VPN 連線：預共享金鑰（PSK）說明

在設定 VPN 連線時，經常會遇到「**預設共享金鑰**」或「**VPN 密鑰**」等選項

VPN 密鑰就像保護您的 VPN 連接的密碼，設定於 VPN 伺服器（例如 WR3600 路由器）上，並且必須與用戶端設備一致，才能建立安全的 VPN 隧道，如果密鑰不正確，設備將無法連線，避免未經授權的存取

VPN 密鑰（PSK）的角色

- 並非帳號密碼的替代，而是額外的驗證層
- VPN 驗證通常包含兩部分：
  1. **帳號/密碼**（使用者驗證）
  2. **預共享金鑰**（裝置驗證）
- 就算帳號密碼洩漏，若沒有正確的密鑰，仍無法成功連接

支援與不支援的機型

- **支援 L2TP/IPsec（含共享金鑰）的機型**
  WR1500、WR3000S、WR3600、M3000
  → 適合連線至大部分需要 PSK 的 VPN 服務，安全性較高
- **僅支援純 L2TP（無共享金鑰）的機型**
  WR300、LT300
  → 僅能使用基本的 L2TP 連線，安全性較低，不建議傳輸敏感資料

使用情境差異

- **L2TP/IPsec（含共享金鑰）**：適用於公司 VPN 或雲端伺服器，安全性高
- **純 L2TP（無 IPsec）**：僅適用於部分舊型伺服器或簡單需求，不建議長期使用

設定注意事項

1. 伺服器與用戶端的 **共享金鑰必須完全相同**（注意大小寫與符號）
2. 若有 NAT 或防火牆，請確認已開放：
   - UDP 500
   - UDP 4500

   以確保 IPsec 正常運作
3. 若連線失敗，可檢查伺服器端 Log 來排除設定錯誤

延伸參考

- L2TP 客戶端設定步驟，請參考 FAQ：
  sfn164【如何設定 Cudy 路由器的 L2TP VPN 客戶端連線?】