1WAN 2LAN VPN 防火牆

具頻寬管理，VPN 與網路安全功能

繁體中文使用手冊

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】所有設置參數均為範例，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置方式，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。

大綱

一、簡介 (Introduction)

1WAN 2LAN VPN 防火牆（以下稱 VPN 防火牆）是一台為小型企業，地區分公司，以及政府學校部門單位等級而設計，符合經濟實惠且高效能整合的全功能 VPN 防火牆。此 VPN 防火牆具備一個 WAN port，WAN 端的對外連線能力滿足絕大多數寬頻市場都適用的規格。局域端 (LAN)內建兩埠 10/100Mbps 乙太網路交換器 (2Port 10BasedT/TX Ethernet Switch)，每個埠口都可以連接額外的交換器以連接更多的上網設備。

VPN 防火牆內建防火牆系統，以滿足多數企業對防禦外部網路攻擊的市場需求。防火牆系統除了 NAT 之外，還具備有防止阻斷服務攻擊 (DoS， Denial of Service)，以及封包主動偵測檢驗技術(Stateful Packet Inspection)，可以預設自動偵測並阻擋外部網路攻擊。

以虛擬私有網路通道加密安全連線 (IPSec VPN， IP Security Virtual Private Network)為主的 VPN 功能，支援 DES (56bit) & 3DES(168bit) 的加密方式，以及 MD5 & SHA 的資料認證模式。VPN 防火牆同時內建有俠諾科技獨特的 SmartLink 快速建立 VPN 加密通道的 QVM 用戶端功能，可以與具有 QVM 服務器(QVM Server)的 VPN 防火牆建立 QVM 連線。

網路地址轉換 Network Address Translation (NAT) 除了可以做私網與公網的 IP 轉換，讓您只需要一個公網 IP(Public IP)就可以讓多人同時連上網際網路。此外，包含虛擬伺服器等 NAT 應用功能，讓網路環境架構具有彈性，易於規劃管理。局域網內的 IP 位址支援 Class C 等級。作業系統應支援多工模式 (multi-task)，並佔用較少記憶體。

VPN 防火牆具有進階的存取規則的設定 (Access Rule)，可讓管理者選擇應該禁止或開放存取的網路服務，以避免佔用網路資源，或是不當使用而遭受潛在的危機。

除了上述的功能之外，VPN 防火牆還具備同級產品所沒有的流量與優先權 (Rating & Priority) 管理，可以讓管理者對有限的網路資源做合理而且有效的分配，達成最有效率的運用。這些管理工具容易理解與設定，可讓網路管理者對 Internet 存取資源管理有明確的策略。同時，透過線上多樣化的日誌 (SysLog) 紀錄，管理者可以清楚的知道網路活動，以此來調整設定，達到網路的使用更安全且更有效率。

二、硬體安裝 (Hardware Installation)

本章介紹產品的硬體介面以及實體安裝。

2.1 VPN 防火牆 LED 顯示燈

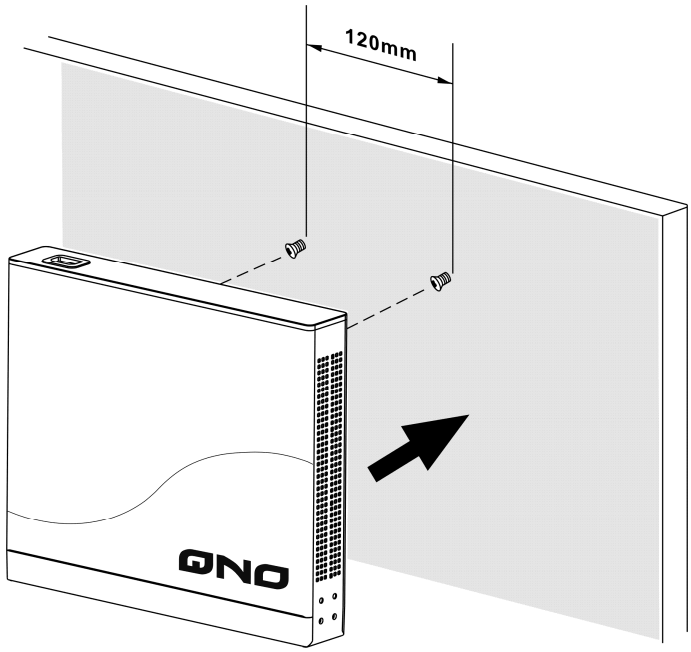
LED 燈號說明

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	綠燈	綠燈亮： 乙太網路連線正常
		綠燈閃爍： 乙太網路埠口正在傳送/接收封包資料傳輸
Speed-速度	綠燈	綠燈亮： 乙太網路連線在 100Mbps 的速度
		綠燈熄滅： 乙太網路連線在 10Mbps 的速度
Connect-網際網路	綠燈	綠燈亮： 廣域端口已經連線並取得 IP 位址

硬體回復 (Reset) 按鍵

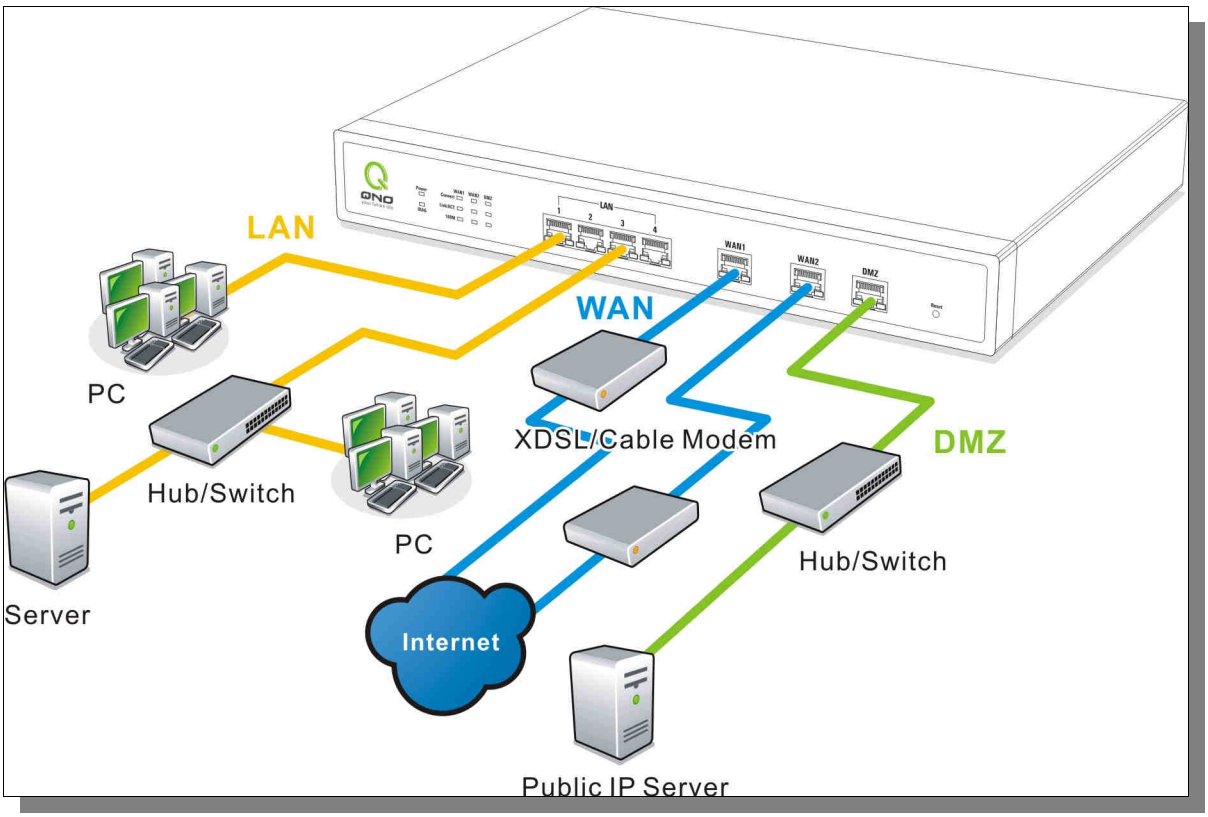
Action	Description
按下 Reset 按鈕 5 秒	熱開機，重新啟動 VPN 防火牆
	DIAG 燈號： 橘色燈號慢慢閃爍
按下 Reset 按鈕 10 秒以上	回復原出廠預設值(Factory Default)
	DIAG 燈號： 橘色燈號快閃

將 VPN 防火牆安裝在牆上



2.2 連接 VPN 防火牆到你的網路上

VPN 防火牆設計了一個可選擇作為 WAN2 或是 DMZ 的廣域網接口 (此功能是經由軟體設定，在下一章節的基本設定中會說明)，因此連接 VPN 防火牆到你的網路上的拓墣如下：



廣域網路連線(WAN connection)： WAN 埠口可以連接如 xDSL Modem，Switch HUB 或是外部路由器。

區域網路連線(LAN connection)： LAN 埠口可以連接如 Switch HUB 或是直接與 PC 連線。

DMZ 埠口： 當設定為 DMZ 模式時，此埠口可以連接具有外部合法 IP 位置的伺服器， 如網頁 (Web) 伺服器以及電子郵件伺服器(Mail servers)等。

三、快速連網設定 (Quick Configuration)

本章介紹登入軟體設定畫面，說明首頁的顯示訊息，以及基本連網設定。

3.1 登入到軟體設定畫面

在連接到 VPN 防火牆 LAN 端的電腦上開啟網頁瀏覽器 (如 IE)，在網址欄輸入 192.168.1.1 (VPN 防火牆的預設網關)，會出現以下的登入畫面：

VPN 防火牆預設的使用者名稱(User Name)與使用者密碼(Password)皆為”admin”，您可以於稍後設定時更改此登入密碼。

注意！

為了安全理由，我們強烈建議您務必在登入之後更改管理密碼！密碼請牢記，若是密碼忘記，將無法再登入至 VPN 防火牆的設定畫面，必須回復到出廠值(Factory Default)。

3.2 首頁顯示 (Home)

首頁 (Home)顯示 VPN 防火牆目前系統所有參數以及狀態顯示資訊。若您想進一部查詢該細部相關設定的話，可以按下各細部選項前端(有底線的文字)的超連結按鈕，即可快速立即進入該選項設定當中。

3.2.1 系統訊息

產品序號：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。

中央處理器：此為顯示 VPN 防火牆 使用的 CPU。

運作時間：此為顯示 VPN 防火牆 目前已經開機的時間。

系統時間：此為顯示 VPN 防火牆 目前正確時間，但是必須注意，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。

3.2.2 實體埠口配置狀態

實體埠口配置狀態

埠口號	1	2	DMZ	Internet
接口位置	區域網		DMZ	廣域網
狀態	啟用	啟用	啟用	連線

在此畫面會顯示系統各埠口(Port)目前即時狀態顯示 (連線-已經連接， 啟用-開啟，關閉)。

3.2.3 一般設定狀態顯示(General Setting Status)

基本項目配置狀態顯示

區域網閘道IP位址：	192.168.1.1	
廣域網 IP位址：	220.130.188.49	釋放 更新
DMZ IP：	0.0.0.0	
預設閘道IP位址(廣域網)：	220.130.188.97	
DNS(廣域網)：	168.95.1.1	

區域網接口 IP 位置(LAN IP)： 此為顯示 VPN 防火牆本身的 LAN 端目前 IP 位置，系統預設為 192.168.1.1，可以按下該超連結直接進入該設定項目中做修改。

廣域網接口 IP 位置(WAN1 IP)： 此為顯示 VPN 防火牆的 WAN 1 端目前的 IP 位置資訊，並且可以按下該超連結直接進入該設定項目中。當使用者選擇自動取得 IP 位置時(Obtain an IP automatically)，他會顯示二個按鈕分別為釋放-release 與更新-renew。使用者可以按下釋放- release 按鈕去做釋放 ISP 端所核發的 IP 位置，以及按下更新- renew 按鈕去做更新 ISP 端所核發的 IP 位置。當選擇 WAN 端連線使用如 PPPoE 或是 PPTP 的話，它會變為顯示”連接”-Connect 與”中斷連線”-Disconnect。

DMZ IP： 此為顯示 VPN 防火牆的 DMZ 目前的 IP 位置設定資訊，並且可以按下該超連結直接進入該設定項目中。

預設閘道 IP 位址 (Default Gateway)： 此為顯示路 ISP 分配給 VPN 防火牆 WAN1 及 WAN2 的網關 IP 位置資訊，並且可以按下該超連結直接進入該設定項目中。

網域名稱解析服務位置 (DNS)： 此為顯示 VPN 防火牆的 DNS(Domain Name Server)的 IP 位置資訊，並且可以按下該超連結直接進入該設定項目中。

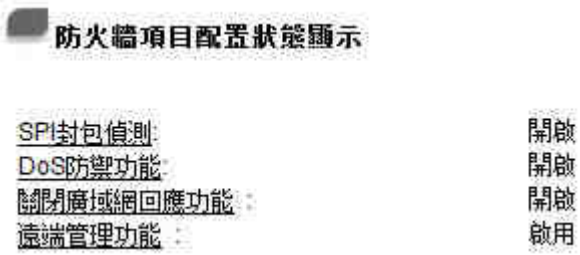
3.2.4 進階設定狀態顯示

DMZ Host： 此為顯示 VPN 防火牆的 DMZ 功能選項是否啟動，並且可以按下該超連結直接進入該設定項目中。系統預設此功能為關閉。

路由器工作模式： 此為顯示 VPN 防火牆的目前工作模式(可為 NAT Gateway 或是 Router 路由模式)，並且可以按下該超連結直接進入該設定項目中.系統預設此功能為 NAT Gateway 模式。

動態網域解析服務(DDNS)： 此為顯示 VPN 防火牆的 DDNS 動態 DNS 功能選項是否啟動，並且可以按下該超連結直接進入該設定項目中。系統預設此功能為關閉。

3.2.5 防火牆設定狀態顯示



主動封包偵測過濾防火牆功能 SPI (Stateful Packet Inspection)： 此為顯示 VPN 防火牆的 SPI(Stateful Packet Inspection)主動封包偵測過濾防火牆功能選項是否開啟 (開啟-On/關閉-Off)。可以按下該超連結直接進入該設定項目中。系統預設此功能為開啟-On。

防止 DoS 攻擊功能 DoS (Deny of Service)： 此為顯示 VPN 防火牆的阻斷來自 Internet 上的 DoS 攻擊功能選項是否開啟 (開啟-On/關閉-Off)。可以按下該超連結直接進入該設定項目中。系統預設此功能為開啟-On。

關閉對外的封包回應 Block WAN Request： 此為顯示 VPN 防火牆的阻斷來自 Internet 上的 ICMP-Ping 的回應功能選項是否開啟(開啟-On/關閉-Off)。可以按下該超連結直接進入該設定項目中。系統預設此功能為開

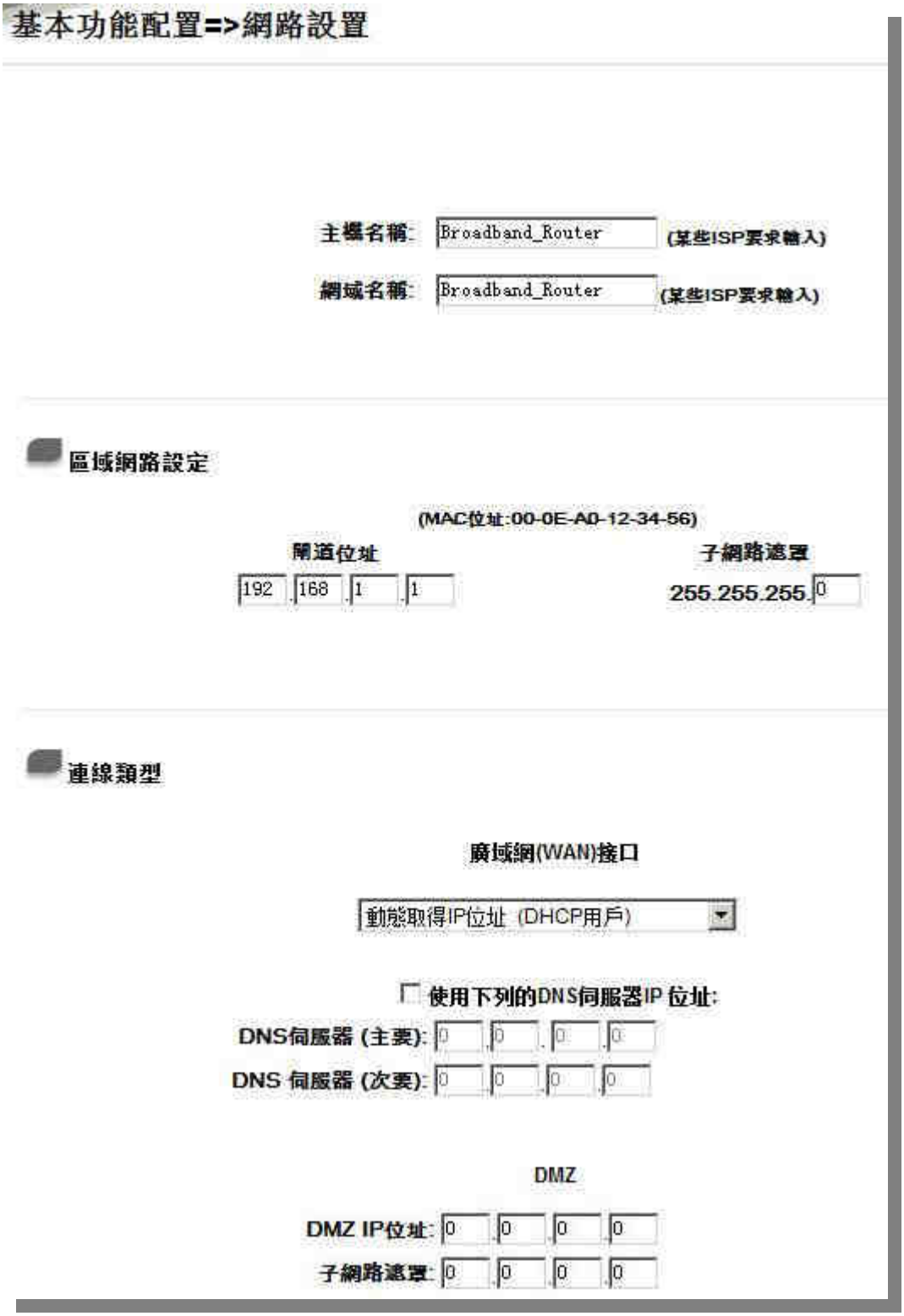
啟-On。

遠程配置管理功能 Remote Management： 此為顯示 VPN 防火牆的遠端管理功能選項是否啟動(開啟-On/關閉-Off)。可以按下該超連結直接進入該設定項目中。系統預設此功能為關閉-Off。

3.3 基本連網設定(General Setting)

基本連網設定(General Setting)提供 VPN 防火牆基本的網路連接設定內容. 對大多數的用戶來說，完成基本的設定已經足夠連接網際網路而不需做任何變更. 網際網路的聯接需要一些 ISP 所提供的進一步詳細資訊.其詳細細部設定，請參考以下各節說明：

3.3.1 基本設定(Configure)



主機名稱與網域名稱： 可輸入 VPN 防火牆的主機名稱以及網域名稱，於大多數的環境中不需做任何設定即可使用，除非特殊 ISP 需求！

區域網路設定：

此為設定 VPN 防火牆的 LAN 端內部網路的 IP 位置，系統預設為 192.168.1.1，子網路遮罩為 255.255.255.0.，現在可以支援到 Class C，您可以依照實際網路架構做更動！

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; 提供一組獨立的 DMZ 介面來設定連接有合法 IP 位置的伺服器.此 DMZ 介面為從 Internet 或從區域網路存取伺服器內容的溝通橋樑.

此 DMZ 的設定可分為 Subnet 及 Range (Future)兩種：

Subnet：

DMZ 與廣域網路 WAN 要在不同的子網路 Subnet 中，也就是若 ISP 端分配給你 16 個合法 IP 如：220.243.230.1-16 / Mask： 255.255.255.240 時，你必須將此 16 個 IP 再切兩組變成 220.243.230.1-8 / Mask：255.255.255.248 及另一組 220.243.230.9-16 / Mask： 255.255.255.248，然後 VPN 防火牆及 Gateway 是在同一組，再將另一組設定在 DMZ 中.

Range (Future)：

DMZ 與廣域網路 WAN 位在相同的子網路 Subnet.

IP Range for DMZ port： 輸入位在 DMZ 埠口的 IP 範圍.

設定完成請按下 ”確認” 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.

※ 於手冊中有標示「Future」功能表示現在可能沒有，但是未來有可能會加入

廣域網路 Internet 連線型態設定 (WAN Connection Type)：

自動取得 IP 位置：

此為 VPN 防火牆系統預設的連線方式，此連線方式為 DHCP Client 自動取得 IP 模式，多為應用於如 Cable Modem 或是 DHCP Client 連線型態等連接，若您的連線為其他不同的方式，請選取相關的設定並依照以下的介紹做設定.

在自動取得 IP 模式，你可以使用自訂 DNS 的 IP 位置(Use the Following DNS Server Address)，於此選項勾選並填入你要使用的 DNS IP 位置.

固定 IP 位置連線 (Static IP)：

若您的 ISP 有核發固定的 IP 位置給您(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

資訊分別依照以下介紹填入相關設定參數中

注意！

有一些 ISP 雖會提供固定一個 IP 位置給您，但是有可能是使用如 DHCP 自動取得 IP 或是 PPPoE 撥接取得一個固定 IP 模式，雖是每次都取得相同 IP 位置，但連線模式您依然要選擇相關之模式才可以！

IP 位址： 輸入您的 ISP 所核發的可使用固定 IP 位置的其中一個。

子網路遮罩： 輸入您的 ISP 所核發的可使用固定 IP 位置的子網路遮罩，如：
發放 8 個固定 IP 位置：255.255.255.248
發放 16 個固定 IP 位置：255.255.255.240

預設閘道： 輸入您的 ISP 所核發的可使用固定 IP 位置的預設通訊閘，若您是使用 ADSL 的話，一般說來都是 ATU-R 的 IP 位置.

DNS 伺服器： 輸入您的 ISP 所規定的名稱解析伺服器 IP 位置，最少頃填入一組，最多可填二組.

PPPoE 撥號連線：

此項為 ADSL 計時制使用(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， 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，你可以自行輸入所需要的自動離線等待時間。

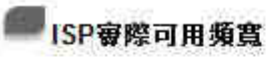
保持連線：自動重撥於斷線後___秒： 此功能能夠讓您的 PPPoE 撥接連線能夠斷線自動重撥，而且可以自行設定重新撥接的時間，預設值為 30 秒.

設定完成請按下 ”確認” 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.

3.3.2 頻寬管理(QoS)

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 的帶寬使用量，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享頻寬，才能有比較穩定、可靠的資料傳送服務。針，。依照以及網路管理人員應該針對公司、社區、或是網咖的實際需求，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。

頻寬設定



接口位置	上傳頻寬 (Kbit/sec)	下載頻寬 (Kbit/sec)
廣域網1	100000	100000

WAN 的頻寬數據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。例如說每個 IP 及 Service Port 可以保障使用的上傳或下載的 Mini.Rate 最小頻寬會依照此 WAN 的實際頻寬相加來換算實際可保障的大小。例如上傳頻寬若為 512Kbit/Sec，有 100 個 IP 在內部網路，要保證每人最小可使用的上傳頻寬，則就把 512Kbit/100=5Kbit，這樣每人可以保證的 Mini.Rate 就可以填 20kbit/Sec，下載同此換算方式。

連線數管制設定（Session Control）

連線數管控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。

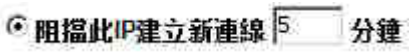
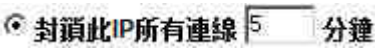
另外，若內網有電腦中了類似衝擊波的病毒而產生大量發起對外連線要求時，也可以達到抑制作用。

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 ___Session：

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。

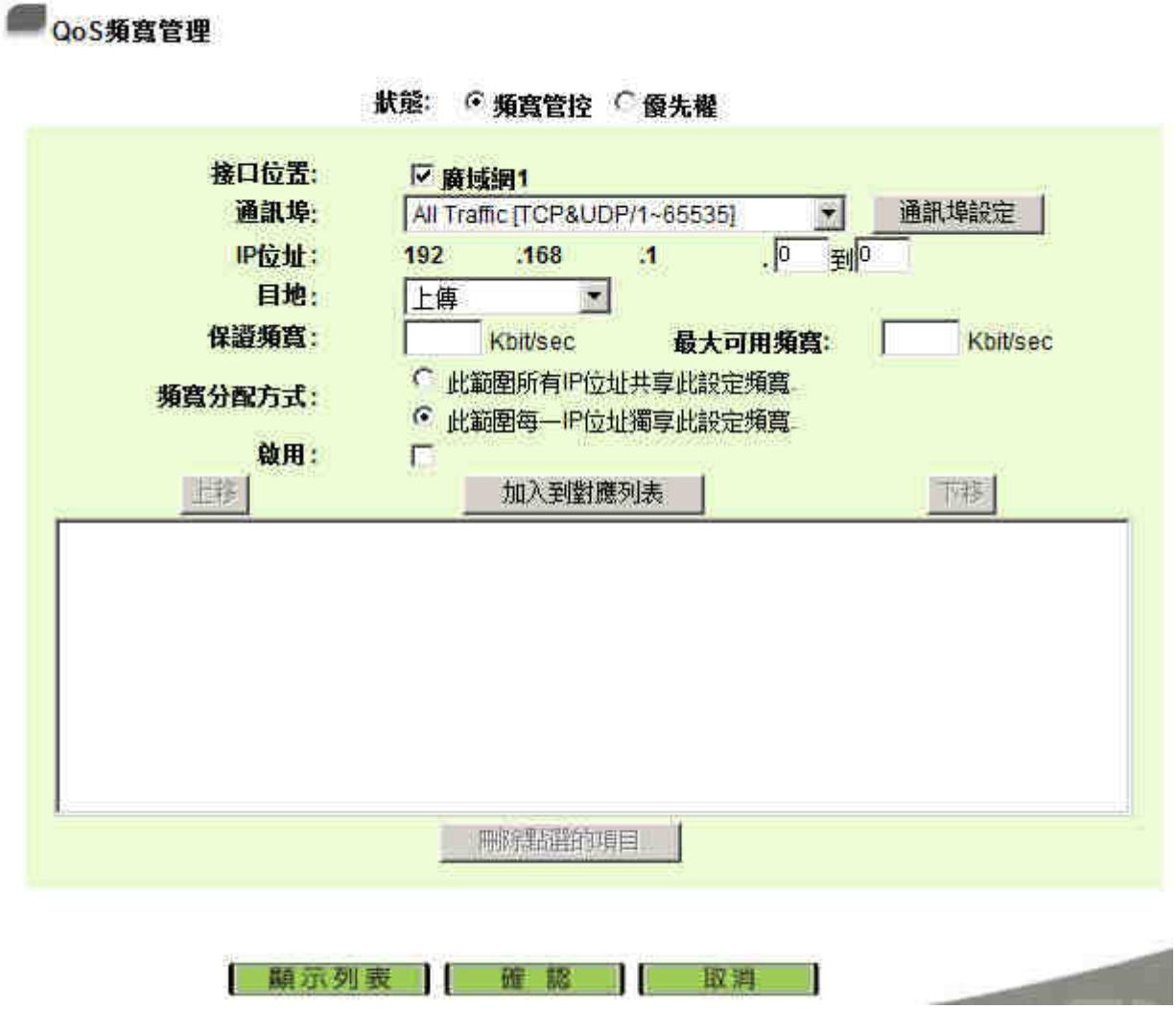
若有 IP 對外連線數到達限制值：	 此選項為當用戶端電腦使用的連線數到達您的設定數值時，此用戶在 5 分鐘之內將無法再增加新連線，就算舊連線已經結束，也必須等到設定時間過後才能再建立新的連線。  此選項為當用戶端電腦使用的連線數到達您的設定數值時，此用戶正在使用的所有連線都將被清除，且在 5 分鐘之內將無法建立任何連線(無法上網)，必須等到設定時間過後才能再建立新的連線。
不受限制的通訊埠或 IP 位址：	可以將公司，企業等重要服務或者用戶 IP 位址加入不受連線數限制
通訊埠：	選取不受連線限制的服務通訊埠
通訊埠設定：	添加或刪除相關服務通訊埠
來源 IP 位址：	添加內不受限制的 IP 位址群
啟用：	勾選啟動加入的規則
加入到對應列表：	將添加的規則增加到清單中
確認：	按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。
取消：	按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認 儲存動作之前才會有效。

QoS 設定

QoS 可以選擇兩種方式，無法同時使用，一為流量控制(Rate Control)，另一個為優先全控制(Priority Control)，設定人員可以依照自己內網需求做兩種模式靈活運用。

依使用量做管理 (頻寬管控)：

網管人員可依照您現有的頻寬大小做每一個 IP 或一組 Range 做使用量限制或保障頻寬。另外也可以針對服務端口(Service Port)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。



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何，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： 此為選擇你所要限制的使用者為何?若您只限制單一 IP，則直接將此 IP 填入，如：192.168.1.100 to 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 to 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內網的所有 User 則可在 IP 的欄位皆填入 0，也就是 192.168.1.0 to 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 B 的範圍。

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：若你有架設對外的 Server 網站在內部，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：**若你有架設網站在內網，則此選項為控制外部對此 Server 上傳資料時的頻寬控制，例如網咖很多都有架設 Game Server，若外部要來做此 Game Sever 做資料 Update 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 Game。
保證頻寬 與 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。
頻寬分配方式：	**此範圍所有 IP 位址共享此設定頻寬：** 若選擇此規則的話，其表示所有 IP 或此 Service Port 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 Service Port 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。
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 與 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，所以你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 Service Port 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。
刪除點選的項目：	刪除在服務列表裡所選擇的項目內容。
顯示列表：	可以顯示出您所有在 Rate Control 設定的規則，並可直接按下”Edit”做修改。
確認：	按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。
取消：	按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

依優先順序做管理（優先權）：

優先順序顧名思義就是可以將你選定想要的服務做先後順序的調配，也就是可以直接選擇 Service Port 將其優先順序做一分配。

會將頻寬做 60%(最高)，10%(最低)，的帶寬分配，也就是若您將 Port 80 選擇為高，那麼只要遇到 Port 80 的封包就會給予 60%的頻寬出去，若您將 FTP Port 21 設定為低，那當有人使用 Port 21 時，只會給它 10%的頻寬使用，其餘未做分配的 Service 就使用 30%頻寬。

接口位置： 勾選此條 Priority 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 Service Port 為何，要針對譬如 FTP 上傳或下載，則選擇 FTP Port21~21，可參考服務號碼預設列表。

目的：
上傳： 指針對此 Service Port 的上傳做優先權控制。
下載： 指針對此 Service Port 的下載做優先權控制。

優先權：
高： 此為保證 60%的頻寬給此 Service Port 使用。
低： 此為只給 10%的頻寬給此 Service Port 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。

刪除點選的項目： 刪除所選擇在服務列表裡的項目內容。

顯示列表： 可以顯示出您所有在 Priority 設定的規則，並可直接按下”Edit”做修改。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認 儲存動作之前才會有效。

3.3.3 密碼設定(Password)

當您每次登入至的設定畫面時，必須輸入密碼。的密碼出廠值為“admin” 。為了安全理由，我們強烈建議您務必在第一次登入並完成設定之後更改管理密碼！密碼請牢記，若是密碼忘記，將無法再登入至 VPN 防火牆的設定畫面，必須回復到出廠值 (Factory Default)。

使用者名稱： 預設為 admin 。

密碼： 填寫原本舊密碼。

輸入新密碼： 填寫所更改密碼。

再次輸入新密碼： 再填寫確認一次更改密碼。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認 儲存動作之前才會有效。

3.3.4 系統時間設定(Time)

可以設定時間，讓您在看的系統紀錄或是設置網路存取的時間設定時，可以了解事件發生的正確時間，以及作為關閉存取或是開放存取 Internet 資源的依據條件。您可以選擇與內建的外部時間伺服器(NTP Server)取得時間同步，或是自己設定正確時間參數。

設定自動與網路上的 NTP 伺服器同步時間：

請於 Time Zone 選項選擇您所在國家區域以及是否要啟動日光節約時間。如果您有專屬使用的時間同步伺服器(NTP Server)的話，您可以輸入此時間同步伺服器的 IP 位址。

手動輸入日期時間參數：

於此輸入正確的小時(Hours)， 分鐘(Minutes)， 秒(Seconds)， 月份(Month)， 日(Day) 與年(Year)。

設定完成請按下 ”確認” 按鈕儲存網路設定變更。若是不想進行變更，請在按下 ”確認” 儲存動作之前按下 ” 取消” 按鈕，將不做任何設定變更。

四、進階功能設定

本章介紹 VPN 防火牆進階功能的設定，包括開啟虛擬服務器的連接，路由設定，實體 IP 與虛擬 IP 對應，以及設置動態域名解析等功能。

4.1 DMZ Host

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 地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。

於使用 “DMZ Host” 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。

按下此按鈕 ”確認” 即會儲存剛才所變動的修改設定內容參數. 按下 ”取消” 即會清除剛才所變動的修改設定內容參數，但是必須在 ”確認” 儲存動作之前才會有效。

4.2 虛擬服務器設定(Forwarding)

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），這個功能可將虛擬服務器主機視為－虛擬的位置，利用 VPN 防火牆的外部合法 IP 位址，經過服務端口 Service Port 的轉換，（如 WWW 為 port 80），直接存取到內部虛擬 IP 的伺服器的服務。例如在設定畫面中，選項填入伺服器位置，如 192.168.1.2 且 port 是 80 的話，當 Internet 外部要進來存取這個網頁時只要鍵入：

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

此時，就會透過 VPN 防火牆的 Public IP 位置去轉換到 192.168.1.2 的虛擬主機上的 Port 80 讀取網頁了。

其他種類的伺服器設定，都如以上設定；只要將所用的 Server 的 Service Port 以及虛擬主機的 IP 位置填入即

可！

通訊埠： 在此選擇欲開啟的虛擬服務器的服務端口號。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！

IP 位址： 在此填上虛擬服務器所要相對應的內部虛擬 IP 位置，如 192.168.1.100。

啟用： 開啟此服務功能。

通訊埠設定： 若您所需要的服務端口沒有在列表裡面,可以利用此功能新增或刪除管理服務埠號列表。

加入到對應列表： 增加到開啟服務項目內容。

新增或刪除管理服務埠號

若您欲開啟的通訊埠項目沒有在表列中，您可以按下 ”通訊埠設定” 新增或刪除管理服務埠號列表功能達成，如以下所述：

服務名稱： 在此自訂欲開啟的服務埠號名稱加入列表中，如 BT 等。

通訊協議： 在此選擇欲開啟的服務埠號的封包格式為 TCP 或 UDP。

通訊埠範圍： 將你所需新增加的服務端口範圍填入。

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： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

離開： 離開此功能設定畫面。

特殊應用程式設置 (Port Triggering)：

有一些特殊應用軟體其進出 Internet 的服務端口號(Port Number)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服務端口號填入相關設定中，如以下畫面所示：

特殊應用程式名稱： 您可以自訂此特殊應用軟體名稱，方便管理使用！

實際對外的通訊埠範圍： 輸入由 VPN 防火牆出 Internet 的使用埠口(Port Number)編號.(如 9000~10000)。

內部映射的通訊埠範圍： 輸入由 Internet 進入的使用埠口(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。

刪除點選的項目： 刪除所選擇的開啟服務項目之一筆內容。

顯示列表： 按下此按鈕即會顯示 Table 上的所有設定項目內容參數。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

4.3 UPnP- Universal Plug and Play

UPnP (Universal Plug and Play) 是微軟 Microsoft 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 WindowsXP)而且您的電腦 UpnP 功能有開啟，您可以將 VPN 防火牆的 UPnP 功能啟動，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，如您要在內網設置虛擬服務器，您可以在前章節介紹的 Forwarding 功能設置，或是在此 UPnP Forwarding 中設置。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！

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： 新增或刪除管理服務埠號列表。

加入到對應列表： 增加到開啟服務項目內容。

刪除點選的項目： 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。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

4.4 路由通訊協議(Routing)

如果在您的網路中有多個路由器與 IP 節點子網路，就必需設定 VPN 防火牆的靜態路由功能(Static

Routing)，這些功能是讓整個不同的網路節點能自動找尋所需路徑，且能讓不同網路節點能相互存取;使用圖中的功能按鈕 “Show Routing Table “ 能知道最新的路徑表。

目的 IP 位址 / 子網路遮罩：	可填入欲繞徑的遠端網路 IP 節點與子網路節點位置， 如另一個子網路節點為 192.168.2.0/255.255.255.0
預設閘道：	此網路節點欲繞送的預設閘道位置。 如 192.168.2.1
中繼路由節點：	此節點的路由器層數，如是在 VPN 防火牆下的二個路由器之一，此應填為 2，預設為 1 (最大為 15)
接口位置：	此網路節點的連線位置，是位於 WAN 端亦或是 LAN 端
加入到對應列表	增加 / 移除一個路由

/ 刪除點選的項目：

顯示列表： 顯示目前最新的路徑表

4.5 一對一 NAT 對應 (One-to-One NAT)

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 地址。VPN 防火牆提供你可將除了本身 WAN Port 以及光纖盒或 ATU-R(Gateway) 各使用一個合法 IP 位址後，所剩的合法 IP 地址可以直接對應到內部的電腦使用，也就是這些電腦在內網雖為虛擬 IP，但當做了 One to One 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 Server”時，由於需要兩個或兩個以上的合法 IP 地址，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 地址，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 位址不行被涵蓋在 One to One NAT 的 IP 範圍設定中。

一對一 NAT 對應設定： 選擇是否開啟此一對一 NAT 功能 “Enable”開啟 Disable 關閉。

內部起使 IP 位址： 虛擬 IP 地址起始 IP 位址。

外部起使 IP 位址： 外部合法 IP 地址起始 IP。

對應範圍的 IP 數量： 填入你同時要有多少個外部合法 IP 地址需要對應。

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。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認 儲存動作之前才會有效。

注意！

一對一的 NAT 模式 (One-to-One NAT) 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 Public IP 的服務伺服器或電腦將會曝露到 Internet 上。若要阻絕 Internet 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 Access Rule 中設定適當的拒絕存取規則條件。

4.6 DDNS-動態網域名稱解析

此 VPN 防火牆的 “DDNS” 功能可以支援 QnoDDNS、Dyndns.org 與 3322.org 等家的動態域名解析功能，其目的是為了讓使用動態 IP 地址(也就是無法有固定 IP 的環境)來架設虛擬服務器、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 地址都會隨 ISP 端要求而改變，當此時使用者申請了 DDNS 後，如”qno.3322.org”，將其設定在 DDNS 設定中，則在遠端只要去 Ping qno.3322.org 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，Internet 使用者只要在網址打上 qno.3322.org 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.dyndns.org 或是 www.3322.org 提出申請，此二個服務是完全免費的！！

另外，為了解決 DDNS 服務器可能會發生不穩定的情況，現在 VPN 防火牆每個 WAN 都可同時對此二家 DDNS 做動態 IP Upgrade。

選擇 DDNS 服務提供者: 可以選擇 QnoDDNS、DyDns、3322 等(可以同時使用)。

使用者名稱： 向 DDNS 服務提供者所申請的使用者名稱。

密碼： 向 DDNS 服務提供者所申請的密碼。

動態網域名稱： 向 DDNS 所註冊的網址，如 abc.dyndns.org or abc.dtdns.net。

內部 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 位置後會自動顯示於此。
狀態：	顯示目前 VPN 防火牆對 DDNS 的更新狀態。
確認：	按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。
取消：	按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

4.7 廣域網 MAC 位址設定-變換實體 MAC 地址

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

使用者自訂廣域網接口 MAC 位址設定：	使用者可以自行輸入提供給 ISP 的網卡位址，目前設備出廠預設的 MAC 位置為 WAN 端的 MAC 位址。
設定與此 PC 的 MAC 地址相同：	目前這台 PC 的 MAC 位址。
確認：	按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。
取消：	按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認 儲存動作之前才會有效。

4.8 DHCP 功能

VPN 防火牆有一組 Class C 的 DHCP 伺服器，預設值是啟動，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 位置，當電腦開機後，就可從 VPN 防火牆自動取得 IP 位址，管理方便。

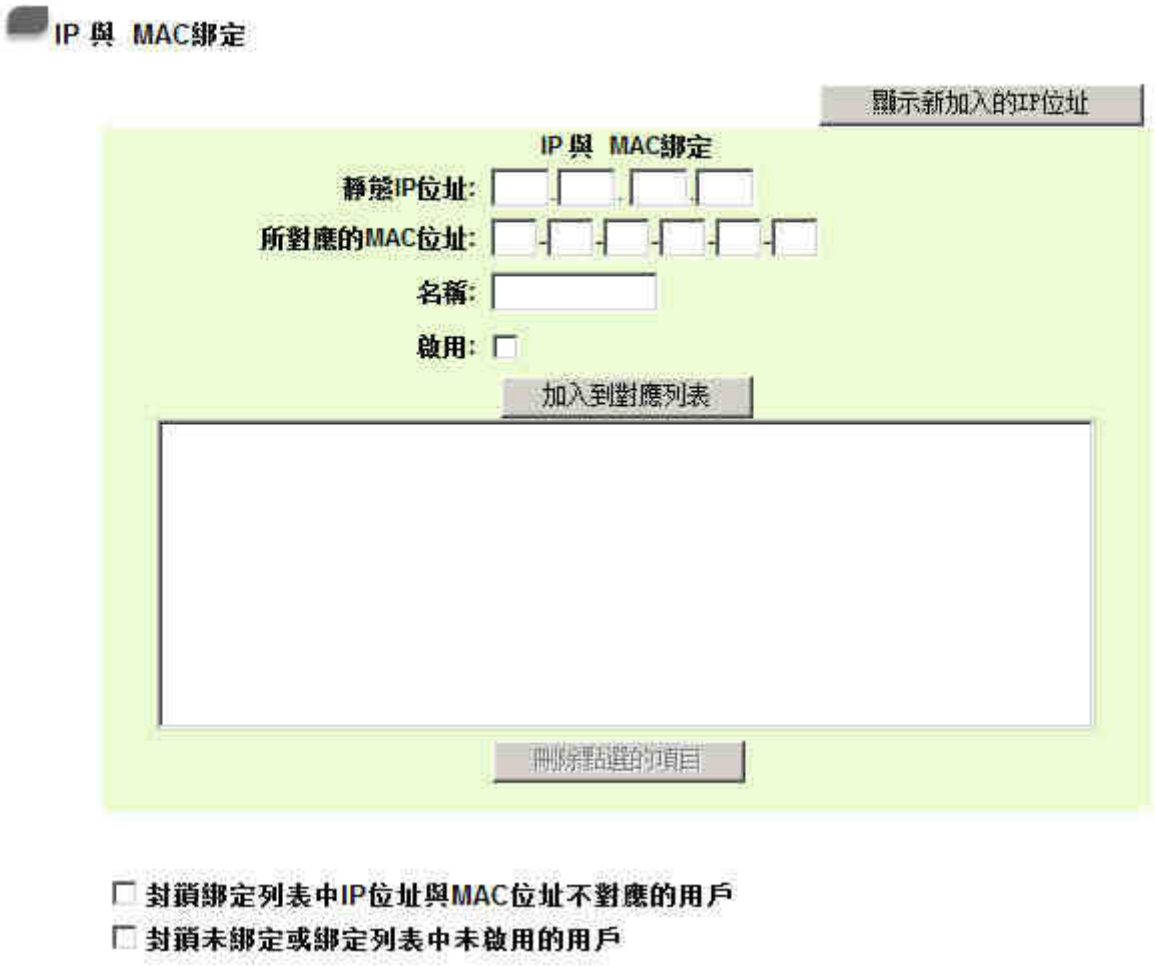
4.8.1 動態 IP 租約到期時間

租約到期時間： 此設定為發給 PC 端 IP 地址的租約時間，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 防火牆再申請一次。您可以依照實際需求來設定。

起使 IP 位址： 系統預設為從 192.168.1.100 的 IP 地址開始發放。您可以依照實際需求來設定。

結束 IP 位址： 系統預設為 192.168.1.149 IP 地址為最後發放 IP，也就是說出廠設定值可供 50 台電腦自動取得 IP 位址。您可以依照實際需求來設定。

4.8.2 IP 與 MAC 位址綁定



靜態 IP 位址：

此欄位有兩種填入方式：

1. 若您只要限制 MAC Address 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配置到同一個 IP，則將你所要求配置給此台電腦的 IP 位址輸入。這樣所要連結伺服器或 PC 端每次重啓都會要到固定的同一個虛擬 IP

所對應的 MAC 位址：

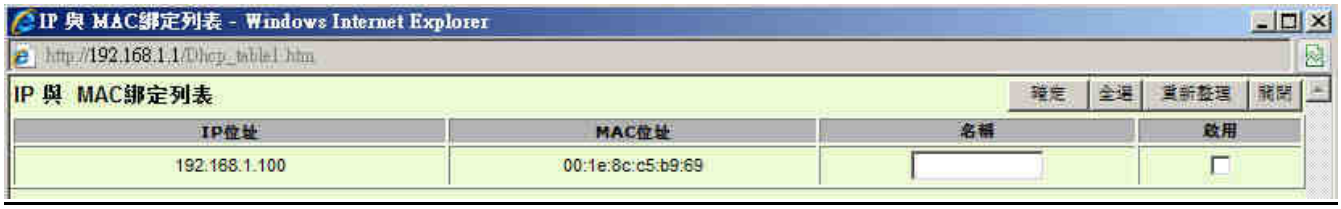
輸入要連結的伺服器或 PC 端固定實體 MAC(網路卡上的位址)

名稱：

填入您所連結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：	啓用此組設定
加入到對應列表：	加入或修正此設定到清單中
刪除點選的項目：	移除清單中所選取的連結
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 自行變更電腦的 IP 或不是清單設定的 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，只要不在清單中的 MAC Address 都無法上網

顯示新加入的 IP 與 MAC 位址



選擇需要連結的 IP / MAC，命名好用戶需要設定名稱，並做啟用

顯示列表 (顯示目前已有綁定的 IP & MAC 資訊)

可以按下 "編輯" 進入編輯該列綁定設定

4.8.3 DNS 與 WINS 服務器設定

網域名稱解析服務伺服器 (DNS Server)：

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 Server，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，也會一並取得指定的 DNS Server 位址。

.

DNS 伺服器 (主要) 1： 輸入主要 DNS 網域伺服器的 IP 位置。

DNS 伺服器 (次要) 2： 輸入次要 DNS 網域伺服器的 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 位置。

WIN 伺服器： 輸入 WINS 網域伺服器的 IP 位置。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

4.8.4 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數據。

DHCP 伺服器 IP 位址： 目前 DHCP 伺服器的 IP 地址。

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 數量： 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 位置。

MAC 位址： 目前此台電腦的 MAC 網路實體位置。

目前租約剩餘時間： DHCP 目前核發 IP 位置的租約時間。

刪除： 刪除此筆核發 IP 紀錄。

五、系統工具設定

此章節介紹用來管理 VPN 防火牆以及測試網路連線的工具。

5.1 自我診斷工能

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 Lookup 以及 Ping 二種。

網域名稱查詢測試 (DNS Name Lookup)

請於此測試畫面輸入您想查詢的網域主機位置名稱，如 www.abc.com 然後按下 Go 的按鈕開始測試。測試結果會顯示於此畫面上。

Ping-封包傳送/接收測試

此項目為主要提供管理者了解對外連線的實際狀況，可以藉由此功能了解網路上的電腦是否存在！

請於此測試畫面輸入您想測試的主機位置 IP，如 192.168.5.20 按下 Go 的按鈕開始測試，測試結果會顯示於此畫面上。

5.2 重新啟動

您可以於此工具中選擇 VPN 防火牆系統重新開機功能，請按下 Restart Router 按鈕即可重新開機啟動。

5.3 回復原出廠預設值

若是選擇“Return Factory Default Setting”， VPN 防火牆會將所有的設定清除，並重新開機。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 Setting Backup 說明)。

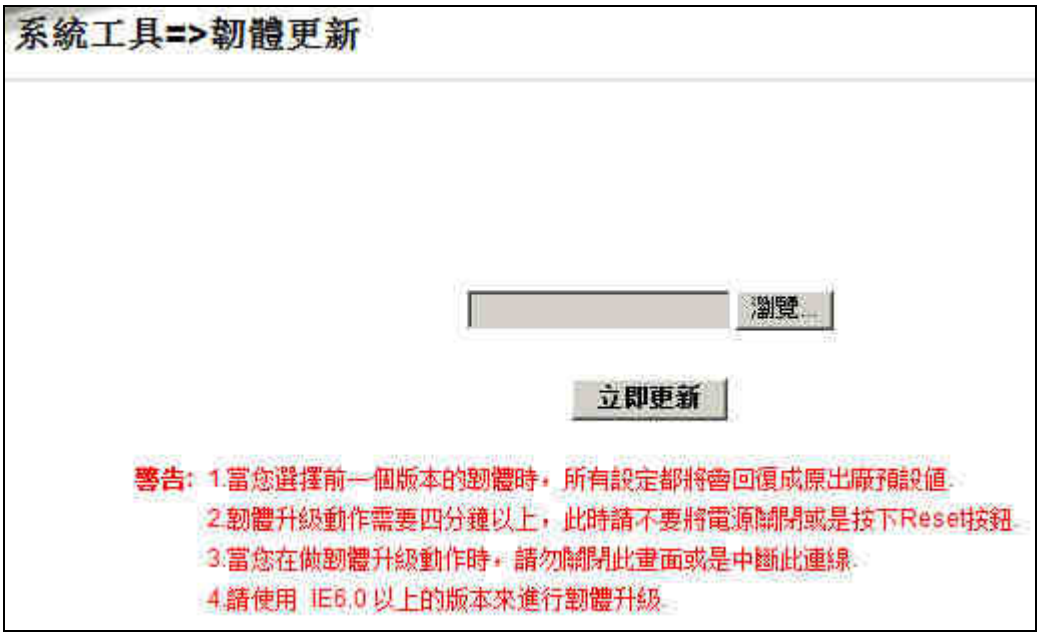
5.4 系統韌體升級

此功能可以讓 VPN 防火牆 在 Web 設定畫面中直接做韌體升級。請您於升級前先確認韌體版本資訊。按下”瀏覽”按鈕，選擇韌體(Firmware)存放資料夾，並於選擇欲升級的韌體後，按下「立即更新」做升級。

注意！

執行韌體(Firmware)升級前，請詳細閱讀畫面中的注意事項。

正在做韌體(Firmware)升級當中時，請勿離開此升級畫面，否則會造成 VPN 防火牆升級失敗。



5.5 系統配置參數備份儲存與匯出

配置參數回復：

此功能為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”至備份參數檔案-"config.exp"存放資料夾，選擇該檔案後，按下匯入按鈕做設定檔案匯入。

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！ 按下匯出按鈕，選擇至備份參數檔案-"config.exp"存放資料夾位置，按下儲存即可。

六、防火牆功能設定

本章節介紹防火牆設定的選項，以及網路存取控制的設定。

6.1 防火牆基本設定

從防火牆功能的一般設定選項當中， 您可以控制開啟(Enable)或是關閉(Disable)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： 此為選擇開啟或關閉防火牆功能。

SPI 封包偵測： 此為封包主動偵測檢驗技術(Stateful Packet Inspection)，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。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。

DoS 防禦功能： 此為保護 DoS 攻擊，如 SYN Flooding， Smurf， LAND， Ping of Death，IP Spoofing 等。

關閉廣域網回應功能： 若是選擇 Enable 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，所以若是你從外部去 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，若您要透過遠端 Internet 直接連線進入 VPN 防火牆的設定畫面，必需將此功能開啟，並於遠端於瀏覽器網址填入 VPN 防火牆的外部合法 IP 位置(WAN IP)，並加上預設可修改的控制埠口(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 Client 端接收此類封包訊息格式。預設值為關閉這個功能。

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中斷連線或部份電腦無法上網。開啓此功能可以避免此種病毒攻擊。

每秒主動發送___筆 ARP 封包.： 網路內發廣播封次 / 每秒防止 ARP 攻擊

MTU： MTU 為 Maximum Transmission Unit 的縮寫， 一般預設的 default 為 1，500。 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 Size：1492)。不過許多的 Server 與 ADSL PPPoE 用戶的 MTU Size 相關，一般使用預設 Auto 即可，不需做任何調整。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認 儲存動作之前才會有效。

特殊網頁存取限制

路由器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，則路由器就不會去阻擋可信任網域的網頁中所帶有的 Java/ActiveX/Cookies 等。

阻擋特定服務

路由器提供一指封 QQ 服務功能，可以通過設定將 QQ 擋住，以方便用戶的管理設定。

如下圖可以看出 QQ 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 QQ 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。

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。

6.2 網路存取規則設定

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權限。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 (Inside-LAN to Outside-WAN) 還是從外部到內部(Outside-WAN to Inside-LAN)，或是設定以使用者的 IP address(IP 位置)、Destination IP address(目地端 IP 位置)、IP protocol type(IP 通訊協定型態)等條件來做管制，管理者可以依照實際的需求調性設置。

管理者定訂的網路存取規則條例，可以選擇關閉(deny)或是允許(allow)來調整使用者對網際網路 Internet 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：

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

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，不受其他自訂規則所影響：

* 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 位置使用)。
* 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)。

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(Priority) 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 Priority 1-2-3…..依序做規則判斷，所以 Priority 是讓您在做 Access Rule 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。

垃圾桶圖示： 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： 可以回復到出廠原有預設存取規則項目並刪除所有的自訂規則內容。

6.2.1 加入新規則

管制動作： 此為設定此規則的管制條例動作：

允許： 允許符合此管制條例行為的封包通過。

禁止： 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你所要允許或不允許的 Service Port 服務項目內容。

日誌： 選擇該存取規則觸發動作時，是否要記錄到日誌內

通訊埠設定： 若是您想要管制的通訊埠或服務內容沒有存在於預設列表內的話，您可以按下右方的通訊埠設定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口，按下加入到對應列表按鈕，即可新增一個管制服務項目內容。

接口位置： 選擇你所要允許或不允許的來源封包介面(例如是從 LAN， WAN1， WAN2 還是 Any)，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 Any， Single or Range)，若是選擇 Single 或是 Range 的話，請輸入此單一或是一區段範圍的 IP 位址。

目的地 IP 位址： 選擇目的端封包的 IP 範圍(如 Any， Single or Range)，若是選擇 Single 或是 Range 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： 你可以將此條規則依照你所需要的執行時間來做控管。例如你可以設定此規則

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。

加入到對應列表時間： 可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。

從： ___到___： 此管制規則有時間限制，設定方式為 24 小時制，如 08：00 to 18：00 (早上 8 點到下午 6 點)。

天： 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。

確認： 按下此按鈕”確認”即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕”取消”即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

七、虛擬私有網路功能設定 (VPN Configuration)

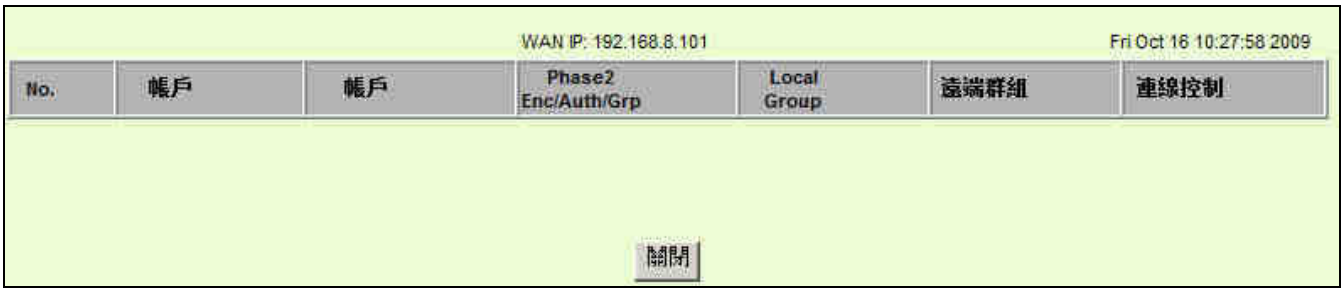
本章節介紹 IPSec VPN 虛擬私有網路的設定方式，附錄一將介紹三種 VPN 環境的案例及其設定方式，提供作為範例參考。

7.1 VPN 狀態顯示 (Summary)

此 VPN 狀態可以顯示目前有關 VPN 方面的即時狀態包含通道-Tunnel ，設定參數以及 GroupVPN-VPN 群組狀態等資訊.

摘要訊息：

詳細訊息： 按下此按鈕可以顯示如以下畫面的目前所有 VPN 組態，讓管理者清楚的管理所有 VPN 連接資訊.



VPN 隧道狀態： VPN 通道目前狀態顯示

新增一條隧道： 按下此按鈕可以新增一條新的 VPN 通道設定。VPN 防火牆 提供閘道對閘道隧道 或是 客戶端對閘道隧道兩種 VPN 設定模式。

閘道對閘道設定：

以下圖例為運作於閘道對閘道模式的 VPN 網路連接環境。VPN 通道連接為 2 台 VPN 防火牆分別透過網際網路 Internet 所組成。當您按下新增"新增一條隧道" 的話， 將會直接導引到閘道對閘道的設定頁面上。

客戶端對閘道：

以下圖例為運作於 Client to Gateway 模式的 VPN 網路連接環境。VPN 通道連接為一台 PC 以及一台 VPNVPN 防火牆分別透過網際網路 Internet 所組成。當您按下新增“Add Now” 的話， 將會直接導引到 Client to Gateway 的設定頁面上。

以下就針對 VPN 隧道狀態的顯示訊息做完整解說：

VPN隧道狀態

跳到___頁，每頁顯示___筆： 您可以從下拉式選單直接選擇你要觀看檢視的頁數資料，也可以自行定義每頁所顯示的資料筆數 (每頁 3 筆或每頁 5 筆)。

No： 顯示您設定 VPN 防火牆之 VPN 功能時所選擇的 Tunnel 通道編號。

狀態： 於此狀態顯示現在連線狀態為 “連線中”，或是”等待連線”等資訊。若是管理者選擇手動設定 IPSec 通道，則此狀態會顯示手動。

帳戶： 目前連線 VPN 通道連接名稱，如 XXX Office，建議您若是有一個以上的通道設定的話，務必將每一個通道名稱都設為不同，以免混淆。

Note： 若是您需要連接其他 VPN 設備(非 VPN 防火牆)，有些會規定此通道名稱要與主控端為相同名稱並做驗證，此通道才會順利連線開啟!

Phase2 Encrypt/Auth/Group： 於此顯示此條 VPN 的加密(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。

Local Group： 此為顯示 VPN 防火牆本地區域網內部做 VPN 連線的群組範圍。

遠端群組： 此為顯示遠端的 VPN 設備的區域網的連線群組範圍。

遠端閘道： 此為遠端 VPN 設備的 IP 位置，也就是遠端的 VPN 防火牆之對外的合法 IP 位置或是 Domain Name 等。

遠端閘道連線控制： 可以按下連接按鈕-Connect 去驗證此通道的狀態，測試結果將會更新於此狀態上。

配置： 設定項目包含編輯以及刪除圖示
若您按下編輯按鈕，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， 所有此通道的設定將會被刪除。

7.2 閘道器對閘道器的 VPN 設定(Gateway to Gateway VPN)

此節介紹閘道器對閘道器的 VPN 設定方式。

7.2.1 通道設定

隧道編號.： 當您設定 VPN 防火牆內建之 VPN 功能時，此設定的 Tunnel 通道編號會自動加 1 表示現在的通道號碼，VPN 防火牆可支援最高 5 條 VPN 通道。

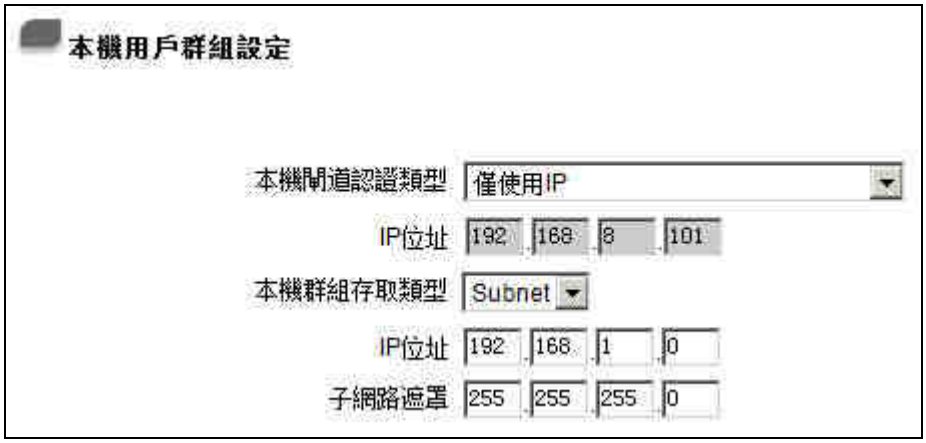
隧道名稱： 設定此通道連接名稱，如 XXX Office，建議您若是有一個以上的通道設定的話，務必將每一個通道名稱都設為不同，以免混。

Note： 若是您需要以 VPN 防火牆連接其他 VPN 設備(非 VPN 防火牆)，有些會規定此通道名稱要與主控端為相同名稱並做驗證，此通道才會順利連線開啟!

啟用： 勾選 Enable 將此 VPN 通道開啟。此項目預設為啟動 Eanble，當設定完成後，可以選擇是否啟動通道設定。

本機用戶群組設定 (Local Group Setup)：

您在 VPN 防火牆上的近端閘道安全群組設定(Local Security Gateway Type)型態必須與 VPN 通道遠端的”遠端閘道安全群組設定(Remote Security Gateway Type)”型態設定相同，才能成功的連接。



本機閘道認證類型： 此為本地端的 VPN 通道結止點，有五種操作模式項目選擇，分別為：

僅使用 IP-只使用廣域網 IP 作為認證

IP + Domain Name(FQDN) 認證，IP+網域名稱

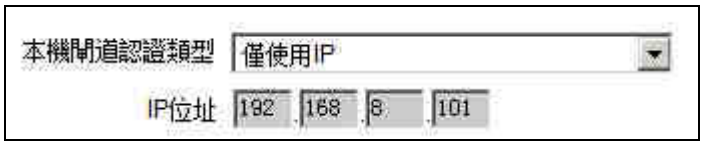
IP + E-mail .(USER FQDN) 認證，IP+電子郵件

Dynamic IP + Domain Name(FQDN) 認證，-動態 IP 位址+網域名稱

Dynamic IP + E-mail Addr.(USER FQDN) 認證. 動態 IP 位址+電子郵件名稱

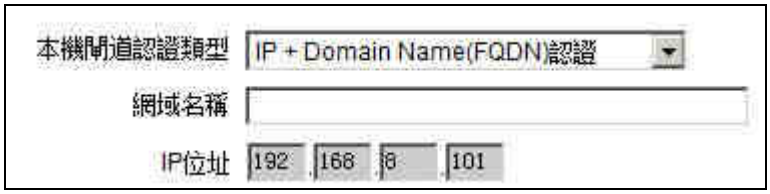
(1) 僅使用 IP：

若您選擇 IP Only 型態的話， VPN 防火牆的 WAN IP 位址，將會自動填入此項目空格內，您不需要再進行額外設定。



(2) IP + Domain Name(FQDN) 認證：

若您選擇 IP+網域名稱型態的話，請輸入您所驗證的網域名稱，VPN 防火牆的 WAN IP 位址將會自動填入 IP Address 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 安全閘道器設定型態相同才可以正確連接。

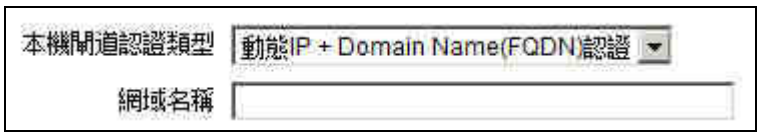


(3) IP + E-mail Addr.(USER FQDN) 認證：

若您選擇 IP 位址加上電子郵件型態的話， 請填入您所驗證的電子郵件位址， VPN 防火牆的 WAN IP 位址將會自動填入 IP Address 項目空格內，您不需要在進行額外設定。

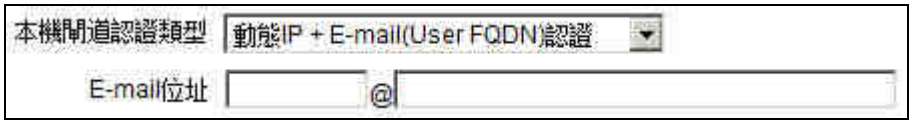
(4) 動態 IP + Domain Name(FQDN) 認證：

若您 VPN 防火牆是使用動態 IP 連接時， 您可以選擇此型態連接 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 通道連線; 若您選擇此型態連接 VPN，請輸入網域名稱即可。



(5) 動態 IP + E-mail Addr.(USER FQDN) 認證：

若是您使用動態 IP 位置連接 VPN 防火牆時， 您可以選擇此型態連接 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 通道連線; 若您選擇此型態連接 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可以使用 VPN 連線的安全群組。請您選擇適當的設置：

(1) IP Address：

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

注意:若是您填入 IP 位址的最後一位數為 0,表示整個網段都可以使用此 VPN 連線。例如圖中所示的設定為： 當此 VPN 通道連線後，於 192.168.1.0~255 的此網段的 IP 位置範圍的電腦可以連線。

(2)Subnet：

此項目為允許此 VPN 通道連線後，每一台於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 通道連線後，只有 192.168.1.0，子網路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 連線。

遠端用戶群組設定 (Remote Group Setup)：

您在 VPN 防火牆上的遠端閘道安全群組設定(Remote Security Gateway Type)型態必須與 VPN 通道遠端的”近端閘道安全群組設定(Local Security Gateway Type)”型態設定相同，才能成功的連接。

遠端用戶群組設定： 遠端安全群組設定，有五種操作模式項目選擇，分別為：

僅使用 IP -只使用 IP 作為認證

IP + Domain Name(FQDN) 認證，IP+網域名稱

IP + E-mail Addr.(USER FQDN) 認證，IP+電子郵件

Dynamic IP + Domain Name(FQDN) 認證，動態 IP 位址+網域名稱

Dynamic IP + E-mail Addr.(USER FQDN) 認證. 動態 IP 位址+電子郵件名稱

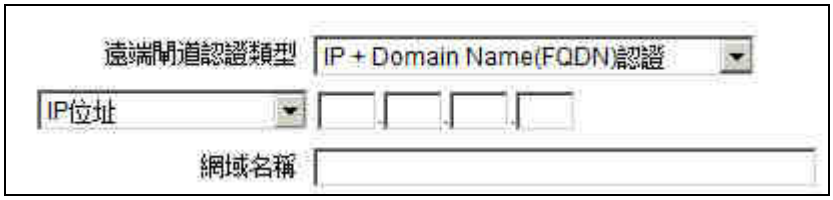
(1) 僅使用 IP：

若您選擇 IP Only 型態的話， 請填入對方 VPN 閘道器的 WAN IP 地址.

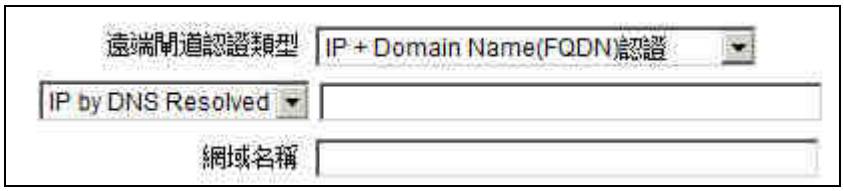
若是遠端 VPN 閘道器的 IP address 為動態 IP，則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address。此網域名稱必須存在 Internet 上可以查詢的到，並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address。

(2) IP + Domain Name(FQDN) 認證：

若您選擇 IP+網域名稱型態的話，請輸入遠端 VPN 閘道器的 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 位置以及網域名稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接。



若是遠端 VPN 閘道器的 IP address 為動態 IP，則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address。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 address。



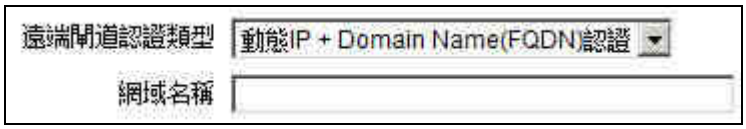
(3) IP + E-mail Addr.(USER FQDN) 認證：

若您選擇 IP 位置加上電子郵件型態的話， 請輸入遠端 VPN 閘道器的 IP 位址以及您所驗證的電子郵件位址。

若是遠端 VPN 閘道器的 IP address 為動態 IP，則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP address。 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 address。

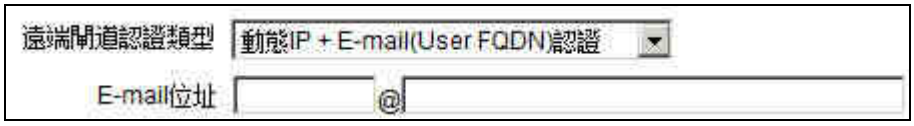
(4) Dynamic IP + Domain Name(FQDN) 認證：

若是遠端閘道器是使用動態 IP 位址做 VPN 連接 VPN 防火牆時，您可以選擇動態 IP 位置加上網域名稱的結合認證方式。



(5) Dynamic IP + E-mail Addr.(USER FQDN) 認證：

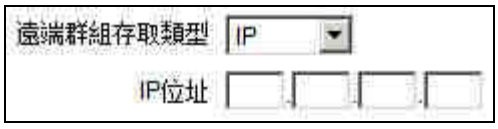
若是遠端閘道器是使用動態 IP 位址做 VPN 連接 VPN 防火牆時， 您可以選擇此型態連接認證方式。當遠端的 VPN 閘道要求與 VPN 防火牆作為 VPN 連線時，VPN 防火牆將會開始驗證並回應此 VPN 通道連線，請輸入電子郵件認證到 E-Mail 位置空格欄位中。



遠端群組存取類型： 此為設定遠端局域網可以使用 VPN 連線的安全群組，以下有幾個關於遠端區域設定的項目，請您選擇適當設置：

(1) IP Address：

此項目為允許此 VPN 通道連線後，只有輸入此 IP 位置的遠端電腦可以連線。



注意：若是您填入 IP 位址的最後一位數為 0，表示整個網段都可以使用此 VPN 連線。例如輸入 192.168.2.0 則表示當此 VPN 通道連線後，於 192.168.2.0~255 的此網段的 IP 位置範圍的電腦可以連線。

(2)Subnet：

此項目為允許此 VPN 通道連線後，每一台於此網段的遠端電腦都可以連線..

例如輸入 192.168.2.0 且 Subnet Mask 為 255.255.255.192 則表示當此 VPN 通道連線後，只有 192.168.2.0，子網路遮罩為 255.255.255.192 的此網段電腦可以使用 VPN 連線。

7.2.2 IPSec 加密機制設定

VPN 通道可以用來安全的傳輸資料，其原理是在傳送資料之前要將資料以密鑰(key)加密，在以封包經過 Internet 傳送，收到封包後再解密還原資料。VPN 通道的兩端加密機制必須要相同才可以將此通道建立起來，資料的收送才會正確。以下介紹密鑰(Key)以及加密機制的設定。

金鑰模式：

此選項為當您設定此 VPN 通道是使用何種加密模式以及驗證模式，然後，必須設定一組交換密碼。請注意此參數必須與遠端的交換密碼參數相同。VPN 防火牆提供了 IKE 自動加密模式- IKE with Preshared Key。

自動加密模式 使用 IKE 協議：

透過 IKE 產生共用的金鑰來加密資料與驗證遠端的使用者。若將完全順向密鑰 PFS(Perfect Forward Secrecy)啟動後，則會在第二階段(phase 2)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 啟動後，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，可以提高安全性。注意，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 蜜要交換群組方式： Group1 或是 Group2/Group5.

階段 1 / 階段 2 加密演算法： 此項目為設定此 VPN 通道使用何種加密模式。您可以選擇 DES： 64-位元加密模式，或是 3DES： 128-位元加密模式。請注意此參數設置必須與遠端的 VPN 設備設定的加密參數相同。

階段 1 / 階段 2 認證演算法： 此驗證選項設定為設定此 VPN 通道使用何種驗證模式，並請注意設置此參數必須與遠端的驗證模式參數相同：
“MD5”/“SHA”.

階段 1 SA 有效時間： 此為設定第一階段所使用的密鑰的有效時間，系統預設值為 28800 秒(8 小時)。於此有效時間內，此 VPN 連線會使用同一個密鑰。於有效時間到期後，系統會自動的生成及更換其他的交換密碼以確保安全。

階段 2 SA 有效時間： 此為設定第二階段所使用的密鑰的有效時間，系統預設值為 3600 秒(1 小時)。於此有效時間內，此 VPN 連線會使用同一個密鑰。於有效時間到期後，系統會自動的生成及更換其他的交換密碼以確保安全。

完全順向密鑰 (PFS)： 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。

共用密鑰： 於此項目中，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，您可以輸入數字或是文字的交換密碼，系統將會自動的將您輸入的數字或是文字的交換密碼自動轉成 VPN 通道連接時的交換密鑰與驗證機

制。此欄位可以填入數字或是文字，最高可輸入 23 個數字文字組合。注意，在此輸入的數字文字組合，必須與遠端 VPN 設備的“Pre-shared Key”欄位中的相同。

7.2.3 VPN 進階設定(Advanced)

只有使用自動交換密鑰模式(IKE Preshareed Key Only)才有此選項。

Aggressive Mode： 在 VPN 防火牆 的 VPN 功能預設為主要模式(Main Mode)，而且與大多數的其他 VPN 設備使用連接方式為相同。若是與 VPN 防火牆做 VPN 連接的遠端的 VPN 設備使用 Aggressive Mode， 您可以將此選項勾選。

保持連線： 若選擇此項目勾選，則連接中的 VPN 通道會持續保持此條 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 位置的遠端使用。

允許 NetBIOS 廣播封包通過： 若選擇此項目勾選，則連接中的 VPN 通道會讓 NetBIOS 廣播封包通過，有助於微軟的系統網路芳鄰等連接容易，但是相對的佔用此 VPN 通道的流量就會加大。

允許穿越 NAT： 使 VPN 相關封包可以穿透前方的 NAT 機制

自動偵測：

若偵測到前方有 NAT 機制，則用 UDP 4500 Port 傳送資料，如果沒有 NAT 機制，則採用 ESP 封包傳送資料。

強制使用 UDP 4500 Port 連線：

一律使用 UDP 4500 Port 傳送資料，原因是有些 ISP 線路可能不支援 ESP，或是前方的 NAT 機制不支援 ESP 封包。

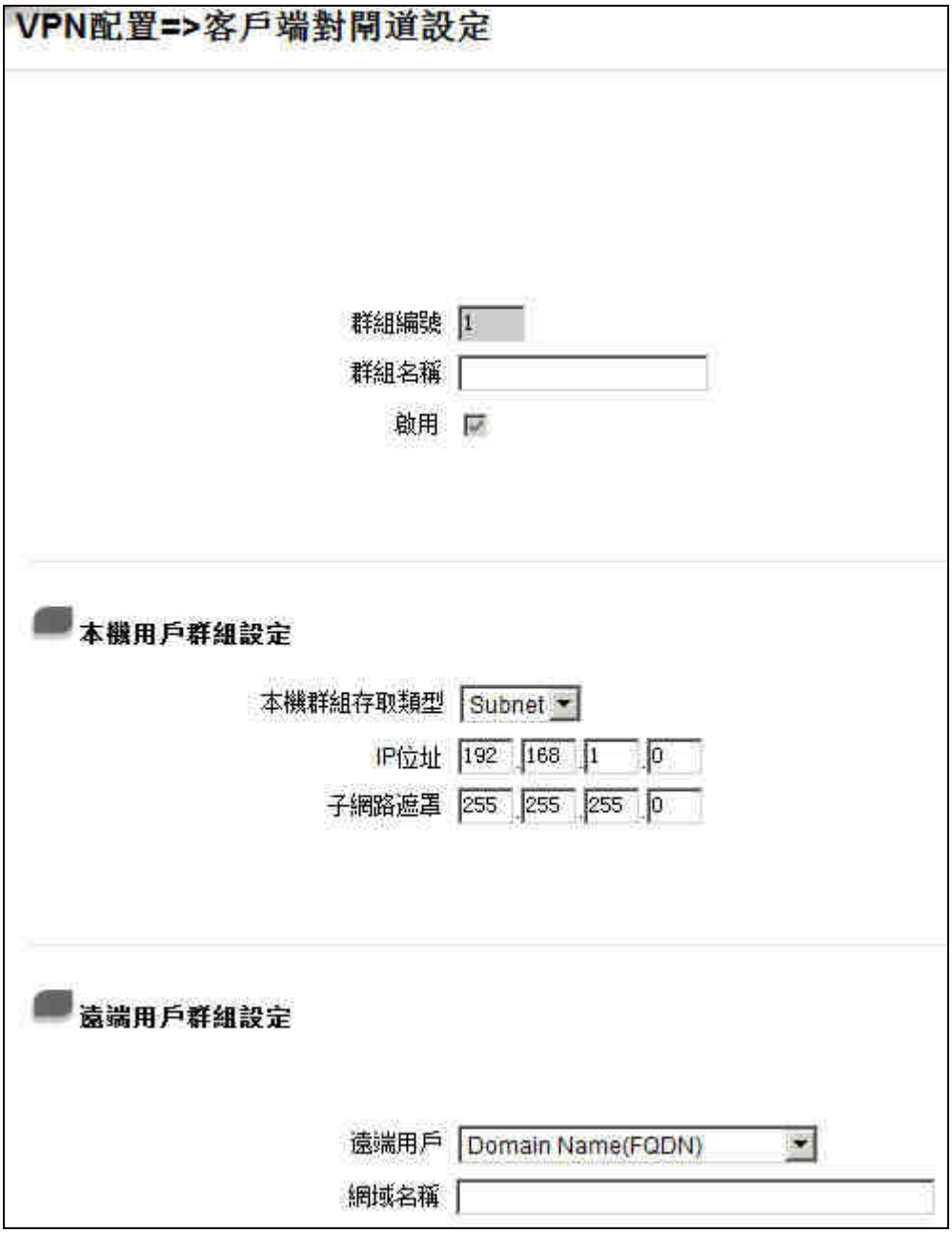
斷線偵測功能 (DPD)
每隔___秒進行偵測：

若選擇此項目勾選，則連接中的 VPN 通道會定期的傳送 HELLO/ACK 訊息封包來偵測 VPN 通道的兩端是否仍有連線存在。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。

7.3 客戶端對閘道器以及群組 VPN 設定(Client to Gateway & Group VPN)

用戶端對閘道器的 VPN 設定有兩個選項：通道模式(Tunnel Mode)以及群組模式(GruopMode)。通道模式(Tunnel Mode) VPN 的設定方式與閘道器對閘道器的 VPN 設定方式大致相同，唯一的不同是 Remote Security 的設定只能設置一個用戶的 IP。

以下介紹群組模式(GruopMode) VPN 的設定方式。



群組編號： 最多可以設定兩組 Group VPN。

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

注意：您需要以 VPN 防火牆連接其他 VPN 設備(非 VPN 防火牆)時，有一些設備規定此通道名稱要與主控端為相同名稱並做驗證，此通道才會順利連線開啟!.

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

本機用戶群組設定： 此為設定本地區域端的 VPN 連線安全群組設定，以下有幾個關於本地區域端設

本機群組存取類型： 定的項目，請您選擇並設置適當參數：

(1)IP Address：

此項目為允許此 VPN 通道連線後，只有輸入此 IP 位置的本地端電腦可以使用此 VPN 通道。

注意：若是您填入 IP 位址的最後一位數為 0，表示整個網段都可以使用此 VPN 連線。例如圖中所示的設定為： 當此 VPN 通道連線後，於 192.168.1.0~255 的此網段的 IP 位置範圍的電腦可以連線。

(2)Subnet：

此項目為允許此 VPN 通道連線後，每一台於此網段的本地端電腦都可以使用此 VPN 通道。

以上圖的設定參考為例：當此 VPN 通道連線後，只有 192.168.1.0，子網路遮罩為 255.255.255.192 的此網段電腦可以使用此 VPN 通道。

遠端用戶群組設定： 遠端用戶端設定，有三種作業模式項目選取，分別為：

Domain Name(FQDN)－網域名稱

E-mail Address(USER FQDN)－電子郵件名稱

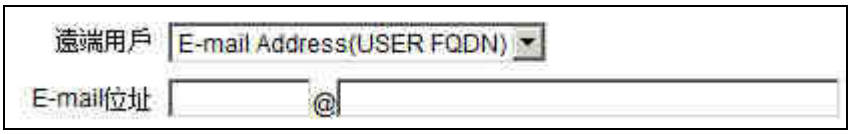
Microsoft XP/2000 VPN Client－微軟 XP/2000 VPN 用戶端

(1) Domain Name(FQDN)：網域名稱

若您選取網域名稱類別的話，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線。

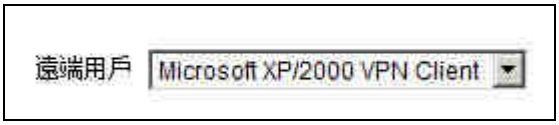
(2) E-mail Addr。(USER FQDN)： 電子郵件名稱

若您選取電子郵件類別的話， 只有固定填入此電子郵件位置可以存取此通道。



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

若您選取微軟 XP/2000 VPN 用戶端形態的話，您不需要在進行其餘設定。



IPSec 的設定細節，請參考 7.2 節中 IPSec Setup 的敘述。

7.4 PPTP 設定

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

啟用 PPTP 伺服器： 當使用者勾選後即可以啟動點對點通道協定 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進入點 IP。起始 IP 位址：請在最後一欄輸入數值。結束 IP 位址：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 / 再次輸入密碼：	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：	移除使用者
所有的 PPTP 隧道狀態：	顯示出使用 PPTP 伺服器通道的使用相關資訊
使用者名稱：	連線建立後的遠端使用者名稱
遠端用戶的 IP 位址：	連線建立後的遠端使用者的 IP 位址
本機對應的 IP 位址：	連線建立後，近端 PPTP 伺服器的 IP 位址

7.5 VPN 透通 (封包穿透路由器功能)

VPN 透通設定可以允許或拒絕區域網內的其他 VPN 設備或是以 PC 上的 VPN 用戶軟體與遠端的 VPN 設備建立 VPN 通道。

IPSec 封包穿透：	若是選擇 Enable 的話，則允許區域網內的其他 VPN 設備或是 PC 端使用 VPN-IPSec 封包穿透 VPN 防火牆，以便與外部 VPN 設備連線。
PPTP 封包穿透：	若是選擇 Enable 的話，則允許區域網內的其他 VPN 設備或 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：	若是選擇 Enable 的話，則允許區域網內的其他 VPN 設備或 PC 端使用 VPN-L2TP 封包穿透 VPN 防火牆，以便與外部 VPN 設備連線。

八、QVM 超快速 VPN 設定

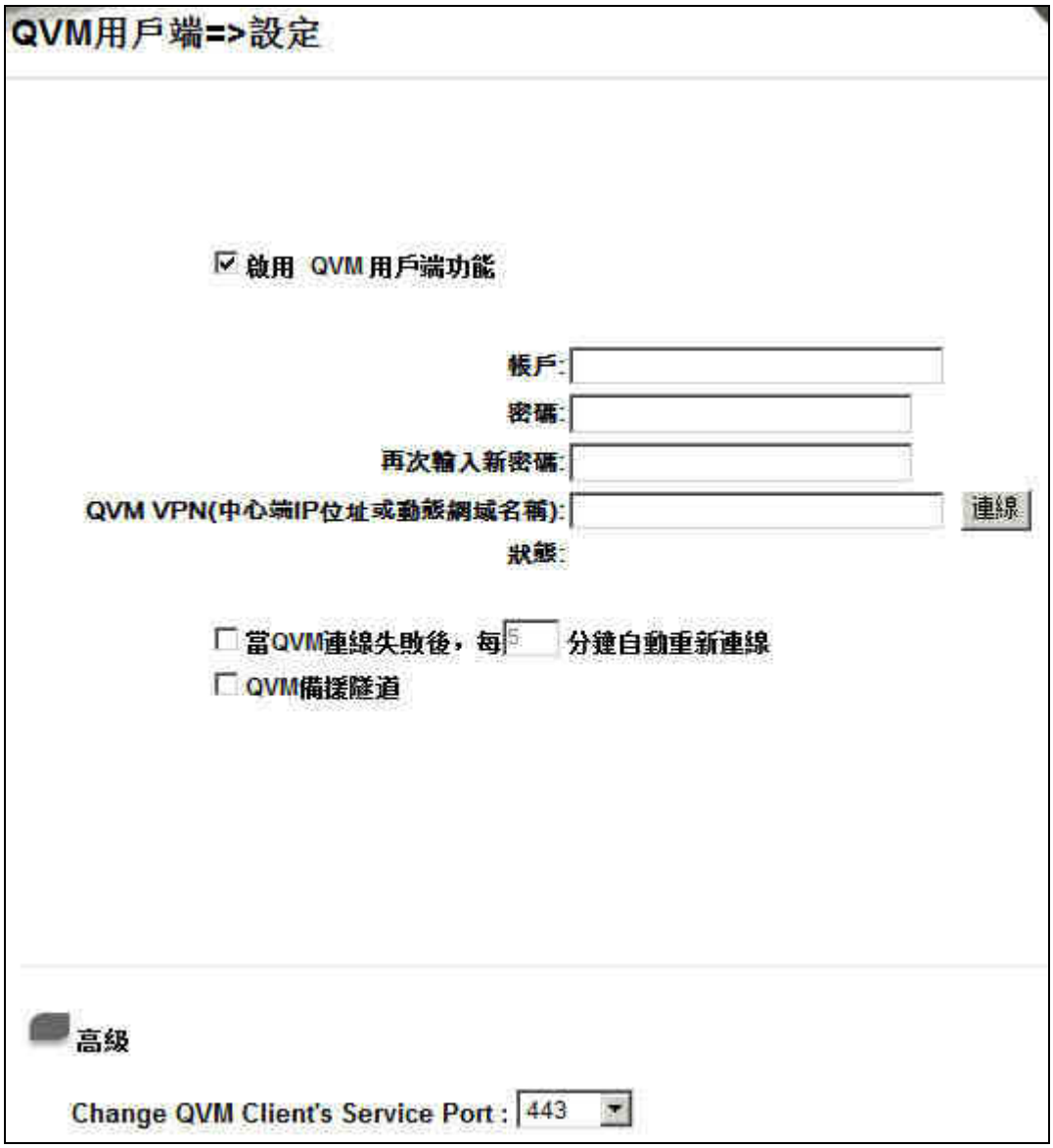
此一功能為 QVM 系列產品獨特功能，特別為簡化虛擬私有網路 IPSec VPN 的複雜配置以及管理方便所設計，符合中大型機構對高性價比以及高整合度負載均衡 VPN 防火牆的需求。你的 VPN 將享有以下特點：

SmartLink 設定： 將原本 IPSec 複雜的設定，簡化為三個參數，仍保有 IPSec 的安全性，減輕網管人員的配置負擔。

遠程管理功能： 網管人員於 VPN 服務器端(QVM SERVER)即可監控各個分支點的聯機及內部相關配置，安全及帶寬管理都可即時完成。

VPN 線路備援： QVM 系列產品於中心端(QVM SERVER)及分支機構(QVM CLIENT)均提供 VPN 線路備援功能，大幅降低 VPN 斷線風險。

在您設定 VPN 防火牆 的 QVM Client 功能時，請確定在 QVM Server (例如 QVM SERVER 有此功能)中建立對應的用戶名(Account ID)以及密碼(Password)，此 QVM 通道才能連接成功。



啟用 QVM 用戶端功能： 若是勾選此選項的話， QVM 功能將被開啟。

帳戶： 輸入已在 QVM Server 中建立的對應用戶 ID。

密碼： 輸入已在 QVM Server 中建立的對應密碼。

再次輸入新密碼： 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 SERVER 中心端 IP 地址或是網域名。

狀態： 在此欄位可以看到 QVM 功能連線狀態。

當 QVM 連線失敗後，每___分鐘自動重新連線： 此功能為 QVM 連線斷開後，重新檢測連接的每間隔時間。出入範圍為 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。

QVM 備援隧道 1/2/3： 輸入對 QVM SERVER 中心端備援連接的 IP 或是網域名。

QVM 連線 Status 的訊息意義如下：

正在連線中。

與 QVM SERVER 認證協議失敗。請檢查對應的用戶名、密碼、中心端 IP、或是網域名是否輸入錯誤。

與 QVM SERVER 連線中斷，請再次重新連線。

與 QVM SERVER 認證完成，但是 IPSec 通道連接失敗。

與 QVM SERVER 認證失敗。請檢查對應的用戶名以及密碼是否正確。

QVM SERVER 服務器錯誤。

與 QVM SERVER 建立連線 QVM SERVER 無反映。

QVM 版本不符合， QVM 建立時，client 須送出 request 並等待 server 的 response。當 server 反應的 QVM function Version 有誤(不是我們所允需的參數)，即顯示該信息。

QVM 訊息無法辨識， QVM 建立時，server 反應的 message type，client 端無法辨識。

與 QVM SERVER 認證完成，正在連接 IPSec 通道。

接收的訊息格式無法辨識， QVM 建立時，client 接收的 server response 不屬於 client 所需的 response 格式。(没有 Vesion 與 status message 等信息)。

QVM 隧道正經由 WAN1 連線至 x.x.x.x (QVM Server IP)。

QVM 隧道經由 WAN1 至 x.x.x.x (QVM Server IP)連線成功。

QVM 用戶端進階設定（Advanced Settings）

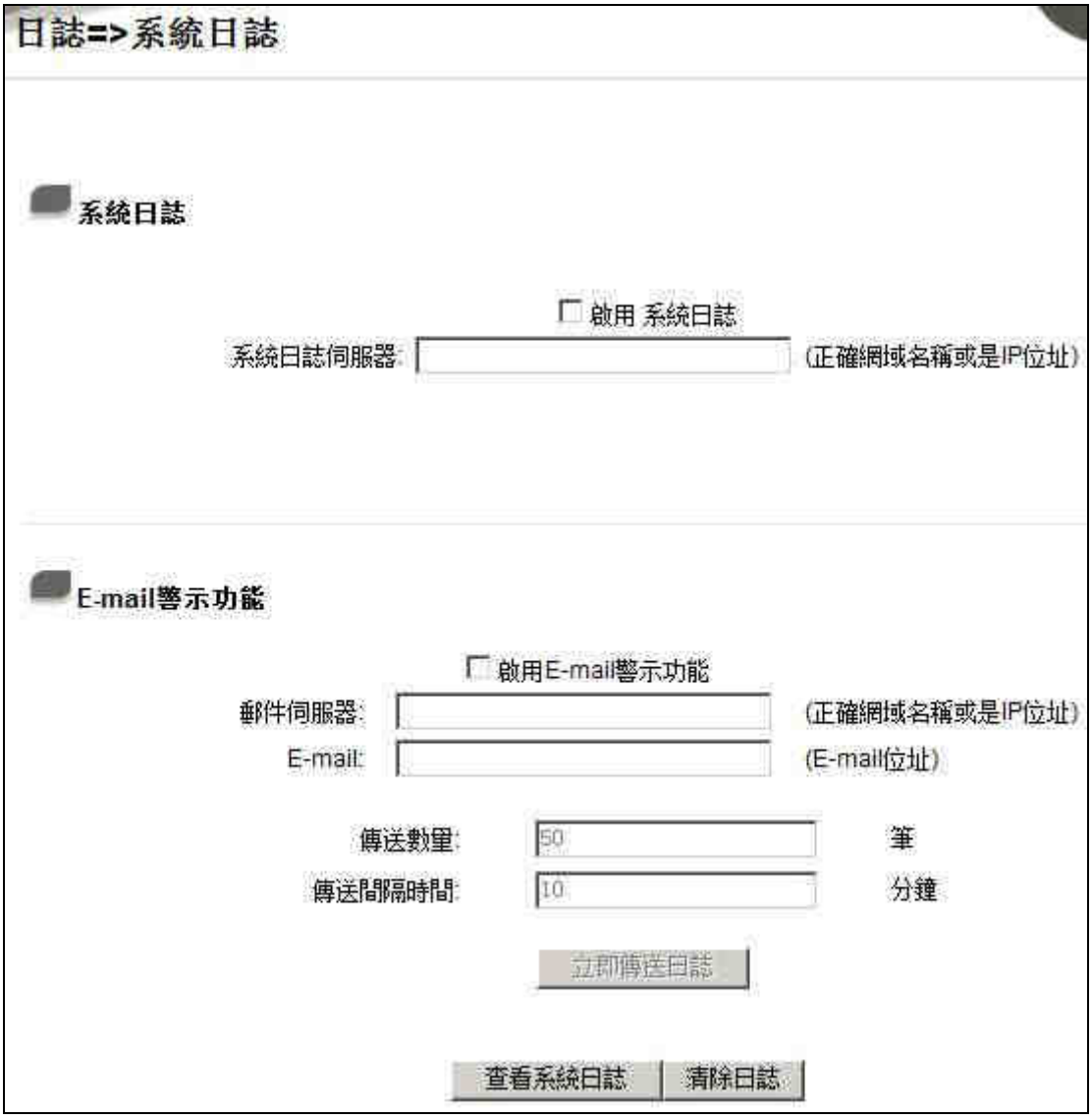
QVM Client 在與中心端 (QVM Server) 進行連線時，是利用 443 Port，但是中心端有時候可能會有 SSL VPN 等服務已經先佔用 443 Port，所以必須使用其他的 Port 如 10443 Port 進行連線。

九、日誌功能設定 (Log Configuration)

日誌(Log)功能紀錄 VPN 防火牆的運行資料，並以可讀的方式呈現再設定畫面上提供給您作為參考。您可以依據需求檢視這些資訊。

9.1 System Log-系統日誌

VPN 防火牆的日誌記錄提供三種設定：系統日誌(Syslog)， 電子郵件通知(E-mail)，以及選擇 Log 的類別。



系統日誌 (Syslog)

啟用系統日誌： 若是勾選此選項的話， Syslog 功能將被開啟。

系統日誌伺服器： VPN 防火牆 提供了外部 Syslog 伺服器收集系統資訊功能。Syslog 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 Syslog 提供了包含動作中的連線來源位置與目地位置， 服務編號(Port Number)以及型態(IP service)。輸入您要接收 Syslog 的伺服器名稱或是 IP 位址於" Syslog Server"的空格欄位內。

電子郵件通知(E-mail)：

啟用 E-mail 警示功能： 若是勾選此選項的話， 電子郵件告警(E-Mail Alert)將會被開啟。

郵件伺服器： 請於此輸入電子郵件伺服器的名稱或是 IP 位置，如 mail.abc.com，此 log 的電子郵件才可以被正確的傳送。

E-mail： 此為設定 Log 收件人電子郵件信箱，如 abc@mail.abc.com。

傳送數量 (筆)： 自訂 Log entries 數量，當到達此數量時，VPN 防火牆 將會自動 Mail 傳送 Log。系統預設為 50 個 entries。

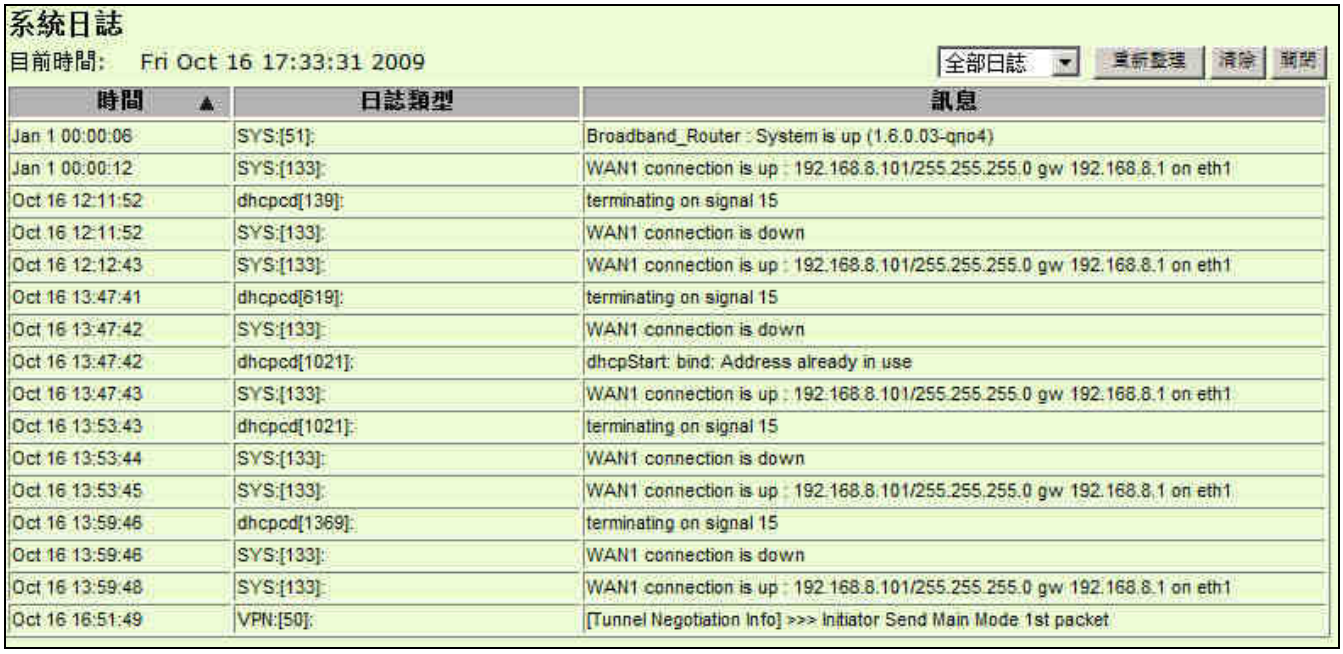
傳送間隔時間 (分鐘)： 自訂傳送 Log 間隔時間，當到達此時間時，VPN 防火牆 將會自動 Mail 傳送此 Log。系統預設為 10 分鐘。

若是您同時設定 entries 數量以及間隔時間，當 entries 數量或是間隔時間其中一個參數先到達，VPN 防火牆 將會自動判別並 Mail 傳送 Log 訊息給管理者。

立即傳送日誌： 使用管理者可以直接於此按鈕傳送 Log。

按下 "查看系統日誌" 可以檢視系統日的相關清單：

此為檢視系統日誌使用，其資訊內容分別可以於 VPN 防火牆連線讀取，包含**全部日誌**，**系統日誌，防火牆日誌**以及 **VPN 日誌**。如下圖所示：



系統日誌

目前時間: Fri Oct 16 17:33:31 2009

全部日誌 | 重新整理 | 清除 | 關閉

時間 ▲	日誌類型	訊息
Jan 1 00:00:06	SYS:[51]:	Broadband_Router : System is up (1.6.0.03-qno4)
Jan 1 00:00:12	SYS:[133]:	WAN1 connection is up : 192.168.8.101/255.255.255.0 gw 192.168.8.1 on eth1
Oct 16 12:11:52	dhcpcd[139]:	terminating on signal 15
Oct 16 12:11:52	SYS:[133]:	WAN1 connection is down
Oct 16 12:12:43	SYS:[133]:	WAN1 connection is up : 192.168.8.101/255.255.255.0 gw 192.168.8.1 on eth1
Oct 16 13:47:41	dhcpcd[619]:	terminating on signal 15
Oct 16 13:47:42	SYS:[133]:	WAN1 connection is down
Oct 16 13:47:42	dhcpcd[1021]:	dhcpStart: bind: Address already in use
Oct 16 13:47:43	SYS:[133]:	WAN1 connection is up : 192.168.8.101/255.255.255.0 gw 192.168.8.1 on eth1
Oct 16 13:53:43	dhcpcd[1021]:	terminating on signal 15
Oct 16 13:53:44	SYS:[133]:	WAN1 connection is down
Oct 16 13:53:45	SYS:[133]:	WAN1 connection is up : 192.168.8.101/255.255.255.0 gw 192.168.8.1 on eth1
Oct 16 13:59:46	dhcpcd[1369]:	terminating on signal 15
Oct 16 13:59:46	SYS:[133]:	WAN1 connection is down
Oct 16 13:59:48	SYS:[133]:	WAN1 connection is up : 192.168.8.101/255.255.255.0 gw 192.168.8.1 on eth1
Oct 16 16:51:49	VPN:[50]:	[Tunnel Negotiation Info] >>> Initiator Send Main Mode 1st packet

9.2 系統狀態

VPN 防火牆 的 System Statistics 管理功能可以提供系統目前運作資訊，包含 Device Name(區域或廣域接口名稱)， Status(目前端連線狀態)， IP Address(IP 地址)， MAC Address(網路實體位置)， Subnet Mask(子網路遮罩)， Default Gateway(預設閘道)， DNS(網域名稱解析伺服器)，Network Service Detection(網路偵測)， Received Packets(收到的封包數量)， Sent Packets(傳送的封包數量)， Total Packets(全部的進出封包數量統計)， Received Bytes(收到的封包 Byte 流量統計)， Sent Bytes(傳送的封包 Byte 流量統計)， Total Bytes(全部進出的封包 Byte 流量統計)， Error Packets Received(收到的錯誤封包統計)以及 Dropped Packets Received ，Session(實際連線數)， New Session/Sec(每秒新增的連線數)等資訊。

日誌=>系統狀態

	區域網	廣域網	DMZ
裝置名稱	eth0	eth1	eth2
線路連線狀態	—	Connected	Enabled
IP位址	192.168.1.1	192.168.8.101	0.0.0.0
MAC 位址	00-0E-A0-12-34-56	00-0E-A0-12-34-57	00-0E-A0-12-34-58
子網路遮罩	255.255.255.0	255.255.255.0	255.255.255.0
預設閘道	—	192.168.8.1	0.0.0.0
DNS伺服器	—	192.168.3.10 192.168.3.15	—
線路偵測機制	—	Disabled	Disabled
接收封包數	78116	36456	0
傳送封包數	89752	32223	0
全部封包數	167868	68679	0
接收封包流量	17327808	30484153	0
傳送封包流量	80653469	12260083	0
全部封包流量	97981277	42744236	0
目前接收流量Bytes/Sec	2199	0	0
目前傳送流量Bytes/Sec	79797	0	0
錯誤封包統計	0	0	0
丟棄封包統計	0	0	0
連線數	—	24	0
新連線數/秒	—	0	0
上傳頻寬使用率(%)	—	0	0
下載頻寬使用率(%)	—	0	0

重新整理

9.3 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。

網路流量統計方式: 依下載流量的IP位置

來源IP位址	bytes/sec	%
192.168.1.100	36	100

Inbound IP Source Address：

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 與所佔的百分比。

網路流量統計方式: 依下載流量的IP位置

來源IP位址	bytes/sec	%
192.168.1.100	36	100

Outbound IP Source Address：

在此圖表中顯示了從內網出去流量的來源端的 IP 位址， 每秒有多少 byte 與所佔的百分比。

網路流量統計方式: 依上傳流量的IP位置

來源IP位址	bytes/sec	%
192.168.1.100	742	100

Inbound IP Service：

在此圖表中顯示了以網路的服務端口來分類進入內網使用流量統計(每秒)byte 與百分比。

網路流量統計方式: 依下載流量的通訊埠

通訊協定	目的埠	bytes/sec	%
TCP	http(80)	49598	99
TCP	443	31	0

Outbound IP Service：

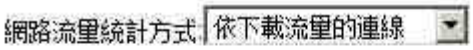
在此圖表中顯示了以網路的服務端口來分類從內網出去的使用流量統計(每秒)byte 與百分比。

網路流量統計方式: 依上傳流量的通訊埠

通訊協定	目的埠	bytes/sec	%
TCP	http(80)	6106	99
TCP	443	30	0
TCP	1863	8	0

Inbound IP session：

在此圖表中顯示了從廣域網絡進來的(Dest. IP)地址所連線的局域網絡的 IP(Source IP)位置所使用的服務端口(Dest.Port)還有現在使用流量(bytes/sec)與百分比。



來源IP位址	通訊協定	來源埠	目的IP位址	目的埠	bytes/sec	%
192.168.1.100	TCP	49689	192.168.3.10	443	696	92
192.168.1.100	TCP	49688	192.168.3.10	443	56	7

Outbound IP Session：

在此圖表中顯示了從局域網絡的 IP(Source IP)地址對外連線的目的地位置(Dest. IP)IP 及所使用的服務端口(Dest.Port)還有現在使用流量(bytes/sec)與百分比。

來源IP位址	通訊協定	來源埠	目的IP位址	目的埠	bytes/sec	%
192.168.1.100	TCP	49710	207.46.124.173	1863	8	100

9.4 特定 IP 位址/通訊埠狀態

VPN 防火牆提供網管人員可以針對某一 IP 或某一特定 Port 去查詢此 IP 去訪問的目的位址，或是有哪些人使用這個 Service Port。其目的可以方便找出某些需要認證的網站無法走 Multi-WAN's 而必須走單一個 WAN 端口，網管人員可以查詢出此目的地的 IP 做 Protocol Binding 綁定來解決此登入問題。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。

日誌=>特定IP位址/通訊埠狀態

特定IP位址/通訊埠狀態: IP位址 IP位址: 192 168 1 100 尋找

來源IP位址	通訊協議	來源通訊埠	接口位置 (WAN)	目地IP位址	目地通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	50172	WAN	192.168.3.10	1155	19	26
192.168.1.100	TCP	49688	WAN	192.168.3.10	443	4	8
192.168.1.100	TCP	56411	WAN	192.168.3.10	1155	0	0
192.168.1.100	TCP	56413	WAN	192.168.3.10	1155	0	0
192.168.1.100	TCP	56412	WAN	192.168.3.10	1155	0	0
192.168.1.100	UDP	51439	WAN	192.168.3.10	53	0	0
192.168.1.100	UDP	56650	WAN	192.168.3.10	53	0	0
192.168.1.100	TCP	56410	WAN	192.168.3.10	135	0	0
192.168.1.100	TCP	49689	WAN	192.168.3.10	443	0	0
192.168.1.100	TCP	49710	WAN	207.46.124.173	1863	0	0
192.168.1.100	TCP	50060	WAN	59.120.77.206	34760	0	0
192.168.1.100	TCP	56414	WAN	192.168.3.10	1155	0	0
192.168.1.100	TCP	56415	WAN	192.168.3.10	1101	0	0
192.168.1.100	TCP	56416	WAN	192.168.3.10	1026	0	0

特定 IP 位址連線狀態：

直接在 IP address 裡填入您想要查詢的 IP 地址，就可以顯示出此 IP 對外連線的所有目的地及 Port Number。

日誌=>特定IP位址/通訊埠狀態

特定IP位址/通訊埠狀態: IP位址 IP位址: 192 168 1 100 尋找

來源IP位址	通訊協議	來源通訊埠	接口位置 (WAN)	目地IP位址	目地通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	50172	WAN	192.168.3.10	1155	19	26
192.168.1.100	TCP	49688	WAN	192.168.3.10	443	4	8
192.168.1.100	TCP	56411	WAN	192.168.3.10	1155	0	0
192.168.1.100	TCP	56413	WAN	192.168.3.10	1155	0	0
192.168.1.100	TCP	56412	WAN	192.168.3.10	1155	0	0
192.168.1.100	UDP	51439	WAN	192.168.3.10	53	0	0
192.168.1.100	UDP	56650	WAN	192.168.3.10	53	0	0
192.168.1.100	TCP	56410	WAN	192.168.3.10	135	0	0
192.168.1.100	TCP	49689	WAN	192.168.3.10	443	0	0
192.168.1.100	TCP	49710	WAN	207.46.124.173	1863	0	0
192.168.1.100	TCP	50060	WAN	59.120.77.206	34760	0	0
192.168.1.100	TCP	56414	WAN	192.168.3.10	1155	0	0
192.168.1.100	TCP	56415	WAN	192.168.3.10	1101	0	0
192.168.1.100	TCP	56416	WAN	192.168.3.10	1026	0	0

特定通訊埠連線狀態：

直接在 Port 裡填入您想要查詢的 Port Number，就可以顯示出此 Port 現在有哪些 IP 正在使用。

日誌=>特定IP位址/通訊埠狀態

特定IP位址/通訊埠狀態: 埠口 埠口: 443 尋找

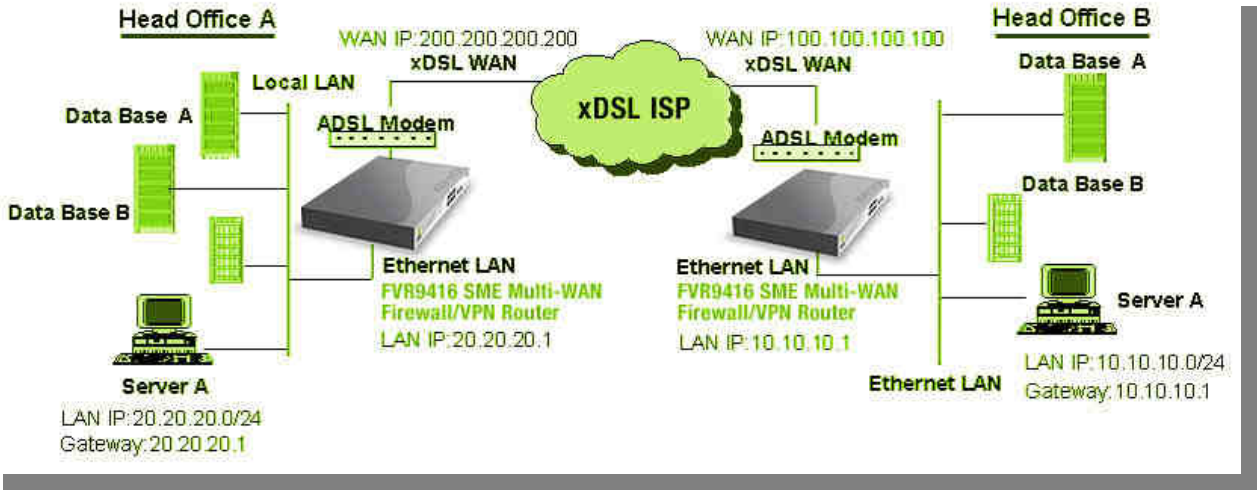
來源IP位址	通訊協議	來源通訊埠	接口位置 (WAN)	目地IP位址	目地通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	49688	WAN	192.168.3.10	443	0	0
192.168.1.100	TCP	49689	WAN	192.168.3.10	443	0	0

十、登出(Logout)

VPN 防火牆的網頁畫面右上方有一個登出(Logout)的按鈕，此按鈕為終止管理 VPN 防火牆並結束此管理畫面。若您下次想再進入 VPN 防火牆管理畫面時，您必須重複進入 VPN 防火牆管理畫面的步驟，並再輸入管理者使用名稱與密碼。

附錄一：虛擬私有網路設定範例 (VPN Setting Example)

VPN Environment Sample 1： Gateway to Gateway



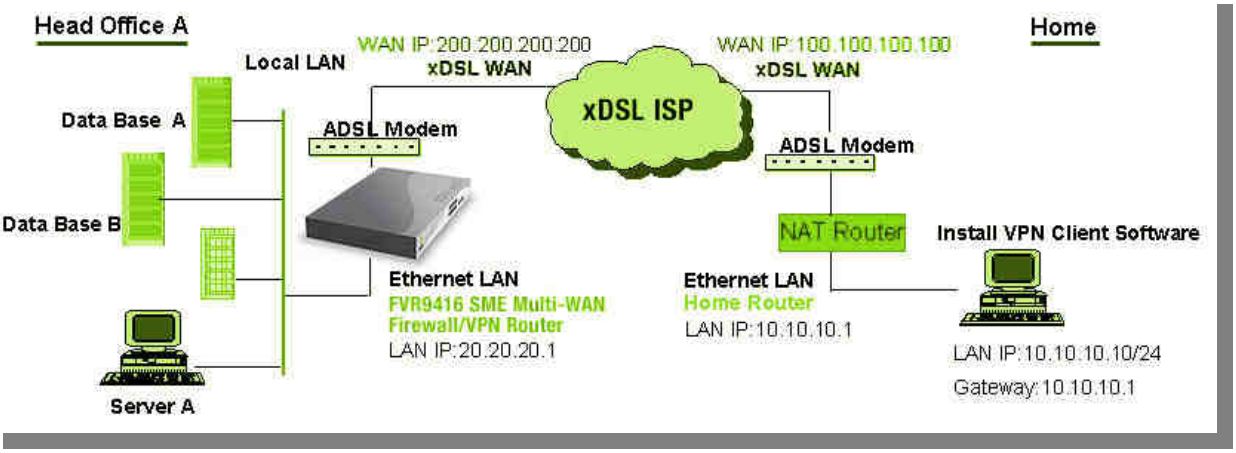
Firewall Setting： Firewall➔General➔Block WAN Request = Disable

VPN Setting： VPN➔Summary➔Add New Tunnel➔Gateway to Gateway

QVM100 VPN Configuration for	Head Office A	Head Office B
Tunnel Name	HOB	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	Subnet
Local Security Group Type➔ IP Address	20.20.20.0	10.10.10.0
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	IP	IP
Remote Security Gateway Type➔ IP Address	100.100.100.100	200.200.200.200
Remote Security Group Type	Subnet	Subnet
Remote Security Group Type➔ IP Address	10.10.10.0	20.20.20.0
Remote Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES

Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Both sides should use the same key.	

VPN Environment Sample 2： Gateway to Gateway

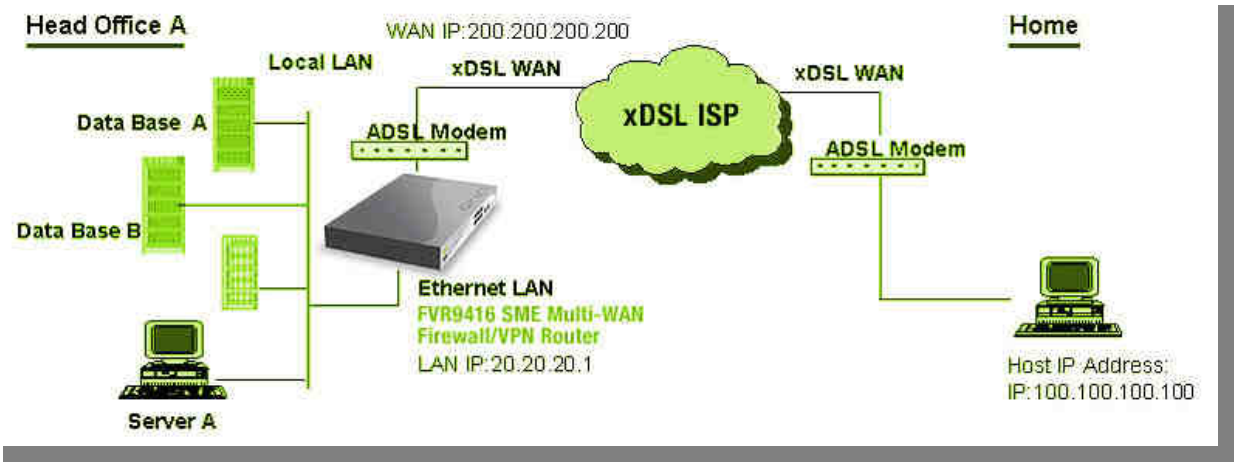


VPN Setting： VPN➔Summary➔Add New Tunnel➔Gateway to Gateway

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	10.10.10.10
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	Domain Name	IP
Remote Security Gateway Type➔ Domain Name	Company domain Name	
Local ID➔ Domain Name		Company domain Name

Remote Security Gateway Type➔ IP Address	100.100.100.100	200.200.200.200
Remote Security Group Type	IP	Subnet
Remote Security Group Type➔ IP Address	10.10.10.10	20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

VPN Environment Sample 3： Client to Gateway (Tunnel)



VPN Setting： VPN➔Summary➔Add New Tunnel➔Client to Gateway➔Tunnel

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN

Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	100.100.100.100
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type➔IP Address		200.200.200.200
Remote Client	Email Address	
Remote Client➔ Email Address	User Email Address	
Local ID➔ Email Address		User Email Address
Remote Client➔ IP Address	100.100.100.100	
Remote Security Group Type		Subnet
Remote Security Group Type➔ IP Address		20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

附錄二：Qno 技術支援資訊

更多有關俠諾產品技術資訊可以聯繫俠諾各經銷商技術部門以及俠諾技術中心。

俠諾台灣官方網站：http://www.Qno.com.tw

俠諾技術中心：E-mail：QnoFAE@qno.com.tw