FG110C SSL VPN 配合 Windows AD 帳號認證設定說明

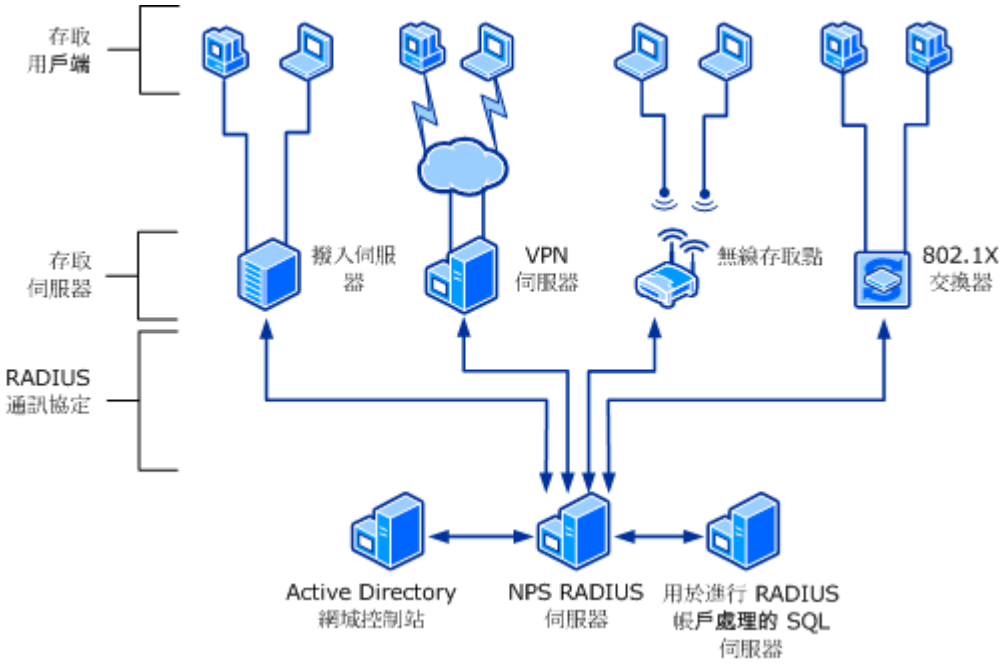
臺中市學術網路管理委員會榮譽委員 沈俊達

壹、目的

解決在 FG-110C 上手動新增帳號及維護密碼的困境，採用與校內 AD 帳號結合方式來管理認證。

貳、Windows Server 2008 R2 使用網路原則伺服器 (NPS) 可用來做為遠端驗證撥號使用者服務 (RADIUS) 伺服器，為 RADIUS 用戶端執行驗證、授權以及帳戶處理。RADIUS 用戶端可以是存取伺服器 (例如 VPN 伺服器或無線存取點)、802.1X 交換器 或 RADIUS Proxy(圖片來源：http://technet.microsoft.com/zh-tw/library/cc755248.aspx)

註：在 Windows Server 2003 使用網際網路驗證服務 (IAS) 做為遠端驗證撥號使用者服務 (RADIUS) 伺服器。



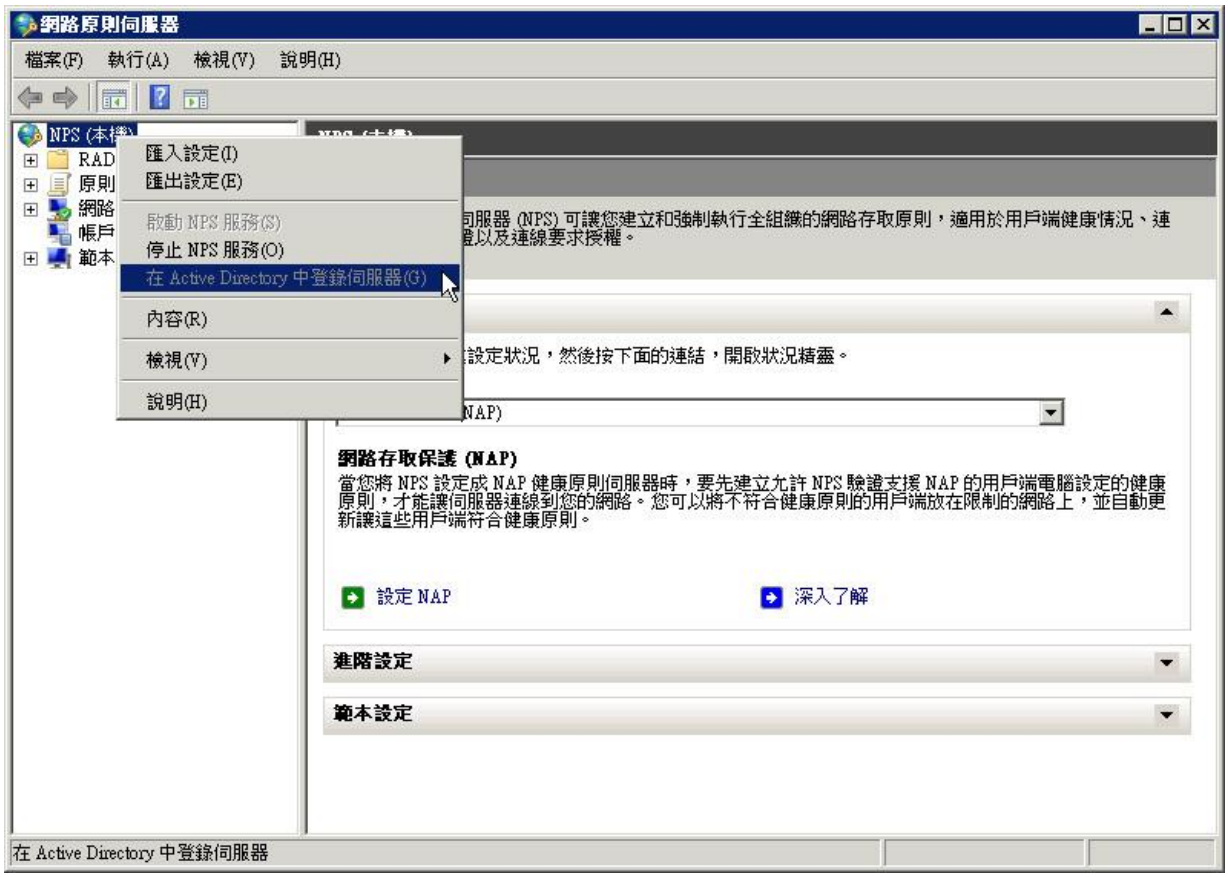
參、RADIUS 伺服器安裝

一、伺服器管理員->角色->新增->勾選網路原則與存取服務

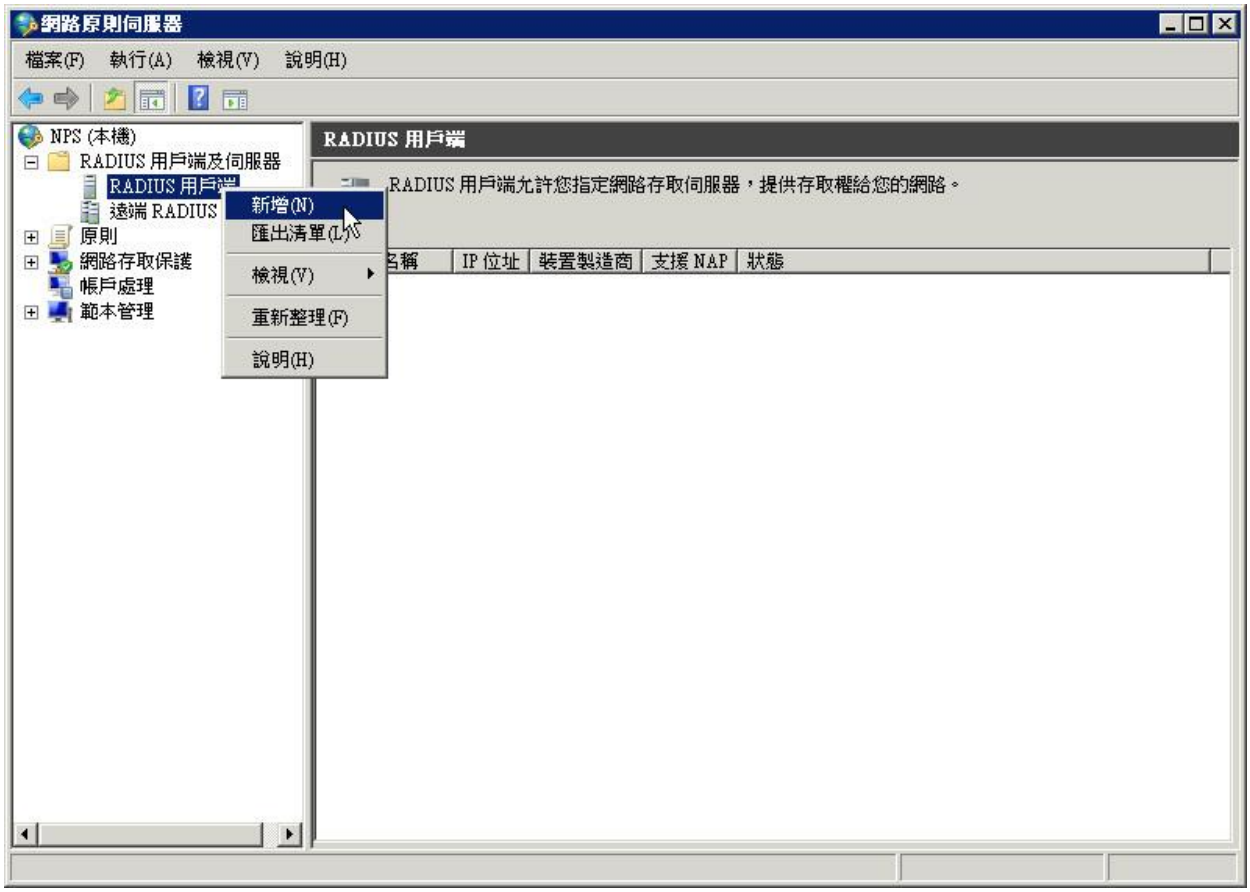
二、勾選網路原則伺服器

三、安裝完成

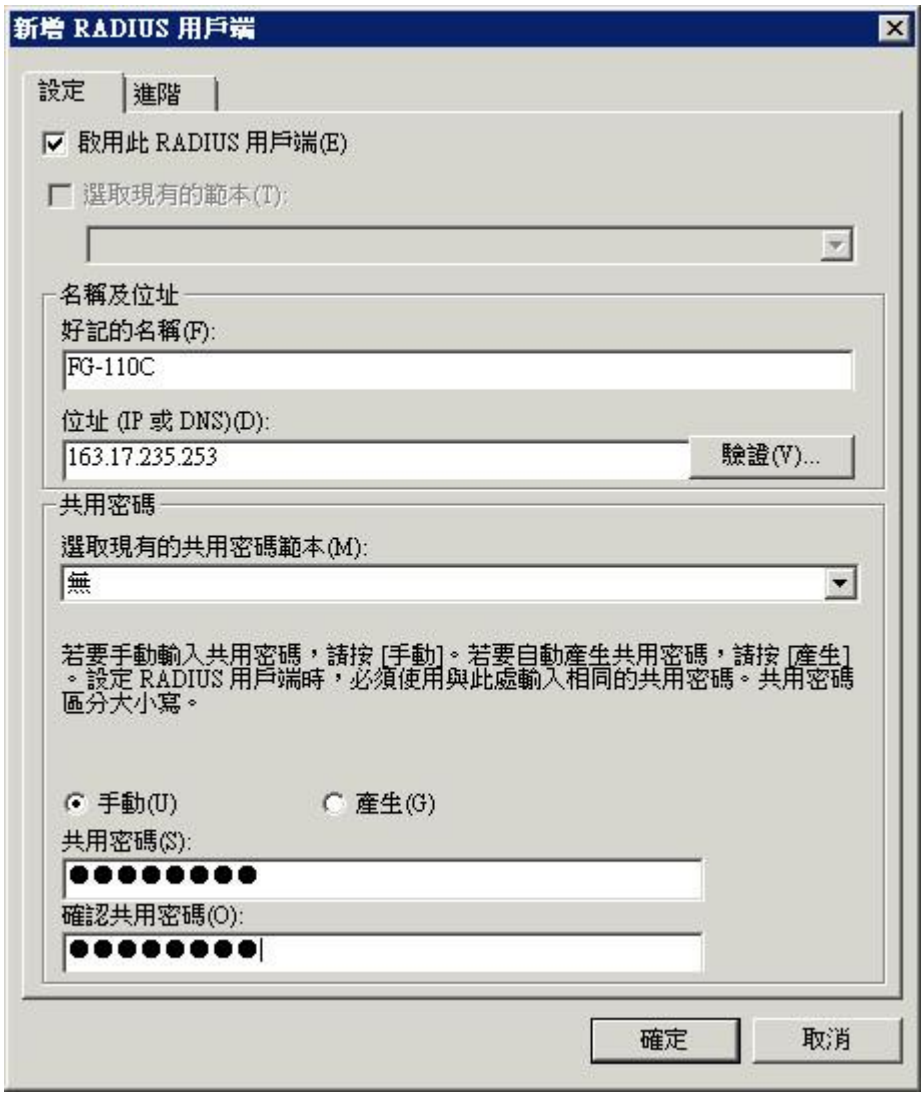
四、讓這部 RADIUS 伺服器可以讀取 AD 帳戶資料：



五、新增 VPN Server(Radius Client)

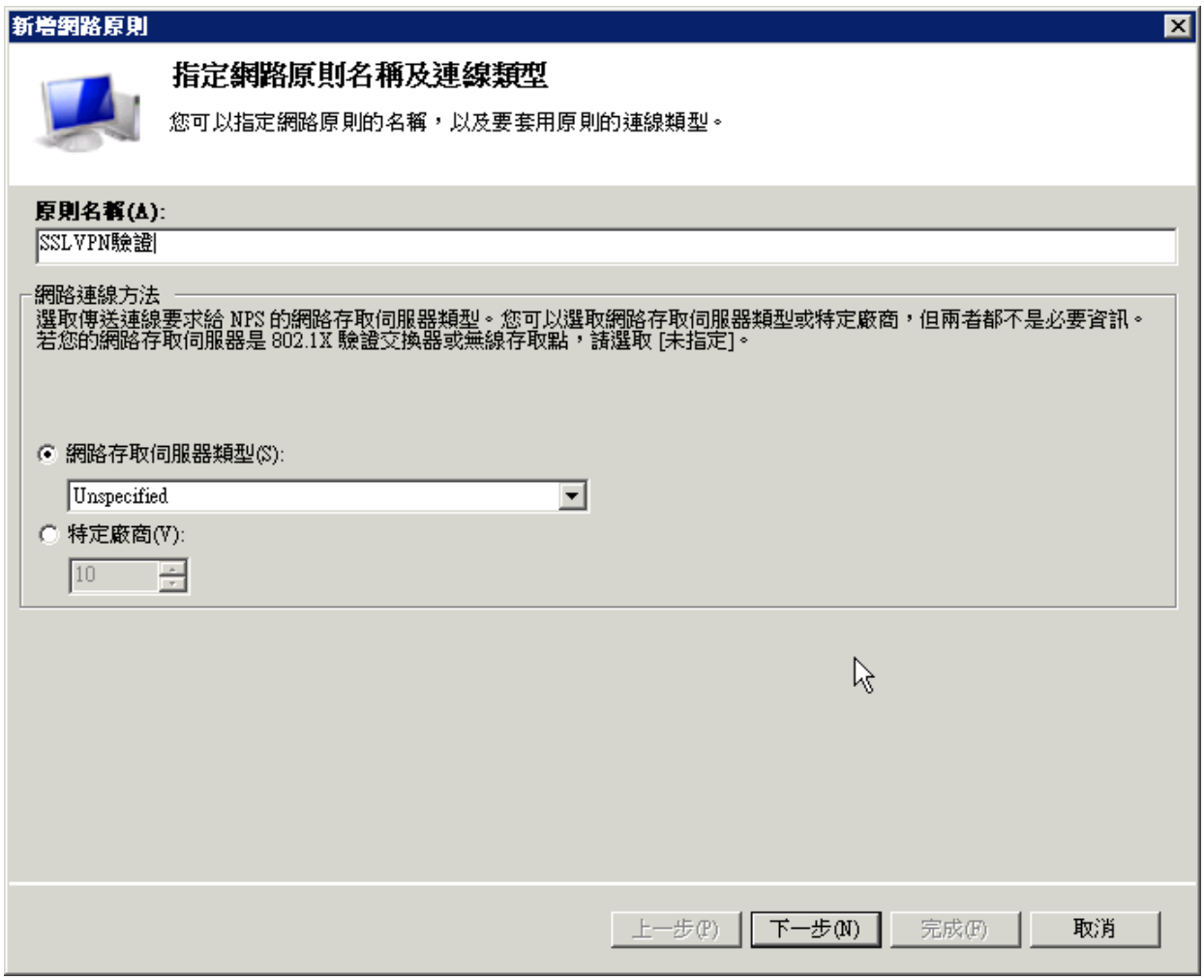


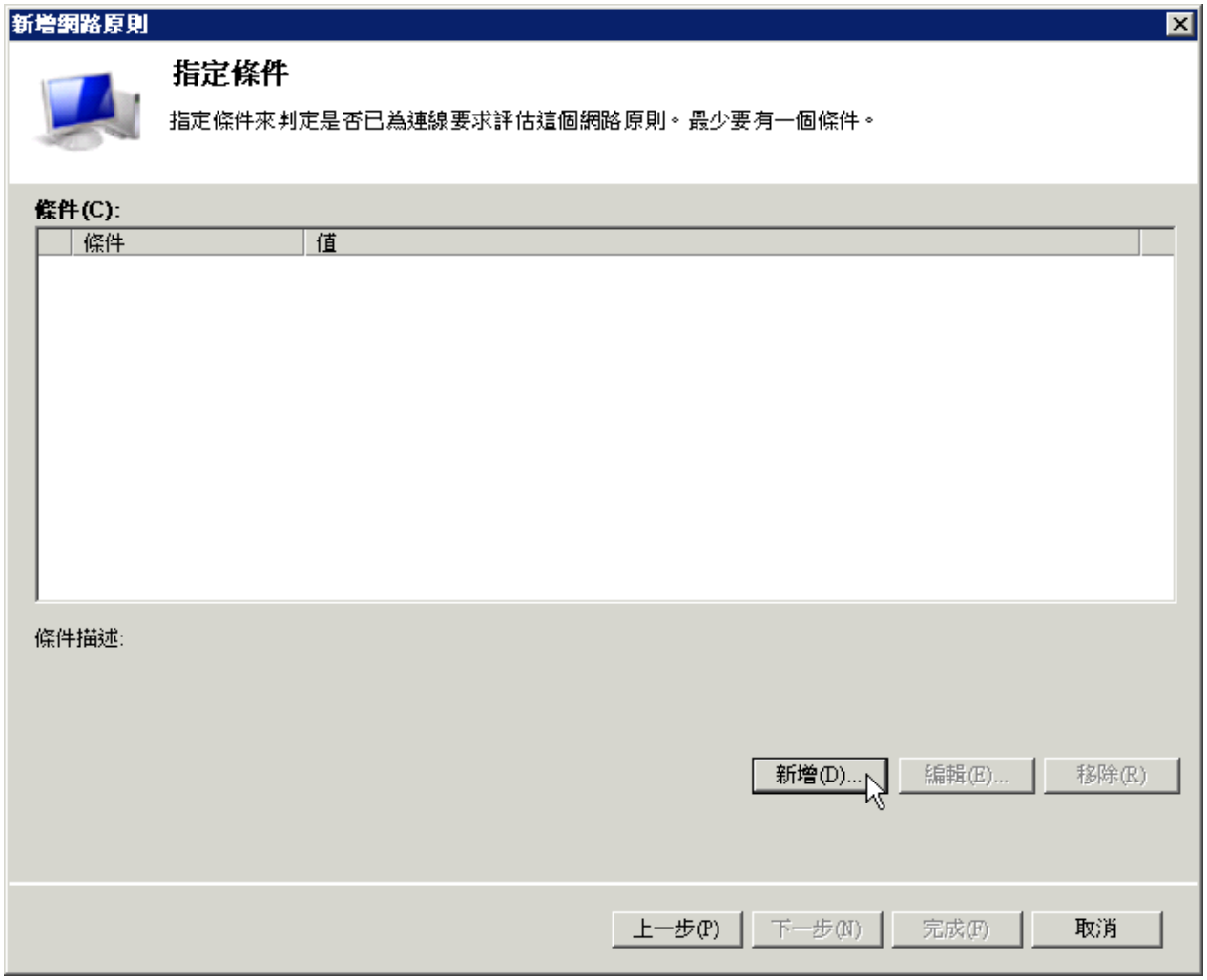
六、建立 Client 名稱與位址及決定共用密碼



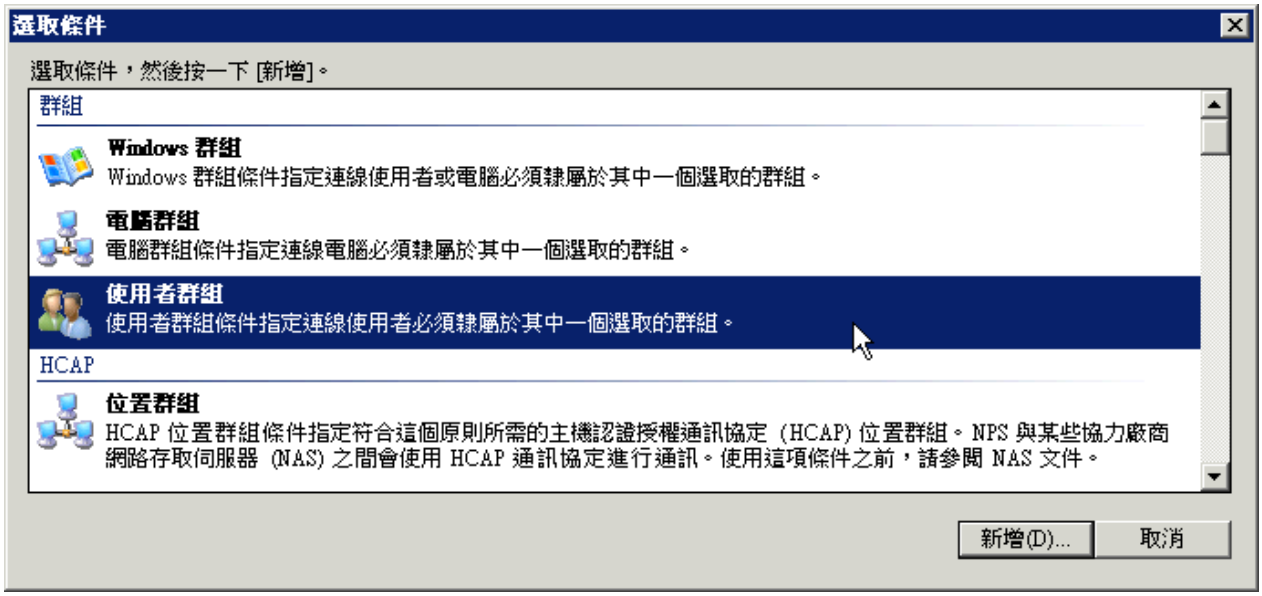
七、新增網路原則

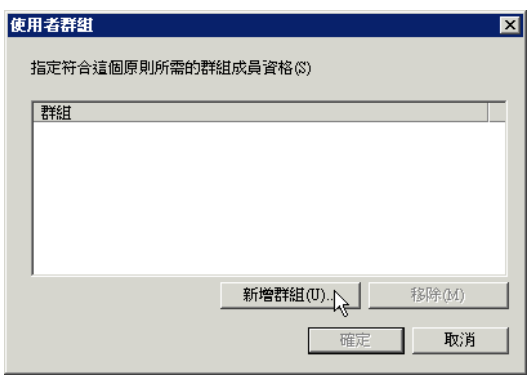

網路原則伺服器
檔案(F)
執行(A)
檢視(V)
說明(H)
NPS (本機)
RADIUS 用戶端及伺服器
原則
連線要求原則
網路原則
健康原則
網路存取保
帳戶處理
範本管理
新增(N)
重新整理(F)
說明(H)
原則
連線要求原則
連線要求原則可讓您指定要在本機處理連線要求，或是轉寄給遠端 RADIUS 伺服器。對於 NAP VPN 或 802.1X，您必須在連線要求原則中設定 PEAP 驗證。
設定連線要求原則
深入了解
網路原則
網路原則可讓您指定得到授權而可連線到網路的人員，以及指定可以連線或不能連線的狀況。
設定網路原則
深入了解
健康原則
健康原則可讓您指定支援 NAP 的用戶端電腦要存取網路所需的設定。部署健康原則的方式是設
新增

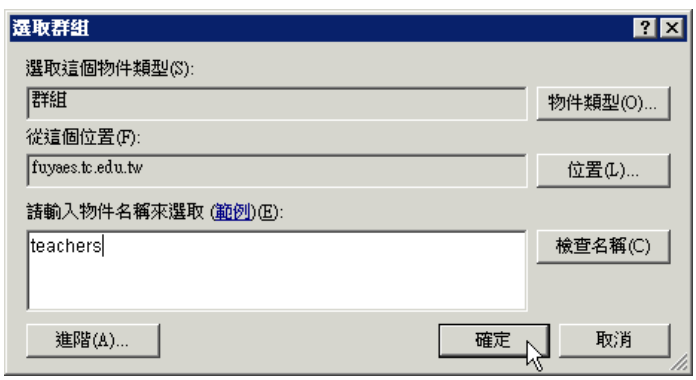

新增網路原則
指定網路原則名稱及連線類型
您可以指定網路原則的名稱，以及要套用原則的連線類型。
原則名稱(A):
SSLVPN驗證
網路連線方法
選取傳送連線要求給 NPS 的網路存取伺服器類型。您可以選取網路存取伺服器類型或特定廠商，但兩者都不是必要資訊。若您的網路存取伺服器是 802.1X 驗證交換器或無線存取點，請選取 [未指定]。
網路存取伺服器類型(S):
Unspecified
特定廠商(V):
10
上一步(P)
下一步(N)
完成(F)
取消



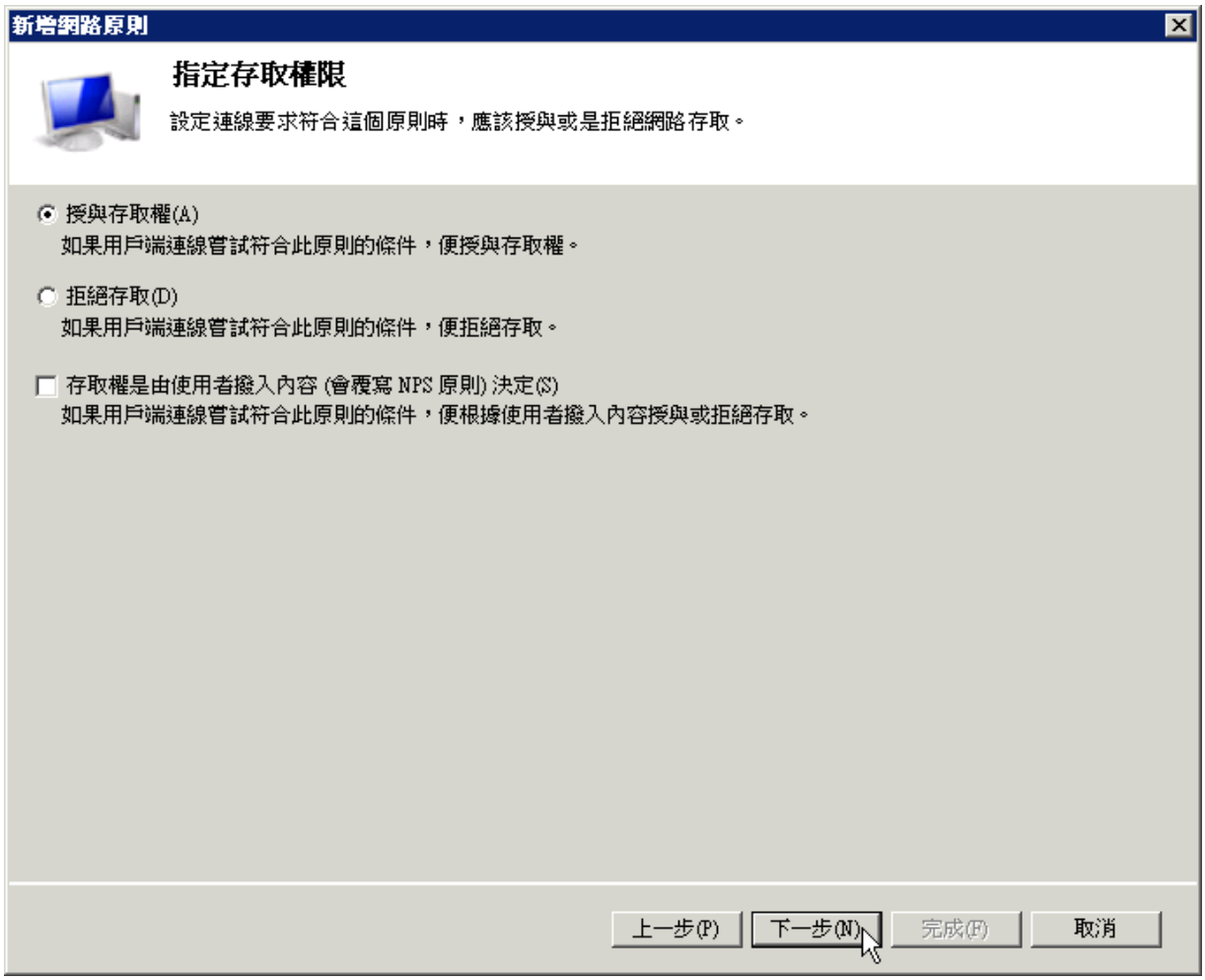
指定要允許使用 SSLVPN 登入的群組



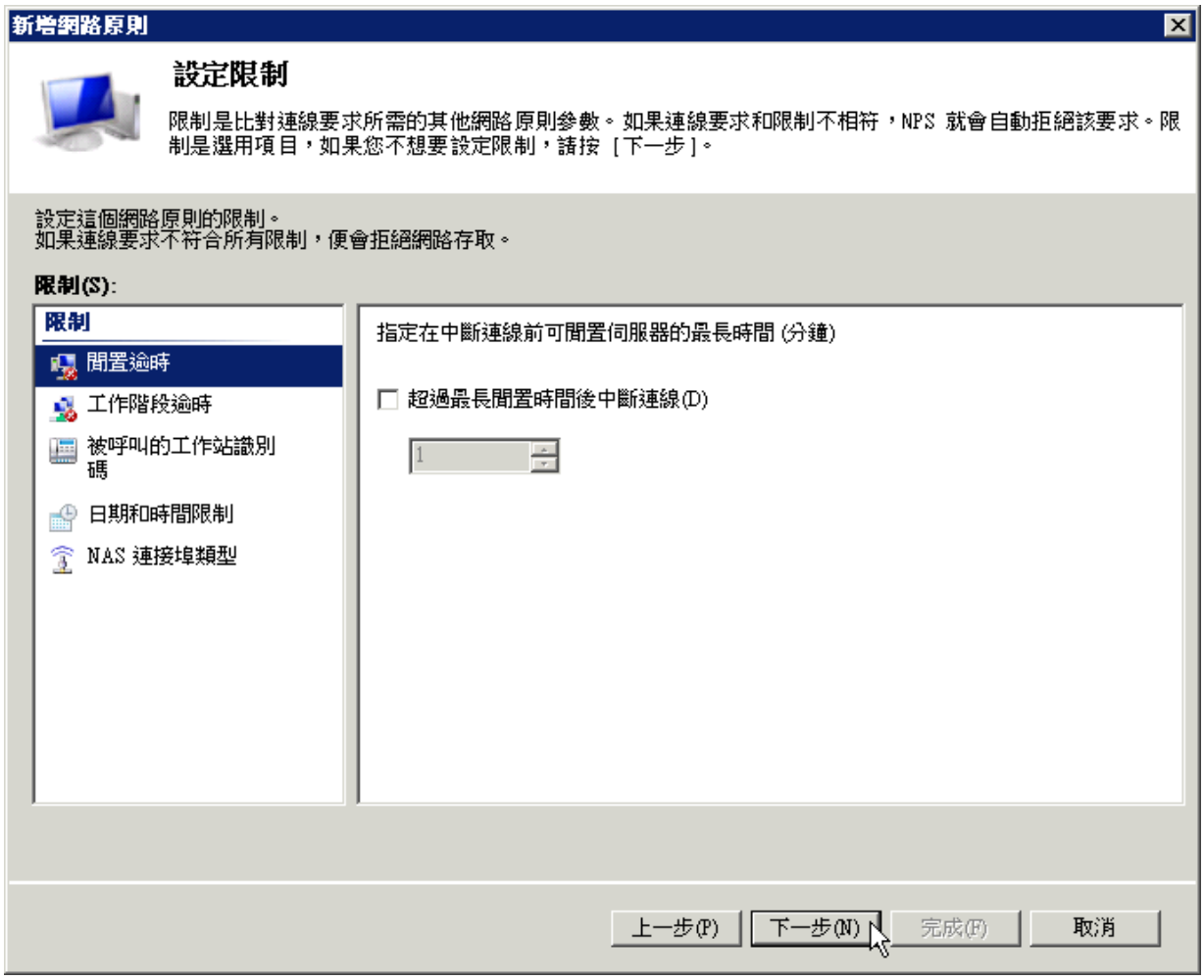


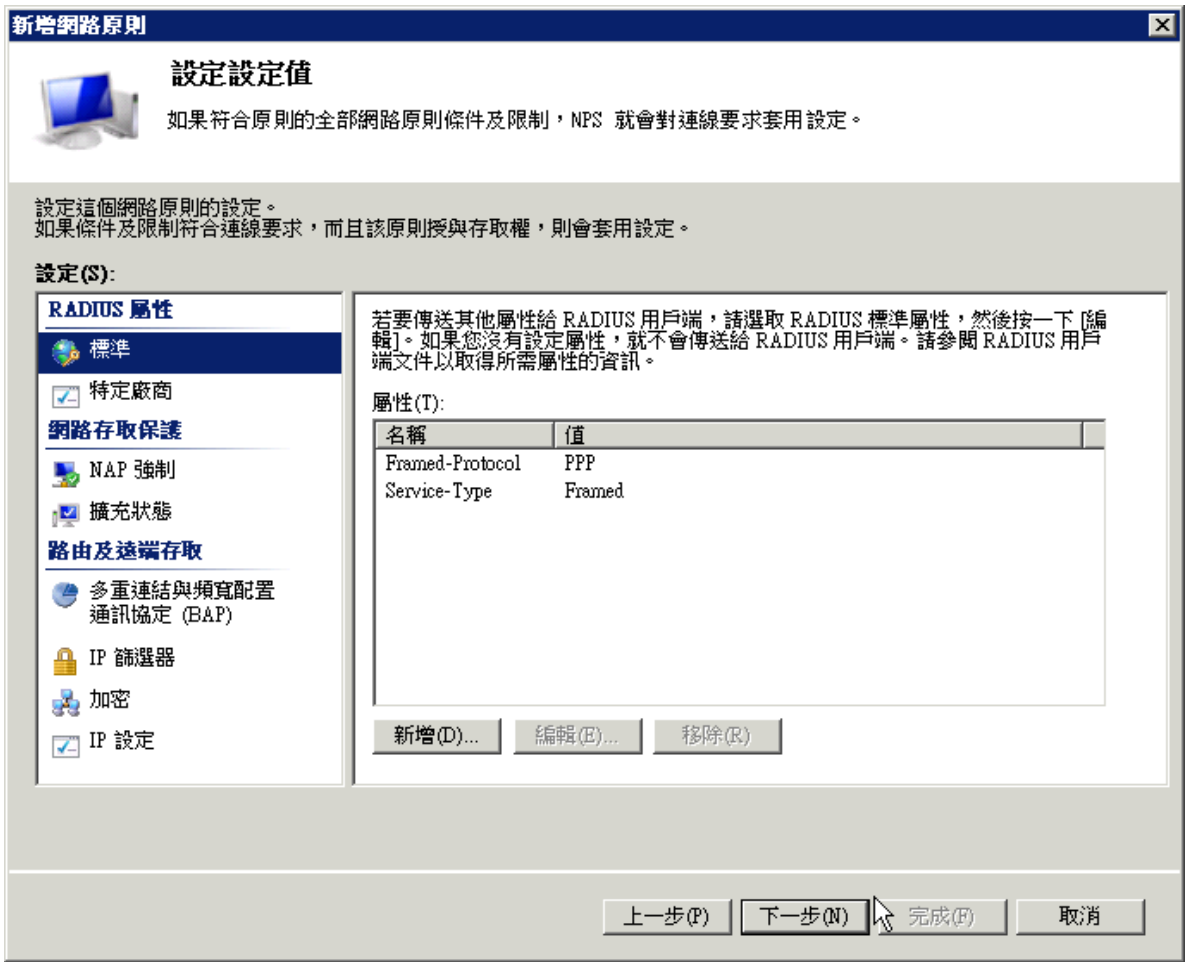


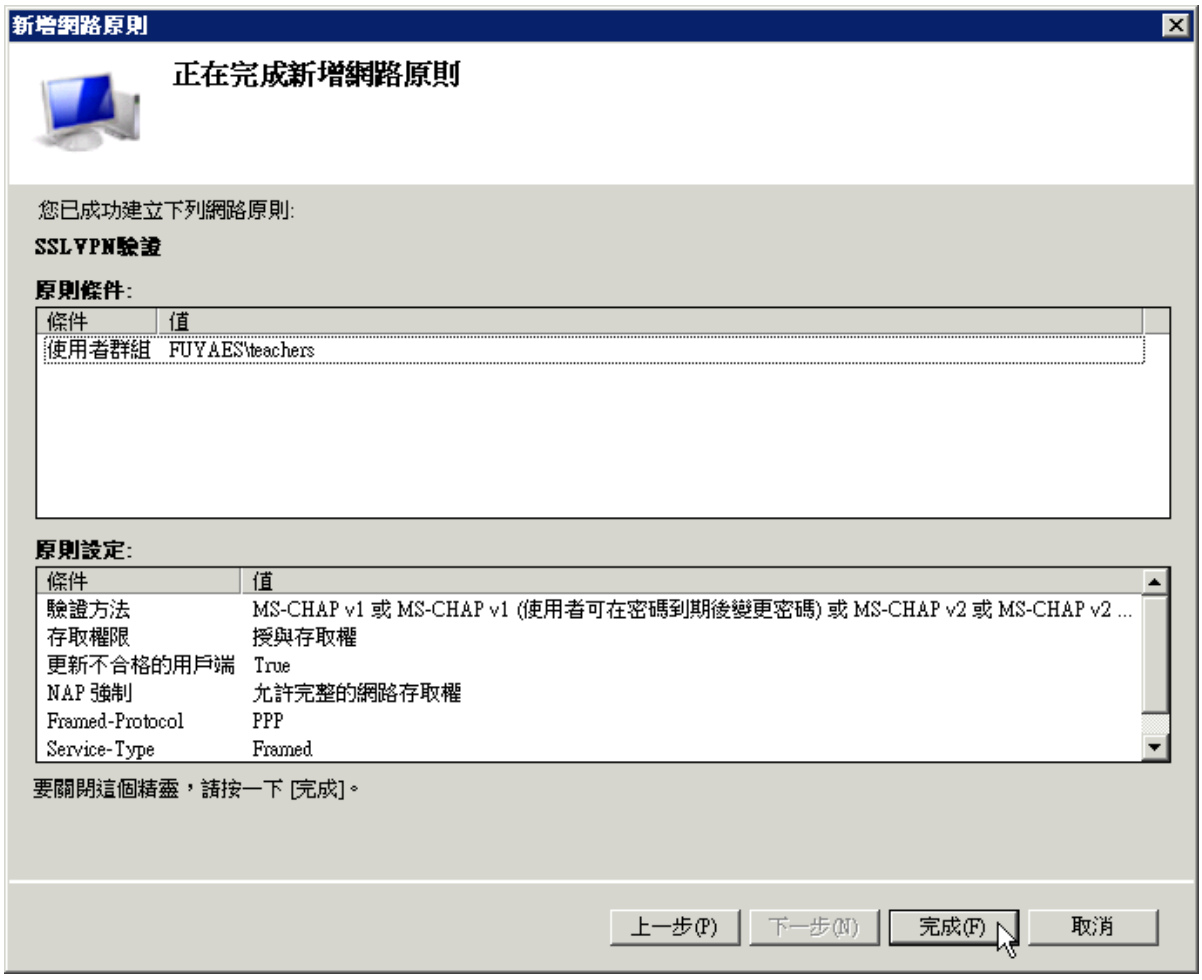
接下來都照預設值即可

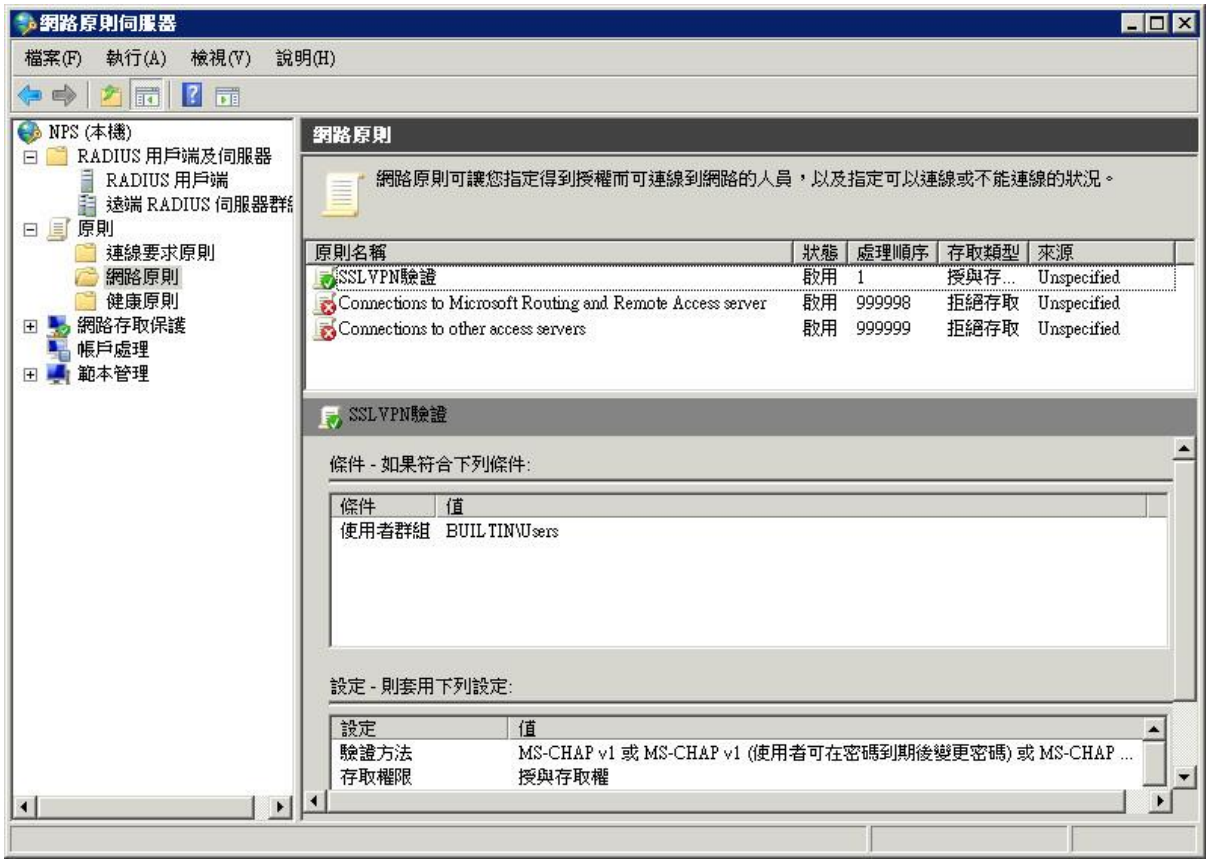

新增網路原則
指定存取權限
設定連線要求符合這個原則時，應該授與或是拒絕網路存取。
授與存取權(A)
如果用戶端連線嘗試符合此原則的條件，便授與存取權。
拒絕存取(D)
如果用戶端連線嘗試符合此原則的條件，便拒絕存取。
存取權是由使用者撥入內容 (會覆寫 NPS 原則) 決定(S)
如果用戶端連線嘗試符合此原則的條件，便根據使用者撥入內容授與或拒絕存取。
上一步(P)
下一步(N)
完成(F)
取消


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


新增網路原則
設定限制
限制是比對連線要求所需的其他網路原則參數。如果連線要求和限制不相符，NPS 就會自動拒絕該要求。限制是選用項目，如果您不想要設定限制，請按 [下一步]。
設定這個網路原則的限制。
如果連線要求不符合所有限制，便會拒絕網路存取。
限制(S):
限制
閒置逾時
工作階段逾時
被呼叫的工作站識別碼
日期和時間限制
NAS 連接埠類型
指定在中斷連線前可閒置伺服器的最長時間 (分鐘)
超過最長閒置時間後中斷連線(D)
1
上一步(P)
下一步(N)
完成(F)
取消


新增網路原則
設定設定值
如果符合原則的全部網路原則條件及限制，NPS 就會對連線要求套用設定。
設定這個網路原則的設定。
如果條件及限制符合連線要求，而且該原則授與存取權，則會套用設定。
設定(S):
RADIUS 屬性
標準
特定廠商
網路存取保護
NAP 強制
擴充狀態
路由及遠端存取
多重連結與頻寬配置通訊協定 (BAP)
IP 篩選器
加密
IP 設定
若要傳送其他屬性給 RADIUS 用戶端，請選取 RADIUS 標準屬性，然後按一下 [編輯]。如果您沒有設定屬性，就不會傳送給 RADIUS 用戶端。請參閱 RADIUS 用戶端文件以取得所需屬性的資訊。
屬性(T):
名稱
值
Framed-Protocol
PPP
Service-Type
Framed
新增(D)...
編輯(E)...
移除(R)
上一步(P)
下一步(N)
完成(F)
取消


新增網路原則
正在完成新增網路原則
您已成功建立下列網路原則:
SSLVPN驗證
原則條件:
條件 值
使用者群組 FUYAES\teachers
原則設定:
條件 值
驗證方法 MS-CHAP v1 或 MS-CHAP v1 (使用者可在密碼到期後變更密碼) 或 MS-CHAP v2 或 MS-CHAP v2 ...
存取權限 授與存取權
更新不合格的用戶端 True
NAP 強制 允許完整的網路存取權
Framed-Protocol PPP
Service-Type Framed
要關閉這個精靈，請按一下 [完成]。
上一步(P)
下一步(N)
完成(F)
取消


網路原則伺服器
檔案(F) 執行(A) 檢視(V) 說明(H)
NPS (本機)
RADIUS 用戶端及伺服器
RADIUS 用戶端
遠端 RADIUS 伺服器群組
原則
連線要求原則
網路原則
健康原則
網路存取保護
帳戶處理
範本管理
網路原則
網路原則可讓您指定得到授權而可連線到網路的人員，以及指定可以連線或不能連線的狀況。
原則名稱 狀態 處理順序 存取類型 來源
SSLVPN驗證 啟用 1 授與存... Unspecified
Connections to Microsoft Routing and Remote Access server 啟用 999998 拒絕存取 Unspecified
Connections to other access servers 啟用 999999 拒絕存取 Unspecified
SSLVPN驗證
條件 - 如果符合下列條件:
條件 值
使用者群組 BUILTIN\Users
設定 - 則套用下列設定:
設定 值
驗證方法 MS-CHAP v1 或 MS-CHAP v1 (使用者可在密碼到期後變更密碼) 或 MS-CHAP ...
存取權限 授與存取權

肆、FG-110C 的設定

使用者認證→遠端→RADIUS 認證→建立新的

設定一個名稱，並輸入 Server 2008 的 ip 位址及共用密碼(安裝 RADIUS Server 步驟六)

伍、新增使用者群組

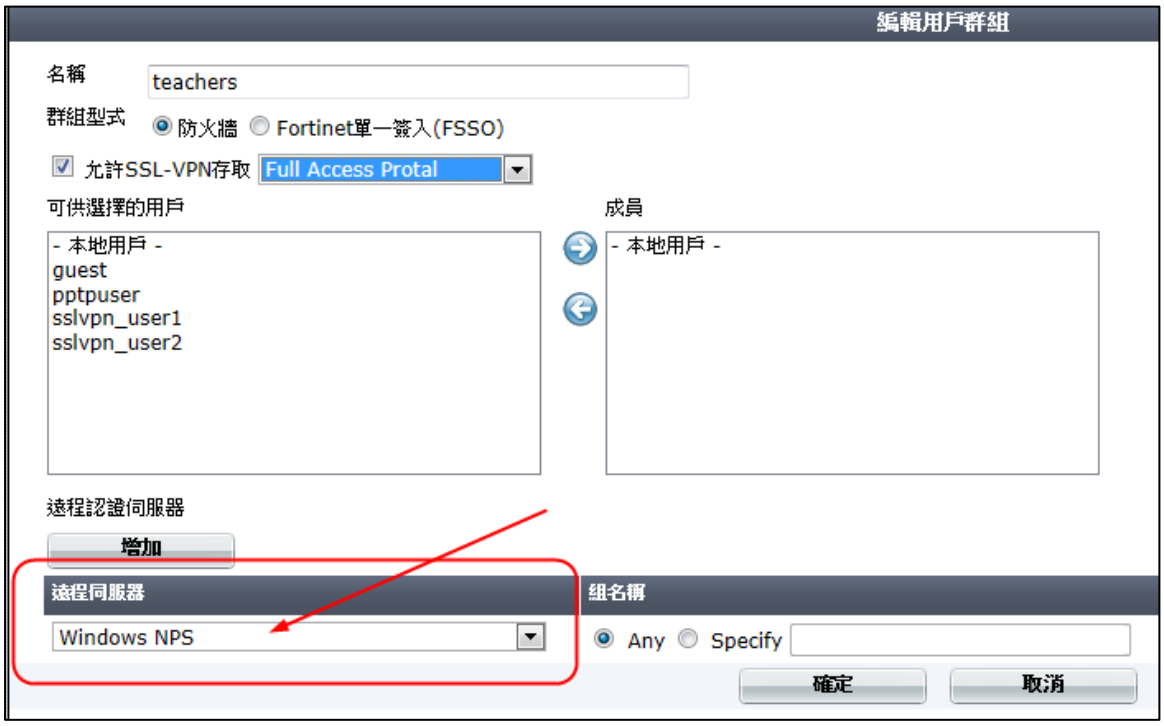
操作步驟：使用者認證→使用者群組→使用者群組→建立新的

1.名稱：自訂一個適當的群組名稱

2.群組類型：防火牆

3.勾選「允許 SSL-VPN 存取」並選擇剛剛建立的「Full Access Protal」，意思是隸屬於這個群組的使用者登入後會使用「Full Access Protal」這個入口頁面。

4.將上一步驟新建的 RADIUS 認證(Windows NPS)加入這個群組的成員。



5.爾後只要是 AD 資料庫內隸屬於 teachers 群組的帳號，都可以使用 SSLVPN 連線了！