新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/6/1- 2009/6/14 第93期

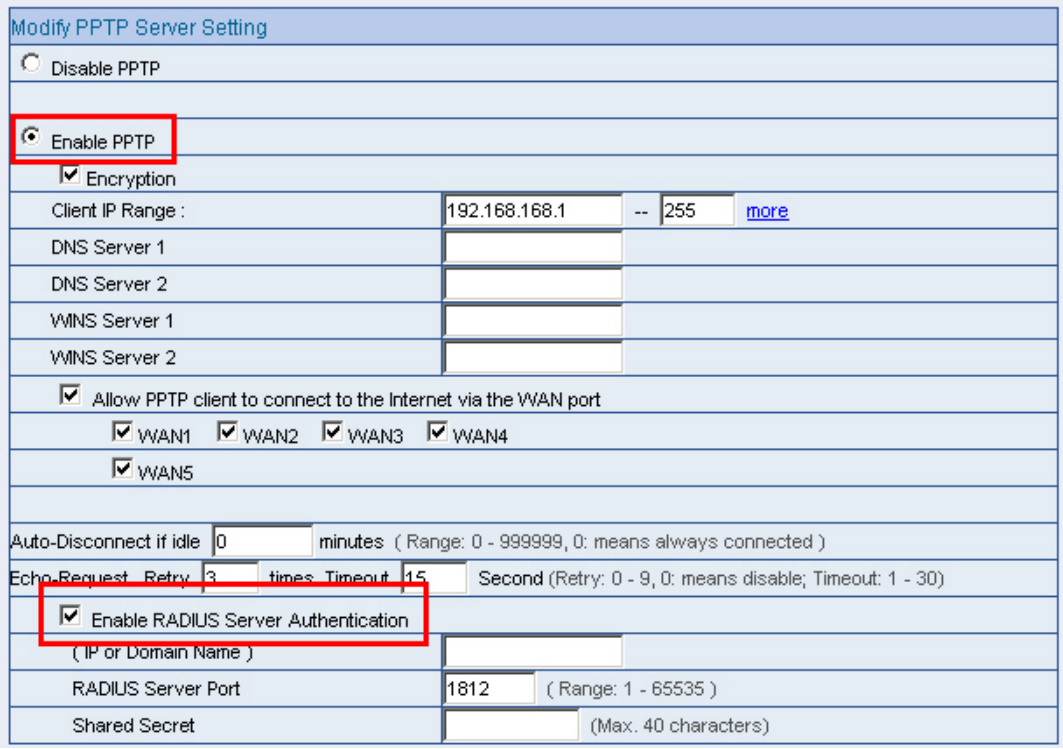
多功能 UTM / MS 系列報導

技術淺談與應用 - PPTP 如需使用 Windows2003 的 RADIUS，WINDOWS 需要有些設置

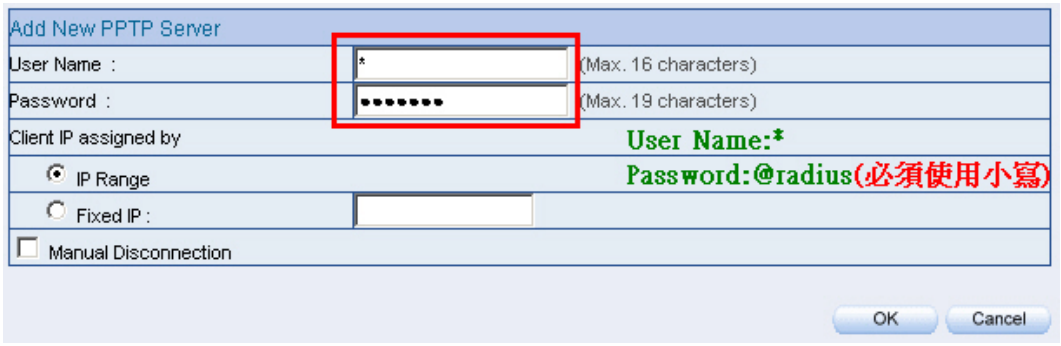
RADIUS（Remote Access Dial In User Service）主要用來提供 Authentication 機制，用來辨認使用者的身份與密碼，確認通過之後，經由 Authorization 授權使用者登入網域使用相關資源。

而新軟系統所推出的 MS 系統產品中也同樣的支援 RADIUS Server Authentication 功能，但對於使用 PPTP 時，在 Windows2003 作業系統的 RADIUS 該如何設置才能正常的與新軟系統產品中的 MS 來正常搭配使用呢？

首先必須於 MH、MS 設備系統中 Policy Object > VPN > PPTP Server 下開啟『PPTP Server』、『RADIUS Server』兩項設定。



並且於 Add New PPTP Server 新增一組帳號及密碼，而帳號為“*”，密碼為“@radius”（特別注意密碼部份必須使用小寫），如此的設定其用意為讓 PPTP Server 主動去問 RADIUS 上的帳號與密碼。

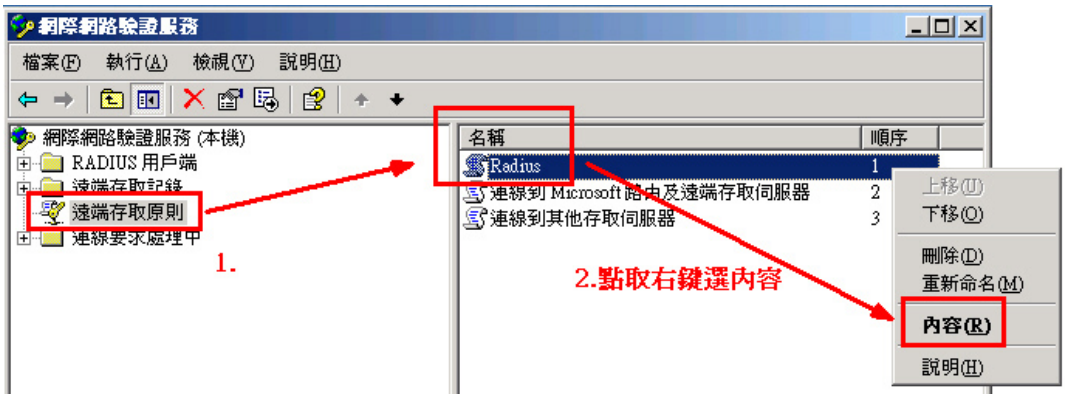


而於 Windows 2003 作業系統中，RADIUS Server 的相關設定方式與內容如下。

步驟一：
點取 Windows 2003 作業系統下的『開始功能表』，選擇『系統管理工具』下的『網際網路驗證服務』

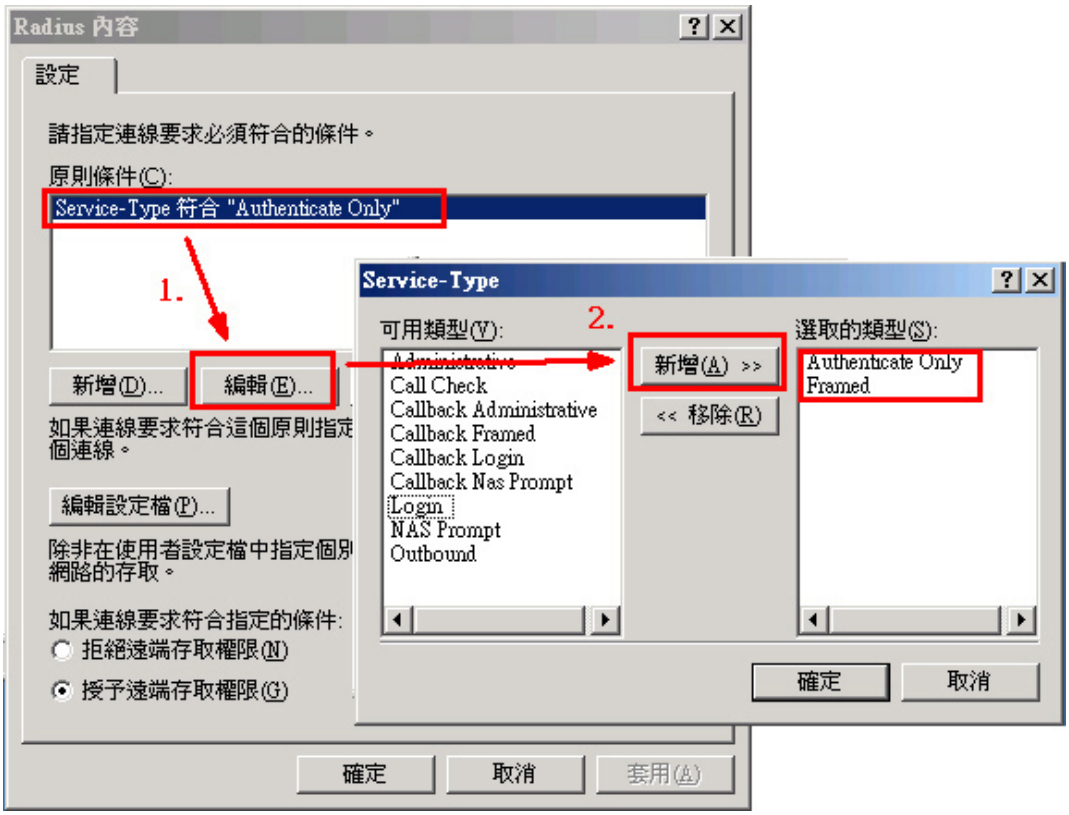
步驟二：

點取進入『網際網路驗證服務』後，選擇底下的『遠端存取原則』，並選擇該公司所設定的 Radius 的名稱，同時利用滑鼠右鍵選取『內容』



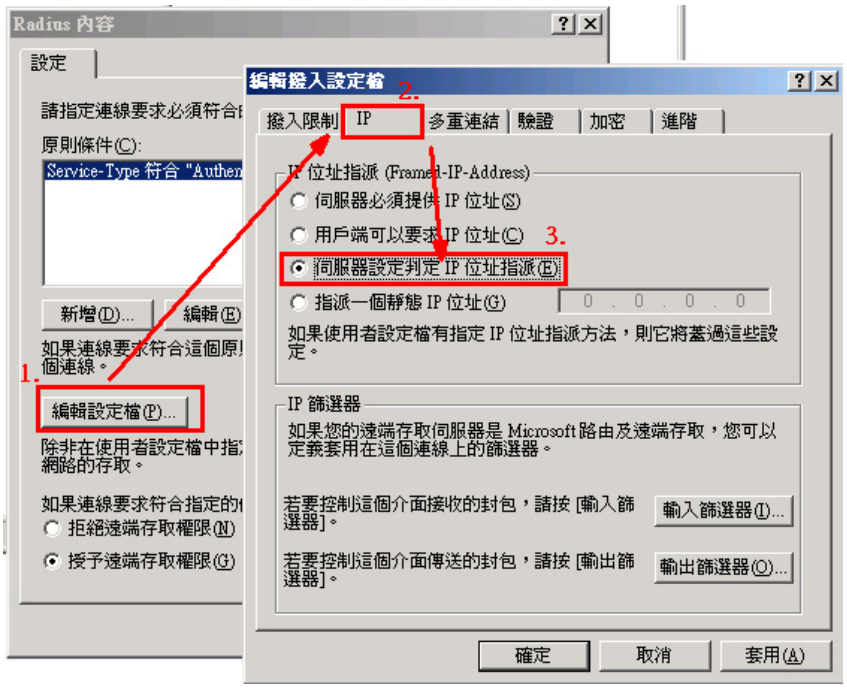
步驟三：

進入內容後，點取原則條件下的『Service-Type 符合" Authenticate Only" 』，並選擇下方『編輯』。於編輯介面中將左方可用類型欄中點選『Authenticate Only』(此為 82 埠用)、『Framed』(此為 PPTP 用)並新增該選項。



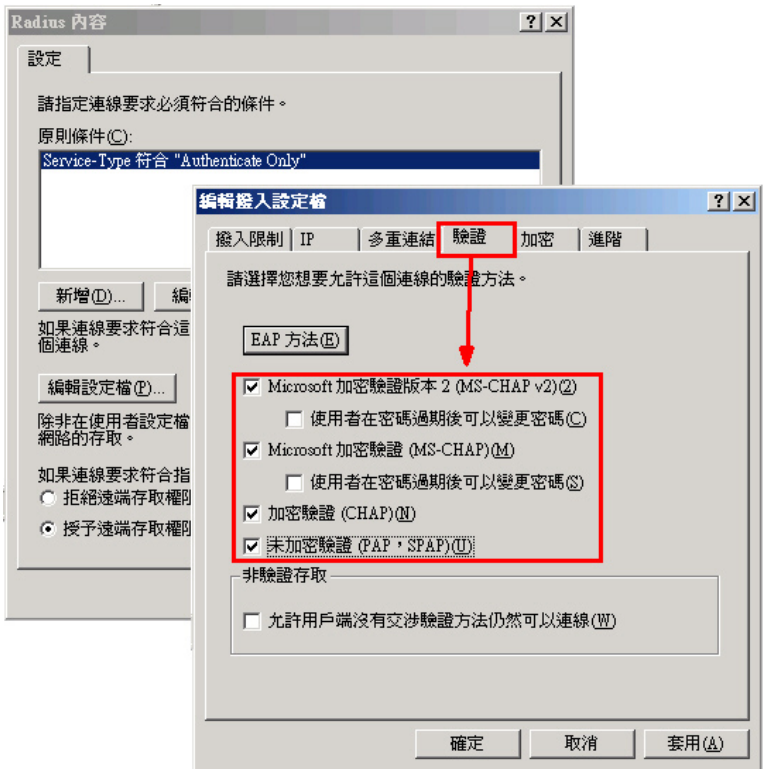
步驟四：

完成上述設定後，回到 Radius 內容介面，並點擊下方的『編輯設定檔』選項進入。於編輯撥入設定檔介面中選擇『IP』設定，將其設定內容中的『伺服器設定判定 IP 位址指派』選擇啟用

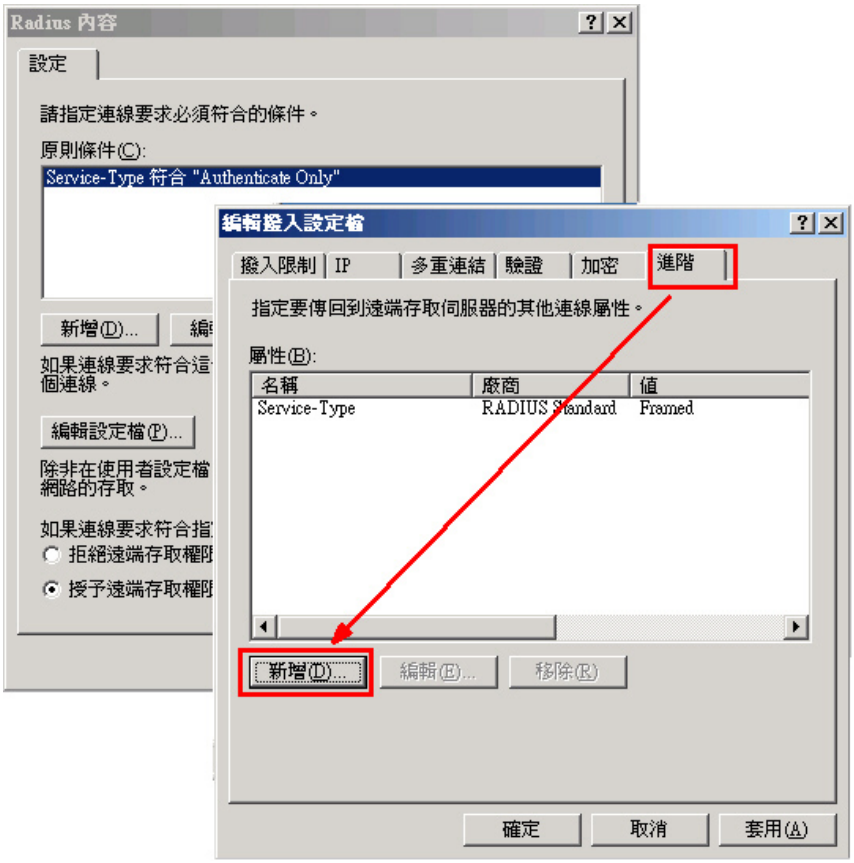


步驟五：

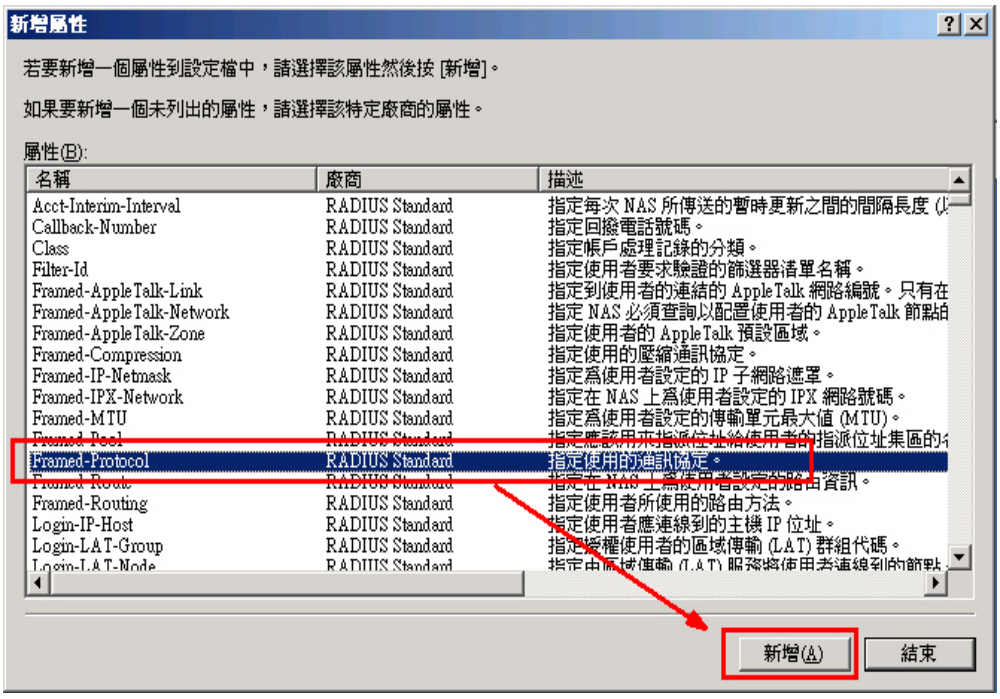
同樣的於編輯撥入設定檔介面中選擇『驗證』設定，將其設定內容中的『Microsoft 加密驗證版本 2（MH-CHAP v2）』、『Microsoft 加密驗證（MH-CHAP）』、『加密驗證（CHAP）』、『未加密驗證（PAP、SPAP）』四項點取啟用。



步驟六：
同樣的於編輯撥入設定檔介面中選擇『進階』設定，並且於下方選擇『新增』。



步驟七：
於新增屬性內容中，新增『Framed-Protocol』。



步驟八：
並設定屬性名稱『Framed-Protocol』屬性值為『PPP』。

步驟九：
將另外的屬性名稱『Service-Type』，屬性值設定為『Framed』。

步驟十：
重新啟動 RADIUS Server，即可。

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - VPN 搭配管制條例，建立真正安全的傳輸管道

現代許多企業為了提高公司營運獲利，因而積極拓展事業版圖，於世界各地設立分公司，但是為了能讓分公司保持對總公司重要訊息連絡的即時性，所以得有一套適當的訊息聯絡方式，因此早期的企業採用電子郵件、即時通訊、FTP 之方式交換訊息，然而這樣之傳輸方式，安全性實在令人不敢領教。所以後來又發展出以架設安全性較高的「專線」來應付如此之需求，但是向電信業者申請一條獨立專線所需花費之費用，對企業來說是相當沉重的一項負擔。

因此在經濟又得實用之商業需求下，以「低成本」、「高安全性」著稱的 VPN 技術逐漸導入於各公司企業內，其原理是將所欲傳送之封包予以加密包裝再送至目的地解密打開，如此之 VPN 技術比起以往赤裸裸的封包傳送方式，以安全性來說是有過之而無不及，而且在成本上也不必依靠高成本所架設的獨立專線來完成，就算是一般 ADSL 線路也可以輕鬆架構完成，因此這樣的 VPN 技術在導入市場初期是相當盛行。

然而，所有科技都會不斷地進步，如此方便之 VPN 技術，雖然可以將來源地封包安全無虞地送到目的地，但是相對的，過於密不通風且無適當過濾機制的傳送架構也漸漸地產生一些問題。例如：來源地電腦已經中毒或是被安裝木馬程式，但是不自知，此時若使用 VPN 技術傳送資料到目的地電腦，等於也將帶有病毒和木馬程式之資料加密保護傳送至目的地電腦內，間接造成目的地電腦跟著中毒。這樣一來，原本以高安全性著稱的 VPN 技術，反而變成電腦與電腦之間互相傳染電腦病毒、木馬程式的最佳途徑。

新軟系統為了做到 VPN 技術 “真正的高安全性” ，將新軟系統 MH／MS 產品與資安管理機制整合，在此以 MS 系列產品為例：當 VPN 在建構時，可以搭配管制條例來過濾 VPN，限定只有某些特定「使用者」能登入，並限定這些使用者能使用哪些特定「服務」（如：FTP、HTTP…等等），另外為了過濾病毒及木馬，可再搭配「IDP」入侵防禦偵測機制及「Anti-Virus」病毒過濾機制一起來使用。藉此，就可有效防範有心人士透過企業內部之間互相信賴的 VPN 通道來做相關違法的事情（如：竊取商業機密、非法存取相關資源…等等）。

	新軟系統多功能 UTM（使用 VPN 時）	一般市售閘道設備（使用 VPN 時）
過濾病毒能力	優 可搭配「Anti-Virus」病毒過濾機制一起使用，在 VPN 中過濾病毒。	無 若來源端電腦所傳送過來的資料中有夾帶病毒，那麼目的端的電腦也將岌岌可危。
過濾木馬能力	優 可搭配「IDP」入侵防禦偵測機制一起使用，在 VPN 中阻擋木馬程式。	無 若來源端電腦所傳送過來的資料中有夾帶木馬程式，那麼目的端的電腦也將會處於後門大開，讓有心人士為所欲為的狀況。

圖 新軟多功能 UTM 與一般市售閘道設備在 VPN 連線上的安全性比較表。

文 黃政銘 ming@nusoft.com.tw