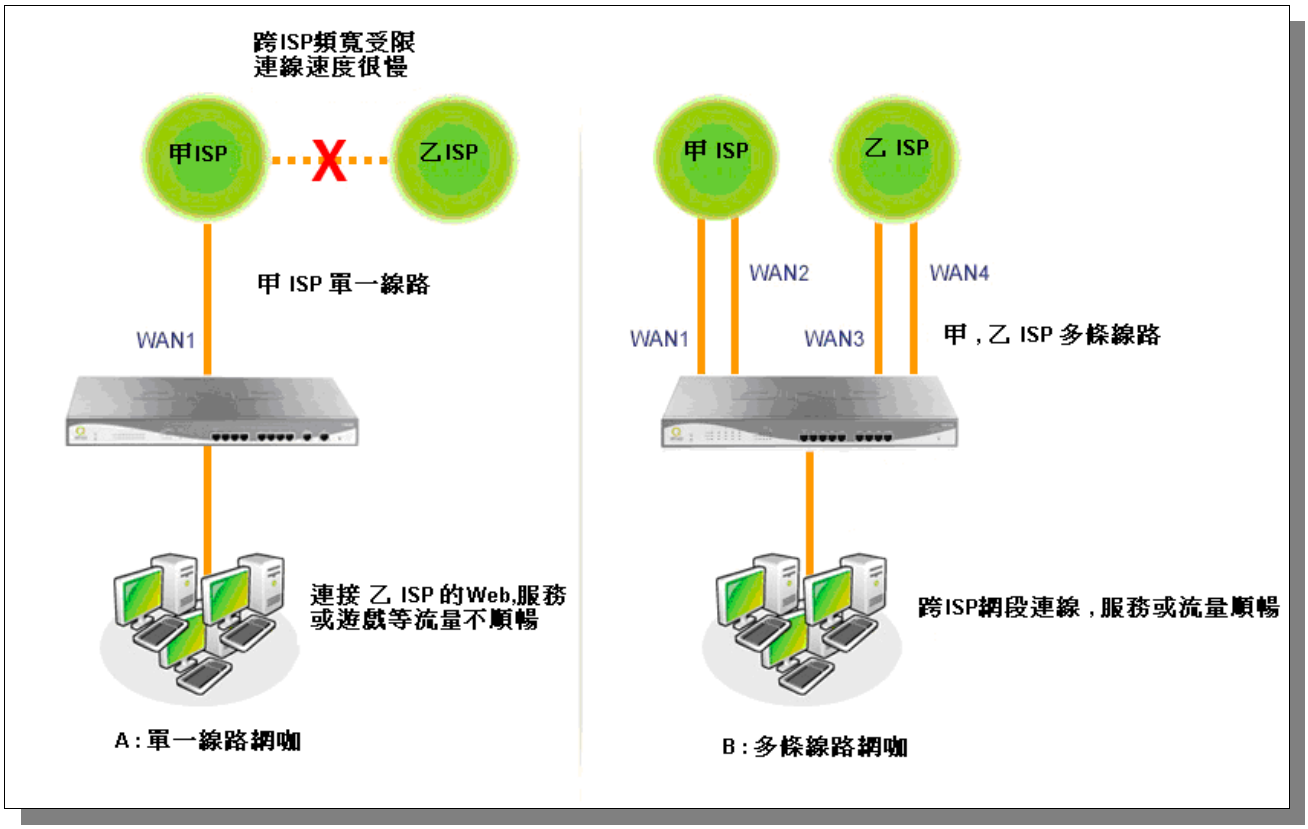
QVM 用戶帳戶名稱：	輸入已在 QVM 服務端中建立的對應用戶名稱
密碼：	輸入已在 QVM 服務端中建立的對應密碼
再次輸入確認密碼：	再輸入一次確認密碼
QVM VPN（中心端 IP 位址或動態網域名稱）:	輸入 QVM VPN 服務端 IP 位址或是網域名稱
狀態：	在此欄位可以看到 QVM 功能連線狀態
保持連接，如斷線( )分鐘後自動重新連接	此功能為 QVM 連線斷開後，重新檢測連接的間隔時間。時間範圍為 1~60 分鐘
QVM 備援隧道：	若是勾選此選項，QVM 備援功能將被開啟。您可以輸入最多三

	個備援連接 IP 或是網域名稱，一旦斷線可從中心服務端 VPN 防火牆的另一個 WAN 埠自動建立 VPN 連線，確保 VPN 服務永不斷線，保證資料傳輸的安全
進階設定： 變更 QVM 用戶端通訊埠：	在某些環境下 443 Port 已被使用，如企業 E-Mail Forwarding，所以為了避免與 QVM 使用衝突，可以將 QVM 的連線通訊埠改為其他加密的埠號如 10443 Port

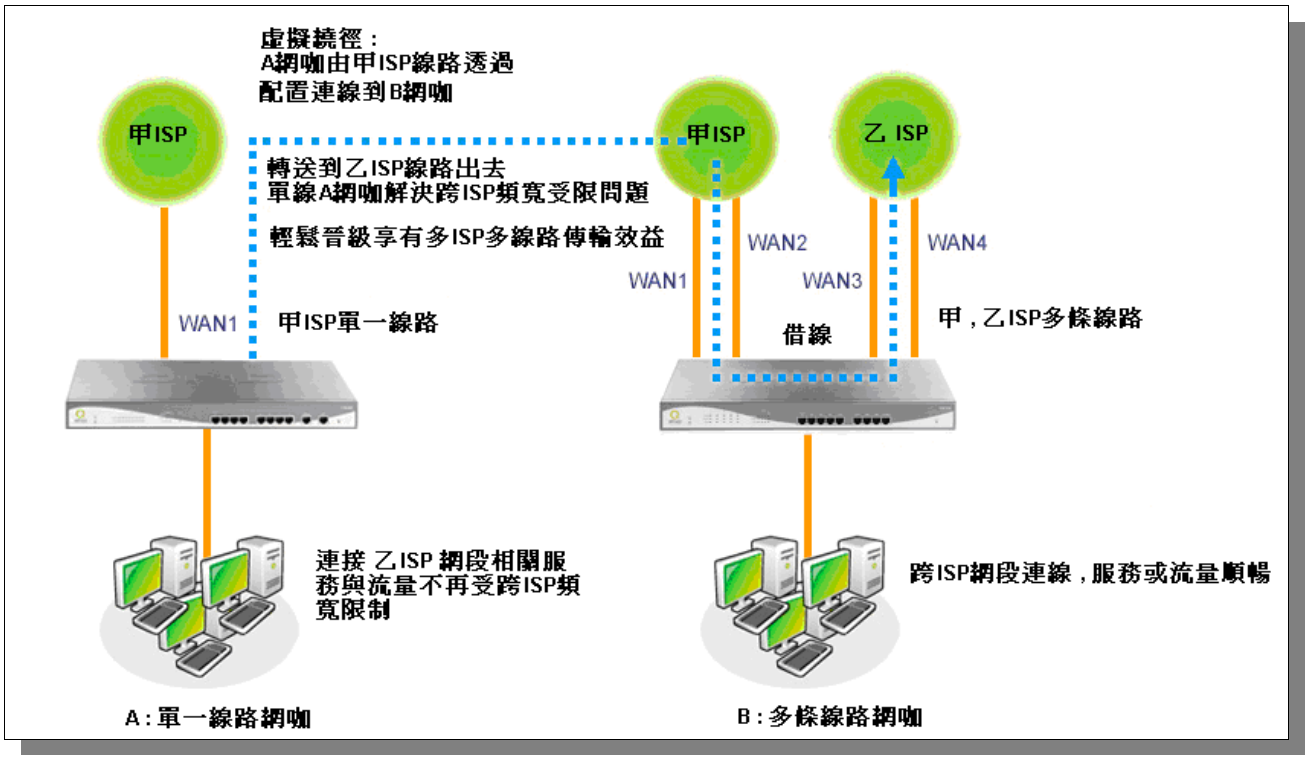
設定修改完成請按下“確定”按鈕儲存網路設定變更或是按下“取消”按鈕不做任何設定變更。

十一、虛擬繞徑設定

虛擬繞徑功能讓單線分點輕鬆晉級享有雙線傳輸，只有單線的企業分點通過設定連線至具有雙線的中心端，通過中心點轉發到另一條線路出去，加速區域間不同 ISP 網段連線，解決了連線瓶頸問題。



如上圖：A 網咖只有甲 ISP 單線傳輸，由於跨 ISP 網段頻寬受限，透過甲 ISP 去訪問乙 ISP 的 WEB，乙 ISP 遊戲等連線速度很慢。而 B 網咖擁有甲、乙 ISP 多線路傳輸，這樣無論訪問甲 ISP 還是乙 ISP，連線速度都很快，玩起遊戲等也順暢，滿足了用戶的需求。



如上圖：在這樣情況下，A 網咖通過設定虛擬繞徑，由甲 ISP 線路連線到 B 網咖的設備，通過 B 網咖轉發到乙 ISP 線路上，這樣就好像 A 網咖也配備了甲乙雙 ISP 雙線路，當 A 網咖用戶需要訪問乙 ISP 網段時，連線速度不再受限而緩慢，遊戲也變得順暢，解決了跨 ISP 網段頻寬受限的問題，讓只有甲 ISP 單線的 A 網咖輕鬆晉級享有多 ISP 多線傳輸的效益。

11.1 虛擬邊徑 服務端（PPTP 伺服器）

本節主要介紹虛擬邊徑服務端如何設定。虛擬邊徑是利用 PPTP 建立在 PPP（點對點協議）的基礎，它提高了 PPP 的安全級別，讓 PPP 可以對 PPTP 伺服器與 PPTP 用戶端之間的資料進行加密傳輸，並使 PPTP 伺服器可以對遠端用戶的身份進行驗證。進入虛擬繞徑項目，勾選"啟用 PPTP 伺服器"選項，開啟 PPTP 伺服器。

PPTP 用戶使用範圍：是當您連線到 PPTP 伺服器後，由伺服器分發給用戶端的 IP 位址範圍。您可以根據需要設定開始 IP 和終止 IP。

新增使用者：在此添加用戶端欲進行連接的名稱和密碼，更新使用者列表。

用戶名稱：	在此添加用戶端欲進行連接的使用者名稱
密碼：	在此輸入用戶端欲進行連接的密碼
再次輸入密碼	再次輸入密碼進行身份驗證
更新使用者	點此按鈕添加或更新到對應列表
刪除使用者	點此按鈕刪除列表中選中的使用者
新增	點此按鈕新增使用者到對應列表

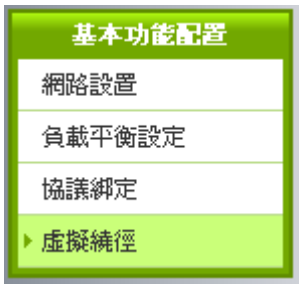
所有的 PPTP 通道狀態：顯示所有連接成功的用戶，包括使用者名稱、遠端 IP 位址和 PPTP 發放的位址。

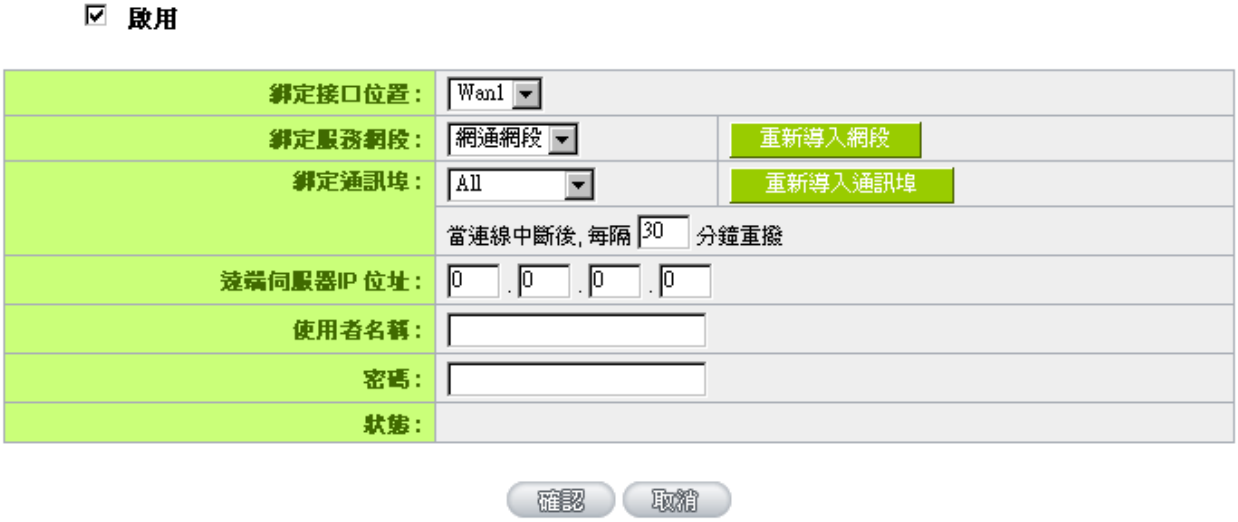
PPTP 用戶連線列表

使用者名稱	遠端用戶的IP 位址	本機對映的IP 位址

重新整理

11.2 虛擬遶徑 用戶端



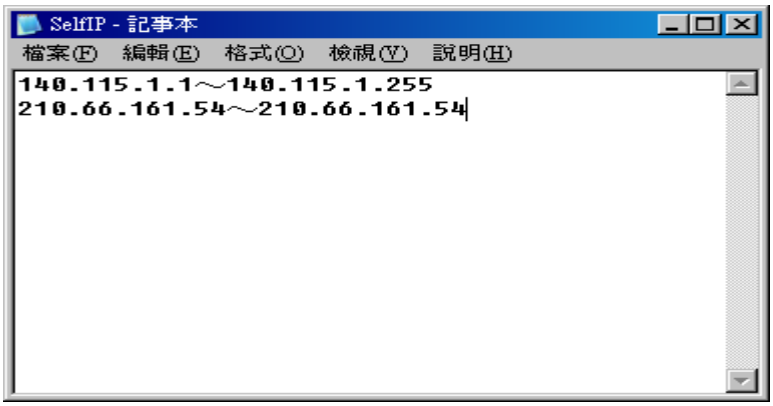


啟用虛擬遶徑功能	勾選此選項,開啟虛擬策略路由功能
綁定接口位置	選擇虛擬遶徑綁定的廣網域 WAN 口
綁定服務網段	在此選擇設定預走虛擬繞徑的網域，可選擇網通或是自定義。這裏您可以根據實際需要自己設定綁定的網域。
重新導入網段	點此按鈕修改虛擬策略路由 IP 段，點選流覽匯入自定義 IP 檔。（自定義 IP 檔的編寫見此表後檔編寫 1）
綁定通訊埠	在此選擇設定預走虛擬繞徑的埠，可選擇所有埠、遊戲埠或是自定義。這裏您可以根據實際需要自己設定綁定的通訊埠。
重新導入埠	點此按鈕修改虛擬策略路由通訊埠，點選流覽匯入自定義埠檔。（自定義埠檔的編寫見此表後檔編寫 2）
當連接中斷後,每隔 30 分鐘重撥	此處填寫當虛擬繞徑中斷連接時,重新嘗試再次連接的時間間隔,預設為 30 分鐘。您可以根據需要填入自定的時間間隔。

遠端伺服器 IP 位址	在此填寫虛擬邊徑伺服器的外部 IP 位址。
用戶名稱	在此輸入虛擬邊徑使用者的名稱。
密碼	在此輸入虛擬邊徑伺服器的密碼。
狀態	顯示虛擬繞徑連接狀態：連線或掉線

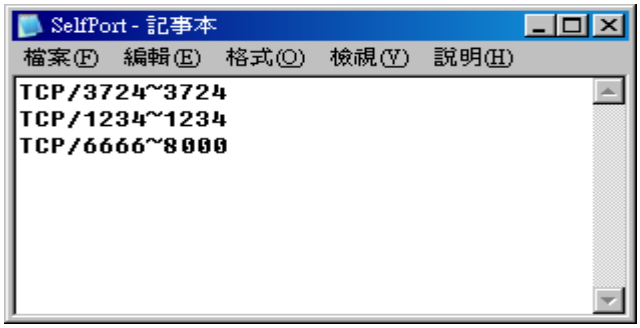
檔編寫 1——自定義 IP 檔

自定義IP檔的建立可以用純文本編輯軟體來撰寫，例如使用Windows系統自帶的文本編輯程式"記事本"來建立。將您要指定的目的 IP 位址按照下圖的格式寫入，例如您要指定的目的 IP 位址範圍是從 140.115.1.1 到 140.115.1.255，則在"記事本"中輸入 140.115.1.1～140.115.1.255。下一個目的 IP 位址範圍則要換行輸入。請注意！若是只有一個目的 IP 位址，也需要以同樣的格式來書寫。例如指定的目的 IP 位址是 210.66.161.54，則必須寫成 210.66.161.54～210.66.161.54 格式。儲存檔後(副檔名應該是.txt)即可匯入修改虛擬策略路由 IP 段。



檔編寫 2——自定義埠檔

自定義IP檔的建立可以用純文本編輯軟體來撰寫，例如使用Windows系統自帶的文本編輯程式"記事本"來建立。將您要指定的埠按照下圖的格式寫入，例如您要指定 TCP/3724~3724 埠，則在"記事本"中輸入 TCP/3724~3724。下一個指定埠則要換行輸入。儲存檔後(副檔名應該是.txt)即可匯入修改虛擬策略路由通訊埠。



十二、其他進階功能設定

本章介紹 VPN 防火牆進階功能的設定，如果內網需要設定伺服器提供 Web/FTP 服務等，可以通過虛擬伺服器的連接設定設定完成，同時應部分用戶需要提供靜態路由以及動態路由協定的設定，一對一 NAT 功能的設定解決實體 IP 與虛擬 IP 對應，以及設定動態網域名稱解析服務滿足用戶獲得 ISP 的動態公網 IP 情況下需要建設 Web/FTP 伺服器等要求。

12.1 DMZ/虛擬伺服器

12.1.1 DMZ 設定

當您將 VPN 防火牆內部的某台 PC 的虛擬 IP 填入到此 DMZ 選項時，VPN 防火牆 WAN1 及 WAN2 的合法 IP 位址會直接對應給此台 PC 使用，也就是說從 WAN 端進來的封包，若是不屬於內部的任何一台 PC，都會傳送到這台 PC 上。

在使用"DMZ 主機"功能後，若您要取消此功能必須於在設定虛擬 IP 位址地方填入"0" 的參數，才會停止此功能使用。

點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。 點選"取消" 即會清除剛才所變動的修改設定內容參數，此操作必須在確認儲存動作之前才會有效。

12.1.2 虛擬伺服器設定

若是您在內網需架設伺服器（意指對外部的服務主機 WEB、FTP、Mail 等），這個功能可將虛擬伺服器主機視為－虛擬的位置，利用 VPN 防火牆的外部合法 IP 位址，經過通訊埠的轉換，(如 WWW 為 80 埠)，直接存取到內部虛擬 IP 的伺服器的服務。例如在設定視窗中，選項填入伺服器位置，如 192.168.1.2 且埠是 80 的話，當外部網路要進來存取這個網頁時只要鍵入：

http：//220.130.188.45 (假設此為 VPN 防火牆的外部合法 IP 位址)

此時，就會通過 VPN 防火牆的公網 IP 位址去轉換到 192.168.1.2 的虛擬主機上的 80 埠讀取網頁了。

其他種類的伺服器設定，都如以上設定；只要將所用伺服器的通訊埠以及虛擬主機的 IP 位址填入即可！

虛擬伺服器

通訊埠：	在此選擇欲開啟的虛擬伺服器的通訊埠號碼預設列表，如 WWW 為 80(80~80)， FTP 為 21~21，可參考服務號碼預設列表！
內部 IP 位址：	在此填上虛擬伺服器所要相對應的內部虛擬 IP 位址，如 192.168.1.100。
啟用：	開啟此服務功能。

通訊埠新增或刪除表： 若您所需要的通訊埠沒有在列表裏面，可以利用此功能新增或刪除管理通訊埠號列表。

加入到對應列表： 增加到開啟服務項目內容。

新增或刪除管理通訊埠

若您欲開啟的通訊埠項目沒有在表列中，您可以點選"服務端新增或刪除表"新增或刪除管理通訊埠號列表，如下圖所示：

通訊埠名稱：	在此自定欲開啟的通訊埠號名稱加入列表中，如 BT 等。
通訊協定：	在此選擇欲開啟的通訊埠號的封包格式為 TCP 或 UDP。
通訊埠的位置範圍：	將您所需新增加的通訊埠範圍填入。
加入到對應列表：	增加到開啟服務項目內容列表，最多可新增 100 組。
刪除點選的項目：	刪除所選擇的開啟服務項目之一筆內容。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。
離開：	離開此功能設定視窗。

12.1.3 特殊應用軟體設定：

有一些特殊應用軟體其進出網際網路的通訊埠號為非對稱的，此時您必須使用此功能選項將一些特殊應用程式使用的通訊埠號填入相關設定中，如以下窗口所示：

特殊應用軟體名稱：	您可以自定此特殊應用軟體名稱，方便管理使用！
實際對外的埠範圍：	輸入由 VPN 防火牆出網際網路的使用埠(Port Number)編號(如 9000~10000)。

內部映射的埠範圍：	輸入由網際網路進入的使用埠(Port Number)編號。 (如 2004~2005) 。
加入到對應列表：	增加到開啟服務項目內容列表。
刪除所選中的項目：	刪除所選擇的開啟服務項目之一筆內容。
顯示列表：	點選此按鈕即會顯示列表上的所有設定項目內容參數。可以以"虛擬主機伺服器"和"特殊應用軟體"分別來查看列表。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

12.2 UPnP 通訊協定

UPnP (Universal Plug and Play) 是微軟所制定的一項通訊協定標準，若是您使用的電腦有支援 UpnP 機制的話(如 Windows XP)而且您的電腦 UpnP 功能有開啟，您可以將 VPN 防火牆的 UPnP 功能啟用，可以從您的電腦上開啟或關閉 UPnP Forwarding 的選項。

UPnP 功能包含有 UPnP Forwarding 的功能，如您要在內網設定虛擬伺服器，您可以在前章節介紹的 Forwarding 功能設定，或是在此 UPnP Forwarding 中設定。不過請不要重複輸入造成衝突。

通訊埠：	在此選擇欲開啟的 UPnP 的服務號碼預設列表，如 WWW 為 80(80~80)， FTP 為 21~21，可參考服務號碼預設列表！
主機名稱或 IP 位址：	在此填上 UPnP 相對應的內部虛擬 IP 位址或名稱，如 192.168.1.100。
啟用：	開啟此服務功能。
通訊埠設定：	新增或刪除管理通訊埠號列表。
加入到對應列表：	增加到開啟服務項目內容。

刪除所選中的項目：	刪除所選擇的開啟服務項目之一筆內容。
顯示列表：	顯示目前所開啟設定的 UpnP Forwarding 列表。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

12.3 路由通訊協定

此節介紹動態路由協定以及靜態路由的設定。

12.3.1 動態路由設定

RIP 是路由通訊協定 Routing Information Protocol 的簡稱，有 RIP I / RIP II 兩個版本。對於一般使用的網路中，大多只有一個路由器(或是閘道器)，所以大部份的情況是不需要使用這個功能。RIP 的使用時機是您的網路中有數個 VPN 防火牆，此台 VPN 防火牆是其中之一，此時若是不想手動設定每台 VPN 防火牆的繞徑表，可以啟用此功能，自動將所有路徑更新！

RIP 是一個很非常簡單的路由協議，採用距離向量的方式以封包到達目的地之前需要經過的路由的個數來

做傳送距離的判斷，而不以實際連線的速率來做判斷。所以所選的路徑是經過最少的路由，但是並不一定反應速度最快的路由及路徑。

動態路由協議

選擇 VPN 防火牆工作模式：	選擇 VPN 防火牆運作模式為 NAT 模式或是路由模式。
動態路由通訊協定 RIP 功能：	選擇按鈕"啟用"開啟使用 RIP 動態路由通訊。
RIP 路由協議版本（接收端）:	可於上下選擇按鈕選擇使用動態路由通訊 None，RIPv1，RIPv2，Both RIPv1 and v2 作為傳送動態路由通訊協定格式。
RIP 路由協議版本（傳送端）	可於上下選擇按鈕選擇使用動態路由通訊 None， RIPv1，RIPv2-Broadcast， RIPv2-Multicast， 為接收動態路由通訊協定格式。

12.3.2 靜態路由設定

靜態路由是以手動設定路由表的方式來達成封包路由。在此 VPN 防火牆的應用可分為兩種方式，一是在內網中連結不同網段或 VPN 防火牆，一是在 Multi-WAN 的環境中讓 VPN 防火牆知道去那個目地位址時就要走那條 WAN。例如常常會遇到 VPN 防火牆不同的 WAN 申請不同家的 ISP 的線路，為了避免有些服務像是郵件伺服器，或遊戲伺服器是架設在不同一 ISP 環境而且 ISP 之間無法彼此互通，此時去郵件伺服器或是去遊戲伺服器就應該走不同的 WAN，而避免繞遠路。這個用意跟協議綁定是有相似的做用。

靜態路由協議

目的 IP 位址和子網路遮罩：	填入目的地的遠端網路 IP 節點與子網路節點位址。
預設閘道：	從此網路節點到目的遠端網路欲繞徑的預設閘道器位址。
路由節點數：	從此網路節點到目的遠端網路所經過路由器層數，如是在路由器下的二個之一，此應填為 2，預設為 1。(最大為 15)。
接口位置：	此網路節點的連接位置，是位於廣域埠 WAN 端亦或是局域埠 LAN 端。
加入到對應列表：	增加此路徑規則到列表中。
刪除所選中的項目：	刪除在表中所選擇的路徑表。
顯示列表：	顯示目前最新的路徑表。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

12.4 一對一 NAT 對應

當您的 ISP 線路為固定制(如 ADSL 固定 IP)時，通常 ISP 會給您多個合法 IP 位址。VPN 防火牆提供您可將除了 VPN 防火牆本身 WAN 埠以及光纖轉換器或 ATU-R(閘道) 各使用一個合法 IP 位址後，所剩的合法 IP 位址可以直接對應到 VPN 防火牆內部的電腦使用，也就是這些電腦在內網雖為虛擬 IP，但當做了一對一對應後，這些對應到的電腦去外部訪問時都是有自己的合法 IP。

例如，當您公司內部環境需有兩台或兩台以上的"WEB 伺服器"時，由於需要兩個或兩個以上的合法 IP 位址，所以可以利用此功能達到將外部多個合法 IP 位址直接對應到內部多個虛擬服務伺服器 IP 位址使用！

範例： 如您有 5 個合法 IP 位址，分別是 210.11.1.1～6，而 210.11.1.1 已經給 VPN 防火牆的 WAN1 使用，另外還有其他四個合法 IP 可以分別設定到 One to One NAT 當中，如下所述：

210.11.1.2→ 192.168.1.3

210.11.1.3→ 192.168.1.4

210.11.1.4→ 192.168.1.5

210.11.1.5→ 192.168.1.6

注意！

VPN 防火牆 WAN IP 位址不能被涵蓋在一對一 NAT 的 IP 範圍設定中。

啟用一對一 NAT 功能：	選擇是否開啟此一對一 NAT 功能 "啟用"開啟 "禁止"關閉。
內部起始 IP 位址：	虛擬 IP 位址起始 IP 位址。
外部起始 IP 位址：	外部合法 IP 位址起始 IP。
對應範圍的 IP 數量：	填入您同時要有多少個外部合法 IP 位址需要對應。
加入到對應列表：	加入此設定到一對一 NAT 列表中。
刪除點選的項目：	刪除所選擇的一對一 NAT 規則。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於"確定"儲存動作之前才會有效。

注意！

一對一的 NAT 模式將會改變防火牆運作的方式，您若設定了此功能，LAN 端所對應有公網 IP 的服務伺服器或電腦將會曝露在網際網路上。若要阻絕網路的使用者主動連線到一對一 NAT 的服務伺服器或電腦，請到防火牆的存取規則中設定適當的拒絕存取規則條件。

12.5 DDNS-動態網域名稱解析

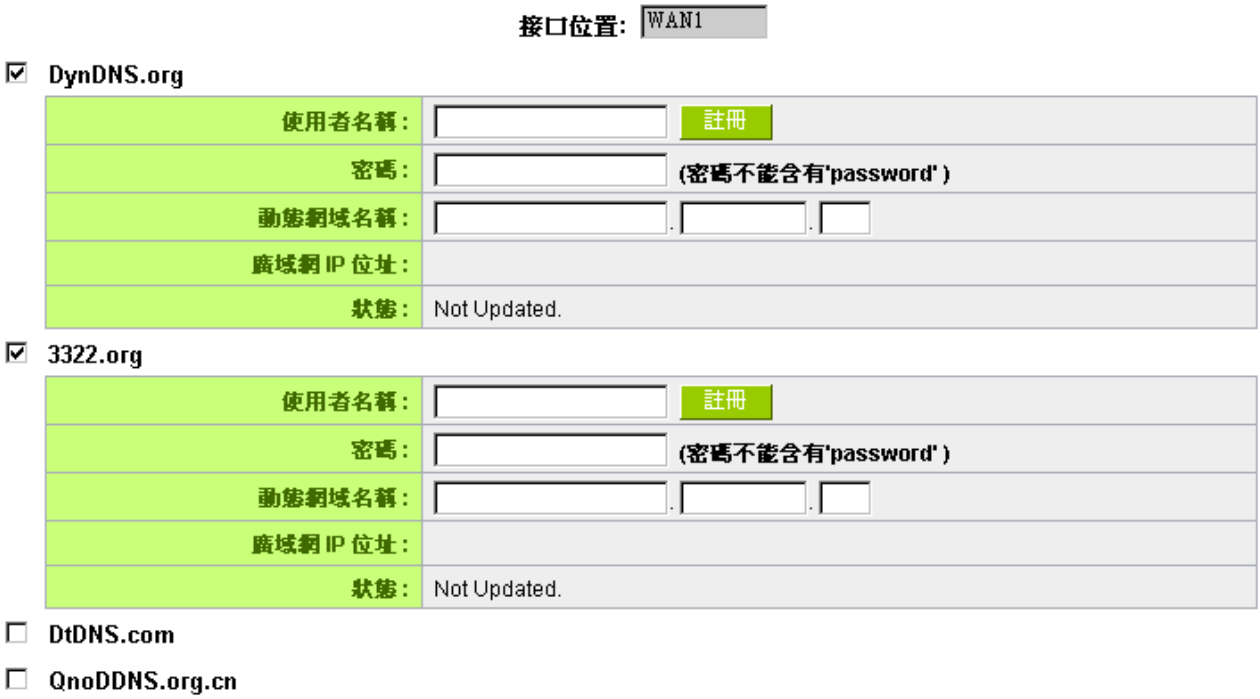
此 VPN 防火牆的 "DDNS" 功能可以支援 QnoDDNS、Dyndns、3322、Dtdns（支援 DDNS 種類依機種不同而相異）的動態網域名稱解析功能，其目的是為了讓使用動態 IP 位址(也就是無法有固定 IP 的環境)來架設虛擬伺服器、建立企業 VPN 使用、及遠端監控時查詢現在的 VPN 防火牆 IP。如 ADSL PPPoE 計時制或是 Cable Modem 的使用者的 WAN IP 位址都會隨 ISP 端要求而改變，當此時使用者申請了 DDNS 後，將其設定在 DDNS 設定中，則在遠程只要去所申請的 DDNS 則可以知道現在 VPN 防火牆的實際 IP。且若是內部有架設網站之類的服務，網路使用者只要在網址打上所申請的 DDNS 就可以直接進入到您內部架設的 WEB。在設定此功能之前，請向 www.qno.com.tw、www.dyndns.org 或是 www.3322.org 提出申請，此服務是完全免費的！

另外，為瞭解決 DDNS 伺服器可能會發生不穩定的情況，現在 VPN 防火牆每個 WAN 都可同時對不同家的 DDNS 做動態 IP 升級。

動態網域解析服務

接口位置	動態網域名稱	狀態	配置
廣域網1	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	編輯
廣域網2	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	編輯
廣域網3	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	編輯
廣域網4	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	編輯

選擇您要設定的廣域網埠，比如"廣域網 1"，點選"編輯"進入廣域網 1 的 DDNS 設定視窗，對要設定的 WAN 口的 DDNS 方式進行勾選。



接口位置	顯示使用者所選取的廣域埠
DDNS 動態網域名稱解析服務：	可以選擇 QnoDDNS、Dyndns 以及 3322(可以同時使用)。(支援 DDNS 種類依機種不同而相異)
用戶名稱：	向 DDNS 服務提供者所申請的使用者名稱。QnoDDN 使用者名稱要填入完整的網址，如：abc.qnoddns.org.cn。
密碼：	向 DDNS 服務提供者所申請的密碼。
動態網域名稱：	動態網址名稱： 向 DDNS 所註冊的網址，如 abc.QnoDDNS.org.cn 或者 abc.dyndns.org。
廣域網 IP 位址：	目前此條 WAN 所取得的 ISP 之動態合法 IP 位址，當 VPN 防火牆得到 ISP 端給的合法 IP 位址後會自動顯示於此。
狀態：	顯示目前 VPN 防火牆對 DDNS 的更新狀態。
確定：	點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

註冊 QnoDDNS 俠諾動態網域名稱

1． 請先至 Qno 俠諾網站，進行產品註冊：http：//www.qno.com.tw

2． 依據產品註冊使用的電郵以及產品序列號，登入 QnoDDNS 俠諾動態網域名稱服務系統；請確認電郵可以確實收信，以利註冊網域名稱後，可收到系統寄出的啟用 QnoDDNS 服務密碼。

3． 網域名稱申請規則：

- 網域名稱最少需為 4 個字，最多 63 個字。
- 網域名稱只能由 a-z(英文小寫)、0-9(數字)所組成，且第一個字需為英文字母。
- 網域名稱不得有特殊符號(例如："."；"-"；"_"等等) 。
- 2 Wan 系列產品最多申請 2 個 DDNS 設定。
- 4 Wan 系列產品最多申請 4 個 DDNS 設定。
- 8 Wan 系列產品(含以上)最多申請 4 個 DDNS 設定。

:: 使用者資料 ::

姓名	
Email	
序號	
型號	
Wan數量	
目前登入IP	
伺服器時間	

:: 申請規則 ::

1. 如果您申請QnoDDNS服務，代表"您無條件同意" Qno傻諾科技動態網域名稱服務條款。
2. "使用者名稱" 最少需要4個字，最多63個字(4-63個字)。
3. "使用者名稱" 只能由a-z(英文小寫)、0-9(數字)所組成，且第一個字需爲英文字母。
4. "使用者名稱" 內不允許含有 'qno'、'dns' 的英文字母在內！
5. "使用者名稱" 不得有特殊符號(例如："."；"-"；"_"…等等)。(範例)
6. 2 Wan 系列產品最多申請 2 組DDNS設定。
7. 4 Wan 系列產品最多申請 4 組DDNS設定。
8. 8 Wan 系列產品最多申請 4 組DDNS設定。
9. 設定 QnoDDNS 之前，請先確認產品之 "系統時間" 正確，請參考系統時間、時間設置。
10. 如果您無法透過網路使用NTP服務來更新路由器時間，請參考伺服器時間來手動更新。
11. Qno NTP Server：1. ntp.qnoddns.org.cn 2. ntp.ddns.org.cn
12. 其他NTP Server：1. 香港天文台 2. 台灣中華電信研究所 3. 國際亞洲NTP Server。
13. 其他注意事項請參考 QnoDDNS服務使用教學。

:: 使用者名稱測試 ::

已輸入0個字

測試 使用者名稱： 網域名稱： qnoddns.org.cn 送出 重設

尚可申請 4 組DDNS

已輸入0個字

第1組 使用者名稱： 網域名稱： qnoddns.org.cn 申請

已輸入0個字

第2組 使用者名稱： 網域名稱： qnoddns.org.cn

已輸入0個字

第3組 使用者名稱： 網域名稱： qnoddns.org.cn

已輸入0個字

第4組 使用者名稱： 網域名稱： qnoddns.org.cn

12.6 廣域網接口 MAC 位址設定

有些 ISP 會要求提供一固定 MAC 位址(網卡實體位址)做為 ISP 端分配 IP 給您的認證使用，此大多適用於 Cable Mode 的用戶。若有此需求的話，可使用此功能將提供給 ISP 的網卡實體位址(MAC 位址：00-xx-xx-xx-xx-xx)填入此項目中，VPN 防火牆就會以此 MAC 位址作為跟 ISP 請求 IP 時的認證！

廣域網MAC地址設定

接口位置	MAC地址	配置
廣域網1	32-10-d1-86-12-9b	編輯
廣域網2	3e-89-8a-a6-3d-b6	編輯
廣域網3	02-ad-39-1f-38-12	編輯
廣域網4	3c-65-62-1f-19-33	編輯

選擇您要設定的廣域網埠，比如"廣域網 1"，點選"編輯"進入廣域網 1 的埠 MAC 位址設定視窗，使用者可以自行輸入提供給 ISP 的網卡實體位址 MAC，點選此按鈕"確認"即會儲存剛才所變動的修改設定內容參數，點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

目前設備出廠預設的 MAC 位置為 WAN 端的 MAC 位址。

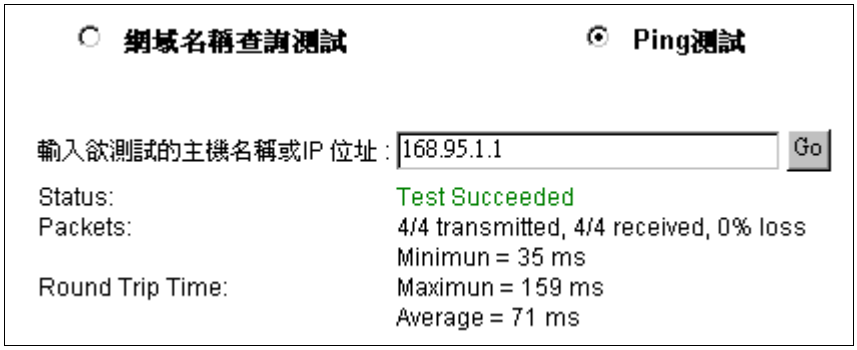
十三、工具程式功能設定

此章節介紹用來管理 VPN 防火牆以及測試網路連線的工具。

考慮安全的因素，建議修改密碼。關於登錄密碼與 VPN 防火牆時間的設定已經在第五章 5.2 節已經介紹，在此就不做重複介紹了。

13.1 線上連線測試

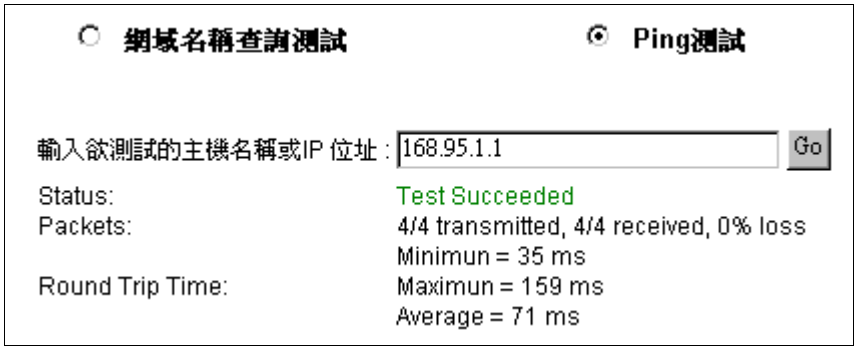
VPN 防火牆提供簡易的線上測試機制，方便於測試線路品質時使用。此包含 DNS 查詢以及 Ping 二種。



網域名稱解析測試

請於此測試視窗輸入您想查詢的網域主機位置名稱，如 www.abc.com 然後點選開始的按鈕開始測試。測試結果會顯示於此視窗上。

Ping-封包傳送/接收測試



此項目為主要提供管理者瞭解對外連線的實際狀況，可以由此功能瞭解網路上的電腦是否存在！

請於此測試視窗輸入您想測試的主機位置 IP，如 168.95.1.1 點選開始的按鈕開始測試，測試結果會顯示在視窗上。

13.2 系統軟體更新

此功能可以讓 VPN 防火牆在 Web 設定視窗中直接做軟體升級。請您於升級前先確認軟體版本資訊。 點選“流覽”按鈕，選擇軟體存放資料夾，並於選擇欲升級的軟體後，點選立即系統軟體更新做升級。

注意！

執行軟體升級前，請詳細閱讀視窗中的注意事項。

正在做軟體升級當中時，請勿離開此升級視窗，否則會造成 VPN 防火牆升級失敗。

13.3 系統設定參數儲存

配置參數回復：

此功能將之前所儲存在電腦的備份設定參數內容回存到 VPN 防火牆中！選擇"瀏覽"至備份參數檔"config.exp"存放資料夾，選擇該檔後，點選"匯入"按鈕做設定檔匯入。

配置參數備份：

此功能為儲存網管人員在 VPN 防火牆的設定參數備份到電腦中，通常做 VPN 防火牆版本升級前，請務必將您現在的 VPN 防火牆設定檔用此功能儲存在電腦中！點選儲存按鈕，選擇至備份參數檔"config.exp"存放資料夾位置，點選儲存即可。

13.4 網路管理設定(SNMP)

SNMP 為 Simple Network Management Protocol 的縮寫，指網路管理通訊協定。此為網際網路上使用的一個管理工具。通過此 SNMP 通訊協定，可以讓已經具備有網路管理的程式 (如 SNMP tools-HP Open View) 等網管程式做即時管理之通訊使用。VPN 防火牆支援標準 SNMP v1/v2c，可以搭配標準 SNMP 網路管理軟體來得知目前 VPN 防火牆上的機器運作情況，以便隨時掌握網路資訊。

啟用：　將 SNMP 功能開啟或關閉。系統預設為開啟此功能。

系統名稱：　設定機器的名稱。

連絡方式：	設定機器的管理聯繫人員名稱。
系統地址：	設定機器的目前所在位置。
Get Community Name：	設定一組管理者參數可以取得此機器的項目資訊，系統預設 “Public”。
Set Community Name：	設定一組管理者參數可以設定此機器的項目資訊，系統預設 “Private”。
Trap Community Name：	設定一組管理者參數可以傳送 Trap 的資訊。
Send SNMP Trap to：	設定一組 IP 位址或是網域名稱名稱的接收 Trap 訊號主機。
確定：	點選此按鈕“確認”即會儲存剛才所變動的修改設定內容參數。
取消：	點選此按鈕“取消”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

13.5 系統恢復

您可以於此工具中選擇 VPN 防火牆系統重新開機功能，請點選“系統恢復”的“立即重新啟動”按鈕即可重新開機啟動。

系統重新啟動

如圖，如果點選系統啟用下的“立即重新啟動”,會彈出提對話方塊提示是否重新啟用 VPN 防火牆，確定 VPN 防火牆就做重新啟用操作。

重新啓動

恢復原出廠配置

恢復原出廠預設值

若是選擇重新恢復"立即恢復原出場配置"， 會彈出提對話方塊提示是否恢復出廠值，確定後 VPN 防火牆將做恢復出廠值操作。

重新啓動

恢復原出廠配置

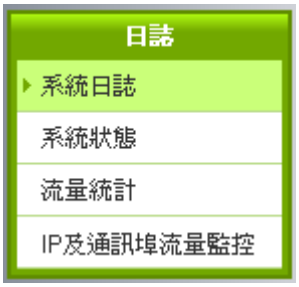
我們建議在做版本升級前請先將 VPN 防火牆現在的設定值存在電腦，等做完版本升級後，使用此功能將機器做回復出廠值設定以確保機器升級後的穩定行，然後再將剛才存在電腦的設定直存回 VPN 防火牆(如何儲存 VPN 防火牆的設定資料及升級完成後如何存回 VPN 防火牆，請參考 13.3 系統設定參數儲存說明)。

十四、日誌功能設定

日誌功能紀錄 VPN 防火牆的運行資料，並以可閱讀的方式呈現再設定視窗上提供給您作為參考。您可以依據需求檢視這些資訊。

14.1 系統日誌

VPN 防火牆的日誌記錄提供三種設定：系統日誌， 電子郵件通知，以及選擇日誌的類別。



系統日誌

啟用傳送到日誌伺服器： 若是勾選此選項的話，傳送系統日誌功能將被開啟。

系統日誌伺服器主機名稱： VPN 防火牆 提供了外部系統日誌伺服器收集系統資訊功能。系統日誌為一項工業標準通訊協定，於網路上動態擷取有關的系統資訊。VPN 防火牆 的系統日誌 提供了包含動作中的連線來源位置與目地位置，服務編號以及狀態。輸入您要接收系統日誌的伺服器名稱或是 IP 位址於"系統日誌伺服器"的空格欄位內。

E-mail 警示功能

啟用傳送到電子郵件信箱：	若是勾選此選項的話，電子郵件告警將會被開啟。
郵件伺服器：	請輸入電子郵件伺服器的名稱或是 IP 位址，如 mail.abc.com。請注意，您必須有許可權經由所填入的電子郵件伺服器寄送日誌電子郵件，否則此日誌電子郵件將無法被寄出。
電子郵件位址：	此為設定日誌收件人電子郵件信箱，例如 abc@mail.abc.com
傳送日誌數量：	自定日誌數量，系統預設為 50 條。 當到達此數量時，VPN 防火牆將會自動 Mail 傳送日誌。
傳送區隔時間：	自定傳送日誌間隔時間，系統預設為 10 分鐘。 當到達此時間時，VPN 防火牆將會自動 Mail 傳送此日誌。 VPN 防火牆將會自動判別當數量或是間隔時間哪一個參數先到達，就 Mail 傳送日誌資訊給管理者。
立即傳送日誌：	使用管理者可以直接按此按鈕傳送日誌。

系統日誌設定

VPN 防火牆提供了包含以下的告警內容資訊，您只要打勾點選即可包含在日誌資訊中。

Syn Flooding：	即在短時間內傳送大量的 syn 封包，造成系統記錄連線的記憶體溢滿。
IP Spoofing：	通過封包監聽程式來攔截網路上所傳送資料，並在讀取後藉由程式修改原發送端位址，進入原目的端的系統內，存取資源。
Win Nuke：	通過侵入或設陷阱的方式將木馬程式送入對方伺服器中。
Ping of Death：	通過傳送來產生超過 IP 協議所能夠允許的最大封包，造成系統當機。

登入認證錯誤： 當系統發現有企圖登錄 VPN 防火牆的入侵者時，就會將資訊傳到系統日誌中。

一般系統日誌資訊

VPN 防火牆 提供了包含以下的一般性內容資訊，您只要打勾點選即可。系統錯誤資訊，被阻擋的管制條例，允許通過的管制條例，認證登錄，系統設定變更。

系統錯誤訊息： 提供系統中各種錯誤給系統日誌。例如：不正確的設定或是功能異常狀況發生。

被阻擋的管制條例： 當有用戶試圖進行存取規則中不允許的規則時，此資訊會傳送到系統日誌中。

允許通過的管制條例： 當用戶進行存取規則所允許的規則時，此資訊會傳送到系統日誌中。

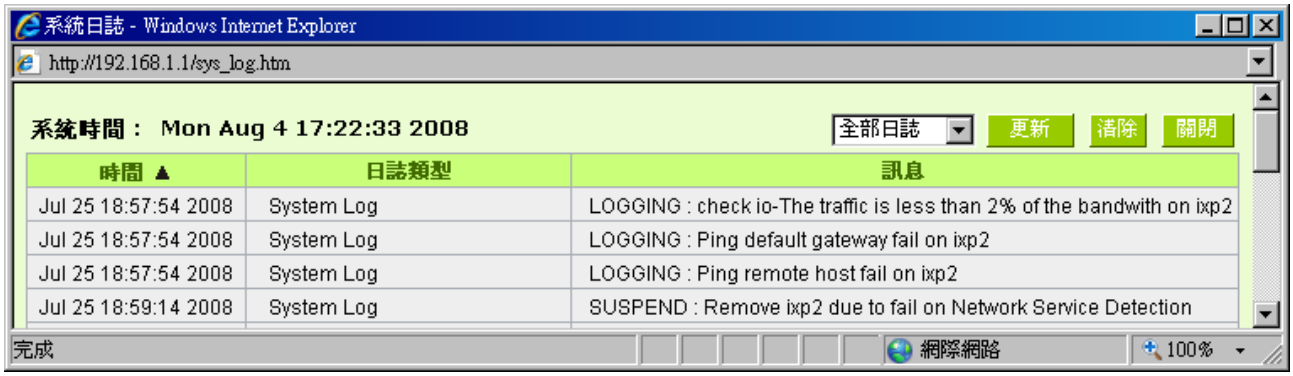
系統配置變更： 當系統的設定值改變時，此資訊回傳送到系統日誌中。

認證登入： 每一個成功登錄系統的 IP 位址都會傳送並記錄到系統日誌中。

以下有四個有關查詢日誌的按鈕，分別敘述如下：

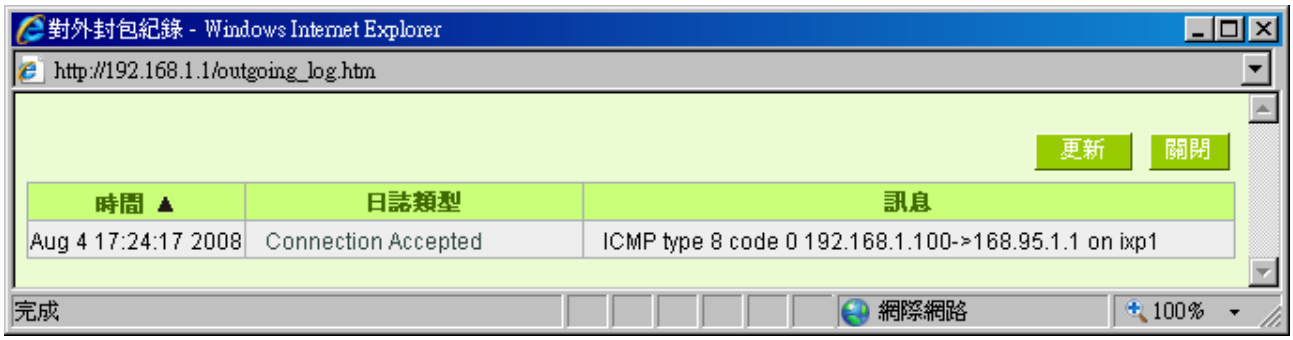
查看系統日誌：

此為查看系統日誌使用，其資訊內容可以從下拉式選單中分類讀取，包含全部日誌，系統日誌，存取日誌，防火牆日誌，VPN 日誌。選擇"刷新"按鈕可以刷新日誌顯示視窗，"清除"按鈕可以清除所有日誌記錄。如下圖所示：



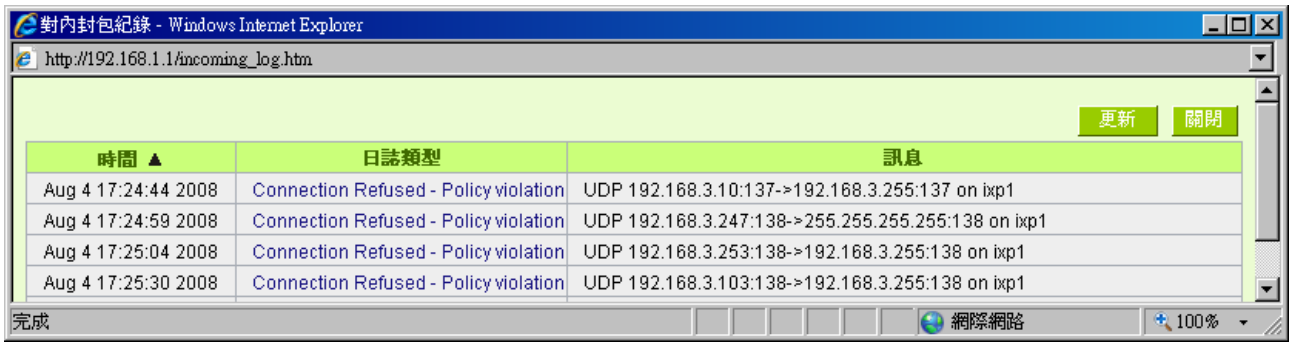
對外封包記錄：

查看內部 PC 對外部網際網路的系統封包日誌，此日誌包含內部網路位址，目的地位址以及所使用的通訊通訊埠號、類型等資訊。



對內封包記錄：

查看外部進入 VPN 防火牆的系統封包日誌，此日誌內含外部來源網路位址，目的地位址與通訊埠號等資訊。



清除日誌：

此按鈕為清除所有目前 VPN 防火牆的日誌相關資訊。

14.2 系統狀態即時監控

VPN 防火牆的系統狀態即時監控管理功能可以提供系統目前的運作資訊，包含局域或廣域埠名稱，目前埠口連線狀態，IP 位址，網路實體位置(MAC 位址)，子網路遮罩，預設閘道，網域名稱解析伺服器(DNS)，網路偵測，收到的封包數量，傳送的封包數量，全部的進出封包數量統計，收到的封包 Byte 流量統計，傳送的封包 Byte 流量統計，全部進出的封包 Byte 流量統計，收到的錯誤封包統計以及埠口丟棄的封包統計，連線數，新連線數，上傳頻寬使用率，下載頻寬使用率等資訊。

系統狀態

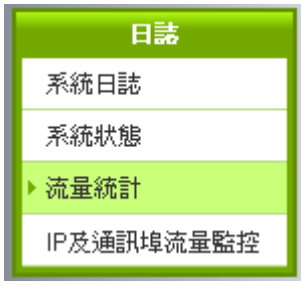
下一頁>>

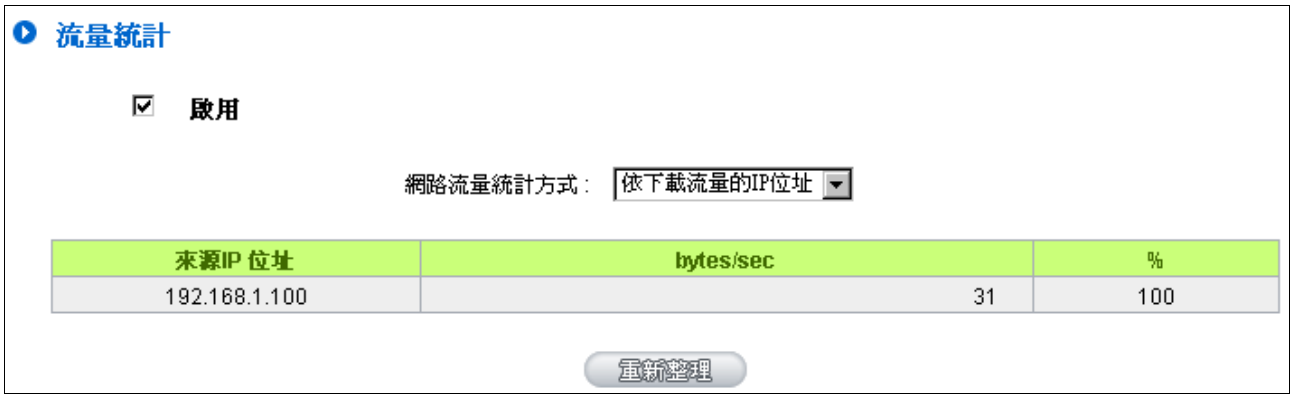
接口位置	廣域網1	廣域網2	廣域網3	廣域網4
裝置名稱	ixp1	ixp2	ixp3	ixp4
線路連線狀態	Connected	Down	Down	Down
IP 位址	192.168.3.134	0.0.0.0	0.0.0.0	0.0.0.0
MAC地址	32-10-d1-86-12-9b	3e-89-8a-a6-3d-b6	02-ad-39-1f-38-12	3c-65-62-1f-19-33
子網路遮罩	255.255.255.0	0.0.0.0	0.0.0.0	0.0.0.0
預設閘道	192.168.3.1	0.0.0.0	0.0.0.0	0.0.0.0
DNS 伺服器	192.168.3.10 192.168.3.2	0.0.0.0	0.0.0.0	0.0.0.0
線路偵測機制	Disabled	Test Failed	Test Failed	Test Failed
接收封包數	11248	0	0	0
傳送封包數	40473	0	0	40473
全部封包數	51721	0	0	0
接收封包流量(Byte)	4882	0	0	0
傳送封包流量(Byte)	8515	0	0	0
全部封包流量(Byte)	13397	0	0	0
目前接收流量Bytes/Sec	0	0	0	0
目前傳送流量Bytes/Sec	0	0	0	0
錯誤封包統計	0	0	0	0
丟棄封包統計	0	0	0	0
連線數	10	0	0	0
新連線數/秒	0	0	0	0
上傳頻寬使用率(%)	0	0	0	0
下載頻寬使用率(%)	0	0	0	0

重新整理

14.3 流量統計

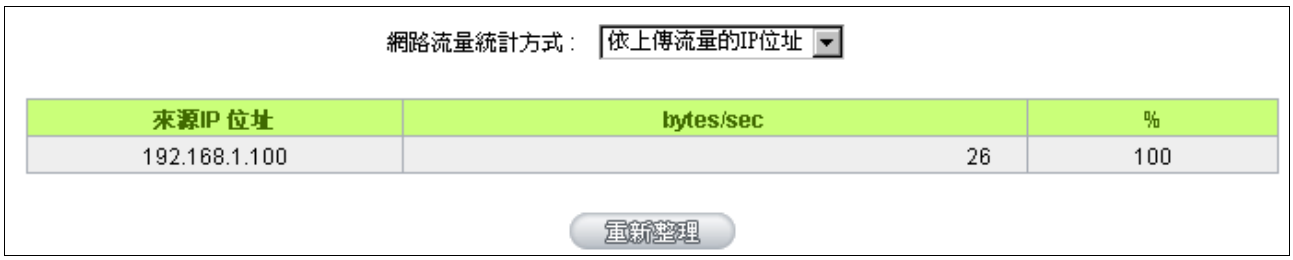
VPN 防火牆提供六種顯示流量統計的資訊，來提供管理者對於流量有更好的管理與控制。





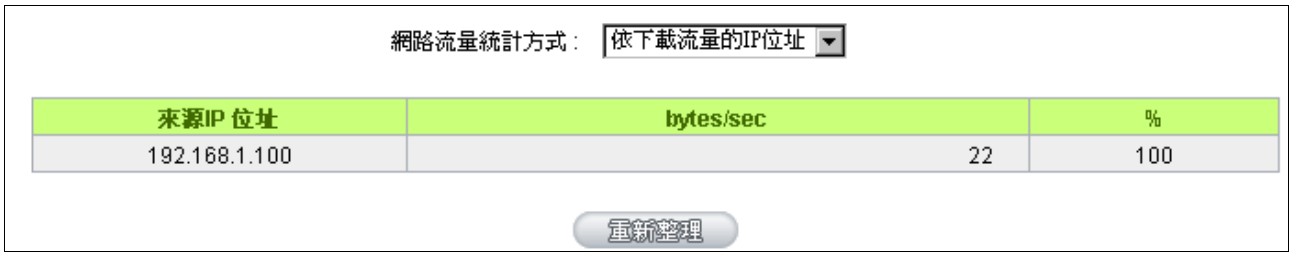
依上傳流量的 IP 位址：

在此圖表中顯示了從外進入內網流量的來源端的 IP 位址， 每秒有多少 byte 與所占的百分比。



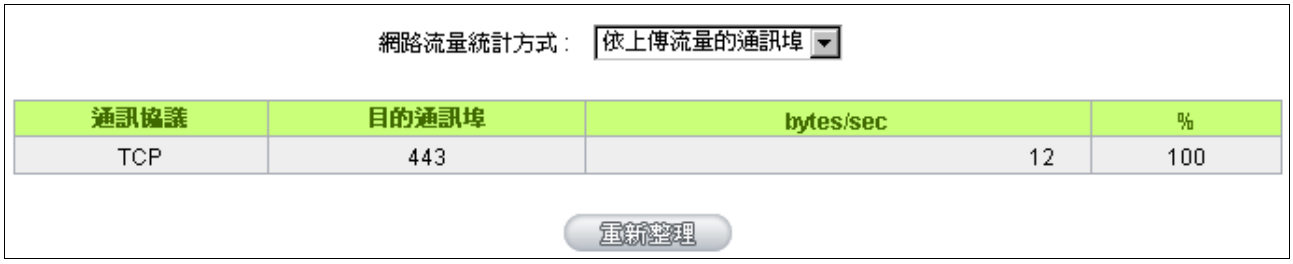
依下載流量的 IP 位址：

在此圖表中顯示了叢內網出去流量的來源端的 IP 位址， 每秒有多少 byte 與所占的百分比。



依上傳流量的通訊埠：

在此圖表中顯示了以網路的通訊埠來分類進入內網使用流量統計(每秒)byte 與百分比。



依下載流量的通訊埠：

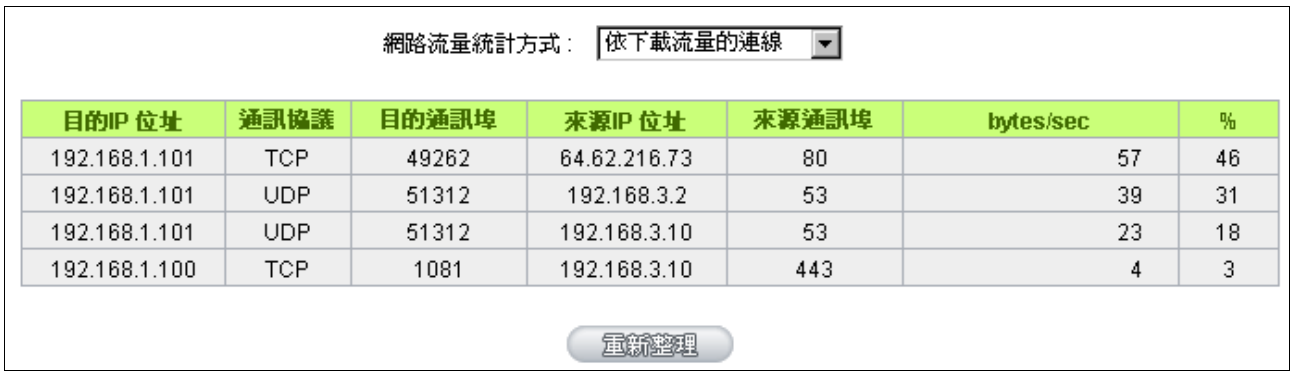
在此圖表中顯示了以網路的通訊埠來分類從內網出去的使用流量統計(每秒)byte 與百分比。

依上傳流量的連線：

在此圖表中顯示了從廣域網路進來的(Dest. IP)位址所連線的區域網路的 IP(Source IP)位置所使用的通訊埠(Dest.Port)還有現在使用流量(bytes/sec)與百分比。

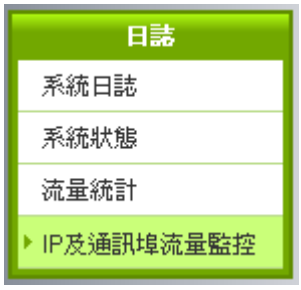
依下載流量的連線：

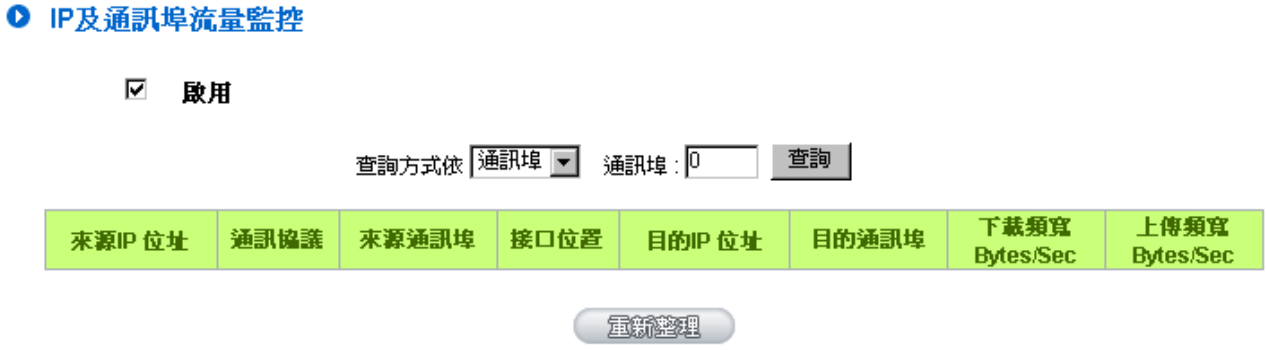
在此圖表中顯示了從區域網路的 IP(Source IP)位址對外連線的目的地位置(Dest. IP)IP 及所使用的通訊埠(Dest.Port)還有現在使用流量(bytes/sec)與百分比。



14.4 特定 IP 及通訊埠狀流量狀態

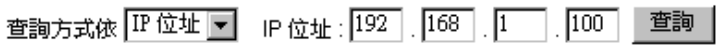
VPN 防火牆提供網管人員可以針對某一 IP 或某一特定通訊埠去查詢此 IP 去訪問的目的位址，或是有哪些人使用這個通訊埠。其目的可以方便找出某些需要認證的網站無法走多 WAN 埠而必須走單一個 WAN 埠，網管人員可以查詢出此目的地的 IP 做協議綁定來解決此登錄問題。另外，若想查詢何人在使用 BT 或 P2P 軟體，也可選擇 Port 做使用者查詢。





特定 IP 狀態：

直接在 IP 位址裏填入您想要查詢的 IP 位址，就可以顯示出此 IP 對外連線的所有目的地及通訊埠號。



來源IP 位址	通訊協議	來源通訊埠	接口位置	目的IP 位址	目的通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	4004	WAN1	207.46.109.114	1863	0	0
192.168.1.100	TCP	1065	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	1066	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	1081	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	1082	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	1799	WAN1	168.95.83.189	21	0	0
192.168.1.100	UDP	55101	WAN1	192.168.3.10	53	0	0
192.168.1.100	UDP	58732	WAN1	192.168.3.10	53	0	0

特定通訊埠狀態：

直接在通訊埠裡填入您想要查詢的埠口號，就可以顯示出此通訊埠現在有哪些 IP 正在使用。

來源IP 位址	通訊協議	來源通訊埠	接口位置	目的IP 位址	目的通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	1065	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	1066	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	1081	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	1082	WAN1	192.168.3.10	443	0	0

十五、登出

VPN 防火牆的網頁視窗右上方有一個登出的按鈕，此按鈕為結束管理 VPN 防火牆並關閉此管理視窗。若您下次想再進入 VPN 防火牆管理視窗時，您必須重複登錄 VPN 防火牆管理視窗的步驟，並輸入管理者的使用名稱與密碼。

附錄一、設定介面及使用手冊章節對照

本章主要通過表格的形式把每個章節具體對照 VPN 防火牆 Web 管理頁面的鏈結與介面對照顯示，進一步方便用戶快速的設定 VPN 防火牆，同時更加瞭解 VPN 防火牆的工作能力。

VPN 防火牆整體介面欄目次序圖如下。

一級欄目	二級欄目	對應章節
首頁		五、確定設備規格、狀態顯示以及登錄密碼和時間的設定 5.1 首頁顯示
基本設定		六、進行廣域網路連線設定
	網路設定	6.1 網路設定
	流量管理	6.2 多 WAN 設定
	協議綁定	6.2 多 WAN 設定
	虛擬邊境	十一、虛擬繞徑設定
QoS 頻寬管理		八、QoS 頻寬管理功能
	頻寬管理	8.1 頻寬設定(QoS)/ 8.3 智慧頻寬管理
	連線數管理	8.2 連線數管控
IP/DHCP 設定		七、內部區域網路設定

	DHCP 設定	7.3 DHCP 發放 IP 伺服器
	DHCP 狀態	7.4 DHCP 狀態顯示
	IP 與 MAC 綁定	7.5 IP 及 MAC 位址綁定
	IP 群組管理	7.6 IP 群組管理
防火牆設定		九、防火牆設定
	基本設定	9.1 基本設定/ 9.2 阻擋特定服務
	訪問規則設定	9.3 訪問規則設定
	內容過濾	9.4 網頁內容管制
進階設定		十二、其他進階進階功能設定
	DMZ/虛擬服務器	12.1 DMZ / 虛擬服務主機
	UPnP 通訊協定	12.2 UPnP- Universal Plug and Play
	路由通訊協定	12.3 路由通訊協定
	一對一 NAT	12.4 一對一 NAT
	動態網域名稱服務	12.5 DDNS-動態網域名稱解析
	廣域網 MAC 位址設定	12.6 廣域網接口 MAC 位址設定
系統工具		十三、工具程式功能設定/五、確定設備規格、狀態顯示以及登錄密碼和時間的設定
	密碼設定	5.2 登錄密碼和時間的設定
	自我診斷	13.1 線上連線測試
	軟體更新	13.2 系統硬體升級
	設定參數備份/恢復	13.3 系統設定參數儲存
	SNMP 網路管理	13.4 網路管理設定(SNMP)
	時間設定	5.2 登錄密碼和時間的設定
	系統恢復	13.5 系統恢復
實體埠口管理（預計未來加入）		七、內部區域網路設定
	埠口設定	7.1 網路埠口管理設定(預計未來加入)
	埠狀態即時顯示	7.2 網路埠口狀態即時顯示(預計未來加入)
VPN 虛擬私有網設定		十、VPN 虛擬私有網
	VPN 狀態	10.1.1 目前所有 VPN 狀態
	閘道對閘道設定	10.1.2.1 閘道對閘道設定
	用戶端對閘道設定	10.1.2.2 用戶端對閘道設定
	PPTP 設定	10.1.3 PPTP 設定與狀態
	PPTP 狀態	10.1.3 PPTP 設定與狀態

	VPN 數據包穿透	10.1.4 VPN 封包穿透防火牆功能
QnoKey		10.2 QnoKey 設定
	設定與連接狀態	10.2.1 -10.2.3 QnoKey 群組與用戶設定
QVM VPN		10.3 QVM VPN 功能設定
	QVM 設定	10.3.1 QVM VPN 中心伺服器端設定 10.3.3 QVM VPN 用戶端設定
	QVM 狀態 (伺服器)	10.3.2 QVM VPN 中央控管功能
日誌		十四、日誌功能設定
	系統日誌	14.1 系統日誌
	系統狀態	14.2 系統狀態即時監控
	流量統計	14.3 流量統計
	IP/埠流量監控	14.4 特定 IP 及埠狀態

附錄二：常見問題解決

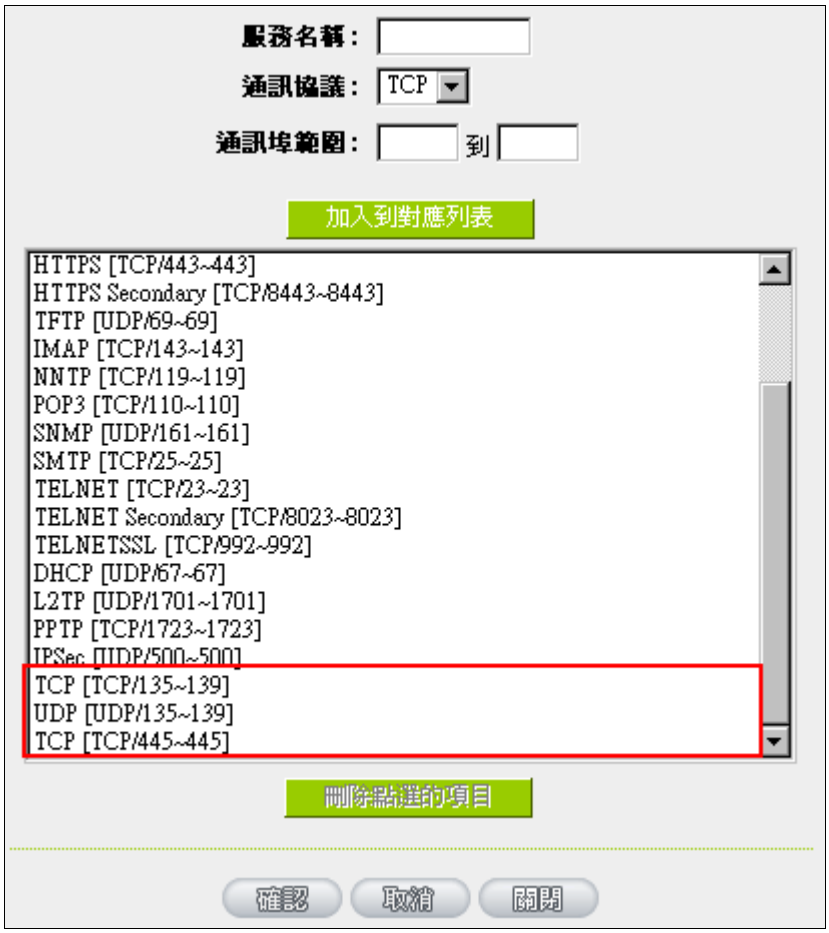
（1）封鎖用戶下載 BT 種子

若您想要封鎖 BT 種子，不讓用戶下載，您可以直接在 "防火牆設定" > "設定禁止連接的網域" 啟用 "網頁內容過濾(關鍵字)" 後將 "關鍵字" 打入".torrent"這樣就可以防止用戶下載種子。

（2） 衝擊波及蠕蟲病毒的防制

由於近來還是發生有許多用戶區域網中衝擊波及蠕蟲病毒造成區域網訪問網際網路很慢及連線數(Session)大量增加造成 VPN 防火牆大量處理，以下將指導您封鎖此些病毒相對應埠以達到防制目的。

a.增加此 TCP135-139， UDP135-139 還有 TCP445 通訊埠：



b.用防火牆裏面的"存取規則"功能將設定好的此三組埠 "封鎖"：

存取規則設定

管制動作：	禁止
通訊埠：	TCP[TCP/135~139] 通訊埠設定
日誌：	關閉
接口位置：	Any
來源IP 位址：	Any
目的IP 位址：	Any

時間排程設定

管制時間爲 所有時間	: 到 : (24小時制)
每天	Sun Mon Tue Wed Thu Fri Sat

返回 確認 取消

用同樣的方法添加好 UDP[UDP135~139]以及 TCP[445~445]通訊埠。

c.將這三組的優先順序至於最高：

跳到 1 / 2 頁　　每頁顯示 5 筆　　下一頁>>

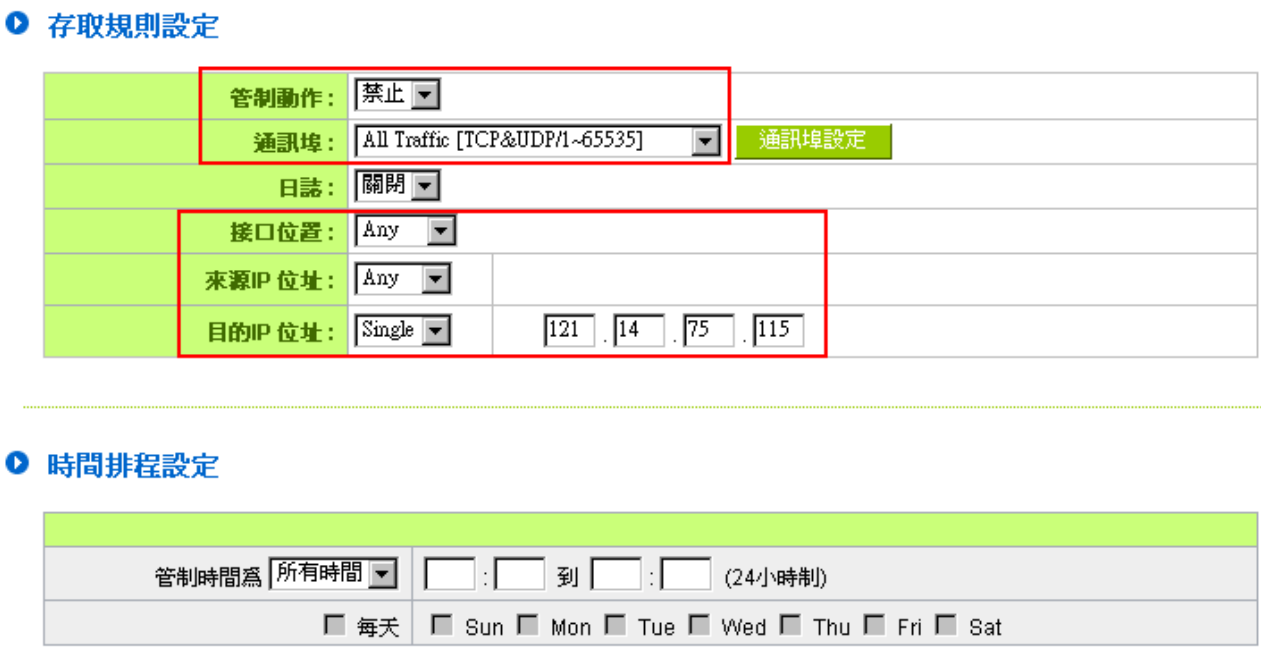
優先權	啓用	管制動作	通訊埠	接口位置	來源IP 位址	目的IP 位址	管制時間	日	編輯	刪除
1	☑	Deny	TCP [445]	*	Any	Any	Always		Edit	
2	☑	Deny	UDP [135]	*	Any	Any	Always		Edit	
3	☑	Deny	TCP [135]	*	Any	Any	Always		Edit	
	☑	Allow	All Traffic [*]	LAN	Any	Any	Always			
	☑	Deny	All Traffic [*]	WAN1	Any	Any	Always			

加入新規則 回復出廠預設值

（3） 阻止 QQLive 視屏直播設定

QQLive 視屏直播軟體是一種流媒體點播軟體，最近好多客戶都在頭痛一個同樣的問題，當區域網有多個用戶使用 QQLive 視屏直播軟體，佔用了比較大的頻寬，造成 VPN 防火牆的負擔過重，使得 VPN 防火牆反應遲鈍或癱瘓，如果我們能夠封鎖 QQLive 的伺服器登錄過程就可以解決這樣的問題，下面就這個問題來結合 Qno 產品的相關功能提出相關的解決方案，來進行 VPN 防火牆設定。

a). 進入 VPN 防火牆 Web 管理頁面，再進入"防火牆設定"的"訪問存取規則設定"。



b). 再點選"增加新的管制規則"，進入"訪問存取規則設定"頁面，在"存取服務規則設定"中的"管制動作"選項中選擇"禁止"，再在"伺服器埠" 選擇"所有埠[TCP&UDP/1~65535]"，選擇"來源接口"為"任何的"，"來源 IP 位址"選擇"任何的"（有相關需求的用戶可以選擇"單獨"或"範圍" 阻止單個 IP 或者一段 IP 的 QQLive 的的登錄），再在"目的 IP 位址"選擇"單獨"填入 QQLive 伺服器的 IP 位址"121.14.75.115"（QQLive 伺服器的 IP 位址不止一個，後面需要重複添加），最後在"時間管制設定"的"此存取規則"選擇"所有時間"對上 QQLive 的登錄時間進行設定（如有需要可以具體設定相關時間的設定），"確定"後進入下一步驟。

c). 重複以上的操作在只替換"目的 IP 位址"裏分別填入以下 IP 位址：

121.14.75.115

60.28.234.117

60.28.235.119

222.28.155.17

可封鎖的 QQ Live 版本：QQ Live 2008 (7.0.4017.0)

測試日期:2008-07-29

重複添加後可以看到相關 QQ Live 的伺服器的連接被封鎖，點擊確認完成對阻止 QQ Live 視頻直播設定

（4） ARP 病毒攻擊防制

1. ARP 問題的提出以及相關知識

近期，國內多家網咖出現短時間內斷線(全斷或部分斷)的現象，但會在很短的時間內會自動恢復。這是因為 MAC 位址衝突引起的，當帶毒機器的 MAC 映射到主機或者 VPN 防火牆之類的 NAT 設備，那麼全網斷線，如果只映射到網內其他機器，則只有這部分機器出問題。多發於傳奇遊戲特別是外掛程式等方面。此類情況就是網路受到了 ARP 病毒攻擊的明顯表現，其目的在於，該病毒破解遊戲加密解密演算法，通過截取區域網中的封包，然後分析遊戲通訊協定的方法截獲用戶的資訊。運行這個病毒，就可以獲得整個區域網中遊戲玩家的詳細資訊，盜取用戶帳號資訊。下面我們談談如何防制這種攻擊。

首先，我們瞭解下什麼是 ARP，ARP "Address Resolution Protocol"（位址解析協定），區域網中，網路中實際傳輸的是"訊框"，封包裏面是有目標主機 MAC 位址的。所謂"位址解析"就是主機在發送封包前將目標 IP 位址轉換成目標 MAC 位址的過程。ARP 協定的基本功能就是通過目標設備的 IP 位址，查詢目標設備的 MAC 位址，以保證通信的順利進行。

ARP 協議的工作原理：在每台安裝有 TCP/IP 協定的電腦裏都有一個 ARP 暫存表，表裏的 IP 位址與 MAC 位址是一一對應的，如表所示。

IP 址	MAC 位址
192.168.1.1	00-0f-3d-83-74-28
192.168.1.2	00-aa-00-62-c5-03
192.168.1.3	03-aa-01-75-c3-06
……	……

我們以主機 A（192.168.1.5）向主機 B（192.168.1.1）發送資料為例。當發送資料時，主機 A 會在自己的 ARP 暫存表中尋找是否有目標 IP 位址。如果找到了，也就知道了目標 MAC 位址，直接把目標 MAC 位址寫入訊框裏面發送就可以了；如果在 ARP 暫存表中沒有找到相對應的 IP 位址，主機 A 就會在網路上發送一個廣播，目標 MAC 位址是"FF.FF.FF.FF.FF.FF"，這表示向同一網段內的所有主機發出這樣的詢問："192.168.1.1 的 MAC 位址是什麼？"網路上其他主機並不回應 ARP 詢問，只有主機 B 接收到這個訊框時，才向主機 A 做出這樣的回應："192.168.1.1 的 MAC 位址是 00-aa-00-62-c6-09"。這樣，主機 A 就知道了主機 B 的 MAC 位址，它就可以向主機 B 發送資訊了。同時它還更新了自己的 ARP 暫存表。

再者，我們先簡單介紹一下什麼是 ARP 病毒攻擊，這種病毒是對區域網的 PC 進行攻擊，使區域網 PC 機的 ARP 表混亂，在區域網中，通過 ARP 協定來完成 IP 位址轉換為第二層實體位址（即 MAC 位址）的。ARP 協定對網路安全具有重要的意義。通過偽造 IP 位址和 MAC 位址實現 ARP 欺騙，能夠在網路中產生大量的 ARP

通信量使網路阻塞。進行 ARP 復位向和攻擊。用偽造源 MAC 位址發送 ARP 回應封包，對 ARP 快取記憶體機制的攻擊。這些情況主要出現在網咖用戶，造成網咖部分機器或全部機器暫時掉線或者不可以上網，在重新啟用後可以解決，但保持不了多久有會出現這樣的問題，網咖管理員對每台機器使用 arp –a 命令來檢查 ARP 表的時候發現 VPN 防火牆的 IP 和 MAC 被修改，這就是 ARP 病毒攻擊的典型症狀。

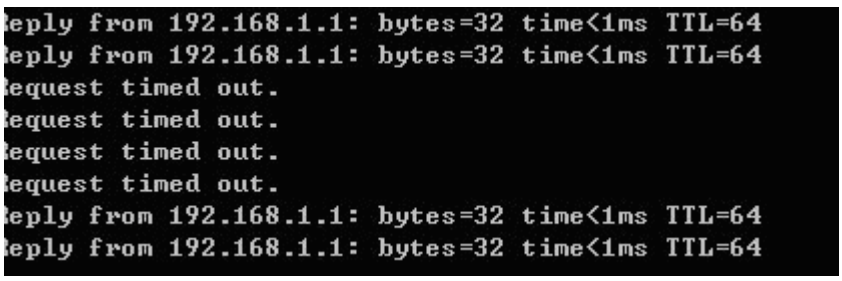
這種病毒的程式如 PWSteal.lemir 或其變種，屬於木馬程式/蠕蟲類病毒，Windows 95/98/Me/NT/2000/XP/2003 將受到影響，病毒攻擊的方式對影響網路連接暢通來看有兩種，對 VPN 防火牆的 ARP 表的欺騙和對區域網 PC 閘道的欺騙，前者是先截獲閘道資料，再將一系列的錯誤的區域網 MAC 資訊不停的發送給 VPN 防火牆，造成 VPN 防火牆發出的也是錯誤的 MAC 位址，造成正常 PC 無法收到資訊。後者 ARP 攻擊是偽造閘道。它先建立一個假閘道，讓被它欺騙的 PC 向假閘道發資料，而不是通過正常的 VPN 防火牆途徑上網。在 PC 看來，就是上不了網了，"網路斷線了"。

就這兩種情況而言，如果對 ARP 病毒攻擊進行防制的話我們必須得做 VPN 防火牆方面和用戶端雙方的設定才保證問題的最終解決。所以我們選擇 VPN 防火牆的話最好看看 VPN 防火牆是否帶有防制 ARP 病毒攻擊的功能，Qno 產品正好提供了這樣的功能，相比其他產品操作簡單易學。

2. ARP 的判斷

如過網路中有一台或多台電腦受到或已經感染了 ARP 病毒，我們就必須學會判斷並採取相應的解決方法處理類似問題的發生，下面來談談 Qno 技術工程師的 ARP 防制經驗談。

通過對 ARP 工作原理得知，如果系統 ARP 暫存表被修改不停的通知 VPN 防火牆一系列錯誤的區域網 IP 或者乾脆偽造一個假的閘道進行欺騙的話，網路就肯定會出現大面積的掉線問題，這樣的情況就是典型的 ARP 攻擊，對遭受 ARP 攻擊的判斷，其方法很容易，你找到出現問題的電腦點開始運行進入系統的 DOS 操作。pingVPN 防火牆的 LAN IP 逾時情況。輸入 ping 192.168.1.1（閘道 IP 位址），如圖。



區域網 pingVPN 防火牆的 LAN IP 有逾時，然後又連上，這很有可能是中了 ARP 攻擊。為了進一步確認，我們可以通過查找 ARP 表來判斷。輸入 ARP -a 命令，顯示如下圖。

```
Interface: 192.168.1.72 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0f-3d-83-74-28     dynamic
  192.168.1.43          00-13-d3-ef-b2-0c     dynamic
  192.168.1.252         00-0f-3d-83-74-28     dynamic

C:\WINDOWS\System32>arp -a
```

可以看出 192.168.1.1 位址和 192.168.252 位址的 IP 的 MAC 位址都是 00-0f-3d-83-74-28，很顯然，這就是 ARP 欺騙造成的。

3. ARP 的解決

我們現在已經理解了 ARP，ARP 欺騙攻擊以及如何判斷此類攻擊，下面的問題就是如何找到行之有效的防制辦法來防止這類攻擊對網路造成的危害。Qno 的一般處理辦法分三個步驟來完成。

a)、啟用防止 ARP 病毒攻擊：

輸入 VPN 防火牆 IP 位址，登陸 VPN 防火牆的 Web 管理頁面，進入"防火牆設定"的"基本設定"，再在右邊找到"防止 ARP 病毒攻擊"在這一行的"啟用"前面做點選，再在頁面最下點選"確認"，如圖。

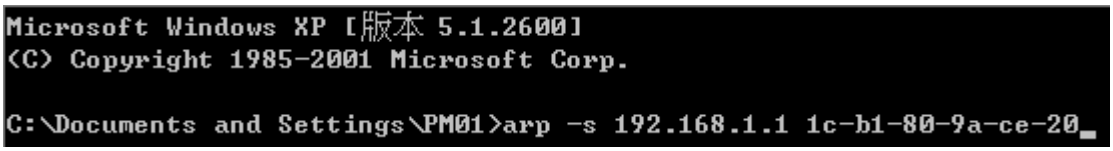
b)、對每台 PC 上綁定閘道的 IP 和其 MAC 位址

進行這樣的操作主要防止 ARP 欺騙閘道 IP 和其 MAC 位址首先在 VPN 防火牆端查找閘道 IP 與 MAC 位址，如圖。

區域網路設定

MAC地址：	1c - b1 - 80 - 9a - ce - 20 (預設值: 1c-b1-80-9a-ce-20)
閘道位址：	192 . 168 . 1 . 1
子網路遮罩：	255 . 255 . 255 . 0

然後在每台 PC 機上開始/運行 cmd 進入 dos 操作，輸入 arp –s 192.168.1.1 1c-b1-80-9a-ce-20，Enter 後完成 pc01 的綁定。如圖



針對網路內的其他主機用同樣的方法輸入相應的主機 IP 以及 MAC 位址完成 IP 與 MAC 綁定。但是此動作，如果重起了電腦，作用就會消失，所以可以把此命令做成一個批次檔案，放在作業系統的啟用裏面，批次檔案可以這樣寫：

@echo off

arp -d

arp –s VPN 防火牆 LAN IP　VPN 防火牆 LAN MAC

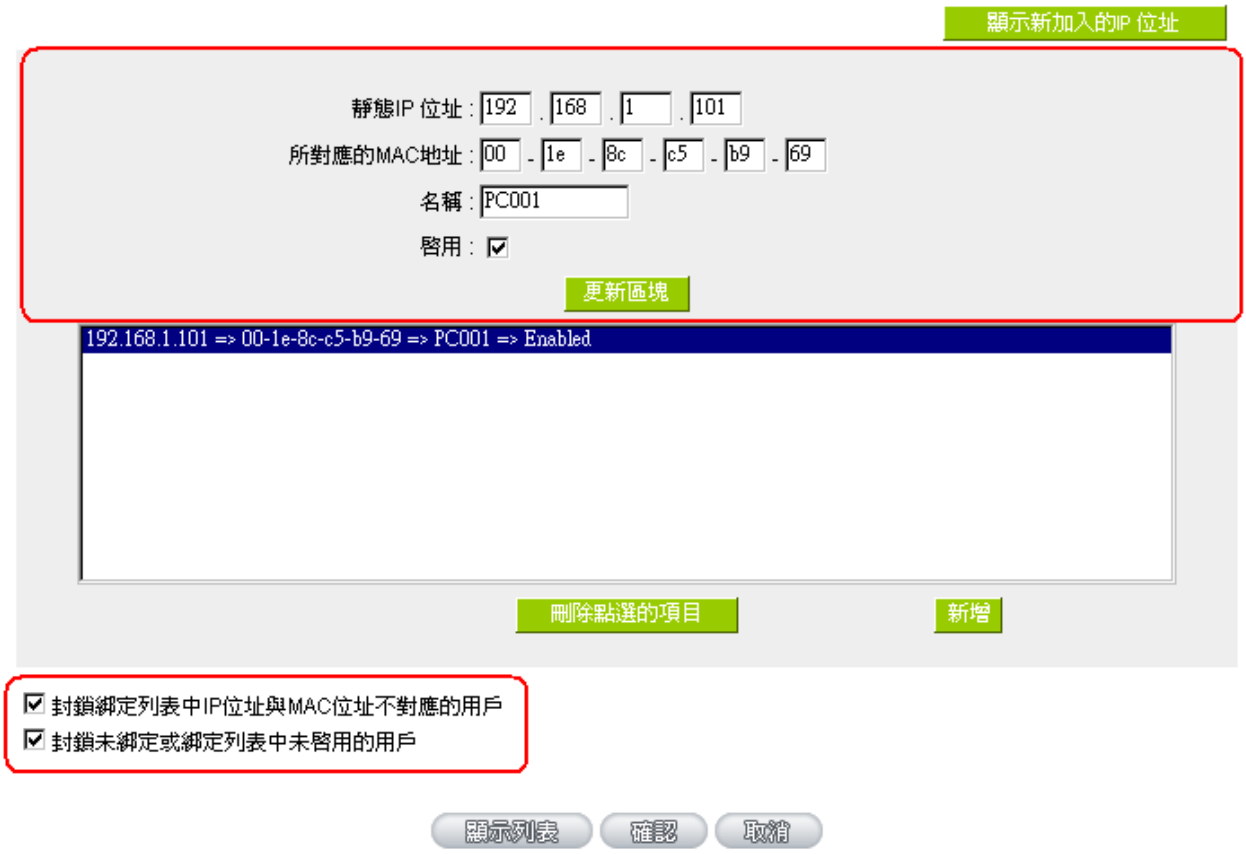
對於已經中了 arp 攻擊的區域網，要找到攻擊源。方法：在 PC 上不了網或者 ping 丟包的時候，在 DOS 下打 arp –a 命令，看顯示的閘道的 MAC 位址是否和 VPN 防火牆真實的 MAC 相同。如果不是，則查找這個 MAC 位址所對應的 PC，這台 PC 就是攻擊源。

其他的 VPN 防火牆用戶的解決方案也是要在 VPN 防火牆和 PC 機端進行雙向綁定 IP 位址與 MAC 位址來完成相應防制工作的，但在 VPN 防火牆端和 PC 端對 IP 位址與 MAC 位址的綁定比較複雜，需要查找每台 PC 機的 IP 位址與 MAC 加大了工作量，操作過程中還容易出錯。

c)、在 VPN 防火牆端綁定用戶 IP/MAC 位址：

進入"IP / DHCP 設定功能"，可以看到"IP 與 MAC 綁定"，你可以在此添加 IP 與 MAC 綁定，輸入相關參數，在"啟用"上點 "√" 選再"添加到對應列表"，重複操作添加區域網裏的其他 IP 與 MAC 的綁定，再點頁面最下的"確定"。

IP與MAC綁定

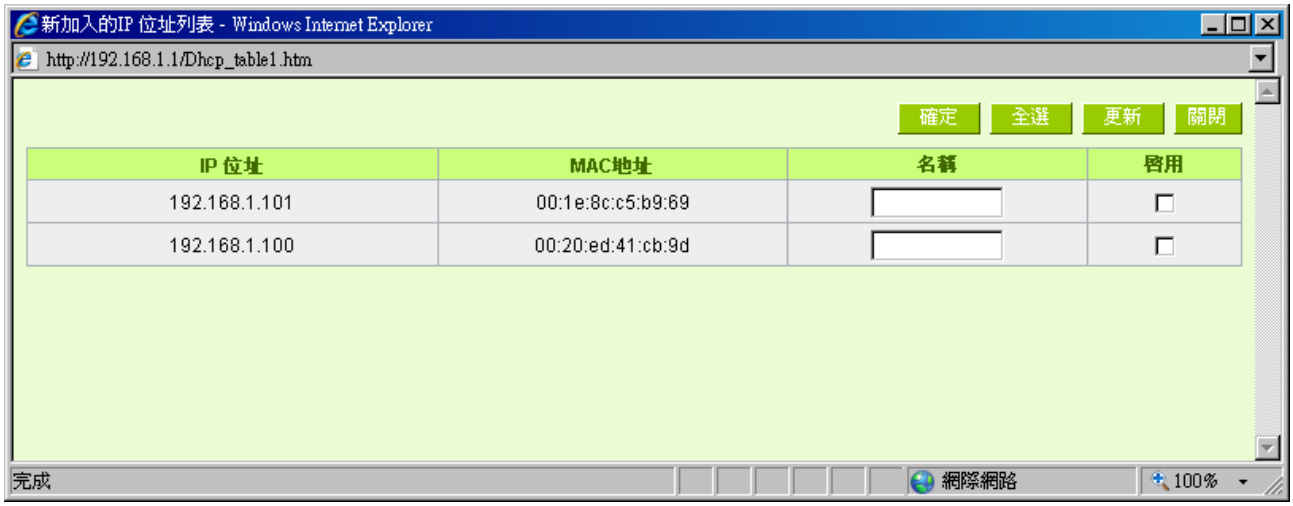


當添加了對應列表之後，其對應的資訊就會在下麵的白色框裏顯示出來。不過建議不採用此方法，這樣操作需要查詢網路內所有主機 IP/MAC 位址工作量繁重，還有一種方法來綁定 IP 與 MAC，操作會相對容易，可以減少大量的工作量，節約大量時間，下面就會講到。

進入"IP / DHCP 設定"的"IP 與 MAC 綁定"右邊有一個"顯示新加入的 IP 位址"點選進入。

IP與MAC綁定

點選之後會彈出 IP 與 MAC 綁定列表對話方塊，此對話方塊裏會顯示網內未做綁定的 pc 的 IP 與 MAC 位址對應情況，輸入電腦"名稱"和"啟用"上 "√" 選，再在右上角點確定。



此時你所綁定的選項就會出現在 IP 與 MAC 綁定列表框裏，如圖 5 再點選"確認"綁定完成。

但是我們單靠這樣的操作基本可以解決問題，但 Qno 的技術工程師建議通過進一步通過一些手段來進一步控制 ARP 的攻擊。

1、病毒源，對病毒源頭的機器進行處理，殺毒或重新裝系統。此操作比較重要，解決了 ARP 攻擊的源頭 PC 機的問題，可以保證區域網免受攻擊。

2、網咖管理員檢查區域網病毒，安裝防毒軟體，對機器進行病毒掃描。

3、給系統安裝更新程式。通過 Windows Update 安裝好系統更新程式(關鍵更新、安全更新和 Service Pack)

4、給系統管理員帳戶設定足夠複雜的強密碼，最好能是 12 位元元以上，字母+數位元+符號的組合；也可以禁用/刪除一些不使用的帳戶

5、經常更新防毒軟體（病毒碼），設定允許的可設定為每天定時自動更新。安裝並使用網路防火牆軟體，

網路防火牆在防病毒過程中也可以起到至關重要的作用，能有效地阻擋自來網路的攻擊和病毒的入侵。部分盜版 Windows 用戶不能正常安裝更新，不妨通過使用網路防火牆等其他方法來做到一定的防護

6、關閉一些不需要的服務，條件允許的可關閉一些沒有必要的共用，也包括 C$、D$等管理共用。完全單機的用戶也可直接關閉 Server 服務

7、不要隨便點選打開 QQ、MSN 等聊天工具上發來的連結資訊，不要隨便打開或運行陌生、可疑檔和程式，如郵件中的陌生附件，外掛程式等。

4. 總結

ARP 攻擊防制是一個任重而道遠的過程，以上方法基本可以解決 ARP 病毒攻擊對網路造成相關問題，而且客戶採取類似的方法也收到了很大的效果，但還是提醒網落管理人員必須高度重視這個問題，而且不能大意馬虎，我們可以採取以上建議隨時警惕 ARP 攻擊，以減少受到的危害，提高工作效率，降低經濟損失。

附錄三：Qno 技術支援資訊

更多有關俠諾產品技術資訊，除了可以登錄俠諾寬頻討論區、三照 FTP 伺服器的相關實例；或是進一步聯繫俠諾各經銷商技術部門、或俠諾大陸技術中心取得相關協助。

俠諾科技官方網站：http：//www.Qno.com.tw

各大經銷商服務聯繫方式：

用戶可以登錄網站先上服務頁面查詢各大經銷聯繫方法：

http：//www.qno.com.tw/web/where_buy.asp

台灣技術中心：

電子郵件信箱：QnoFAE@qno.com.tw