

TWAREN SSL-VPN 申請連線須知

一、目的

台灣高品質學術研究網路(TaiWan Advanced Research and Education Network, TWAREN)為提昇國內學術研究水準及規模，TWAREN特提供專屬之SSL-VPN服務。SSL-VPN可針對不同的帳號認證，提供不同的VPN 網路連結，提供學研界使用者可於不在單位時，仍可透過SSL-VPN 接取服務連回校園網路或工作單位使用內部資源。因應連線單位之網路服務申請要求，特訂定本文件，以俾申請作業時有所依循。

二、申請規範

1. 各公私立大學、教育機關以及學術、研究或教育性質之網路，可以機構、機關或代表單位為申請單位向國家高速網路與計算中心(簡稱國網中心)申請SSL-VPN服務。其他機構如：國家級研究機構、政府機關、相關之非營利性研究機構單位或財團法人因從事研究或先進應用系統之開發所需，亦可以專案(即有連線期限者)方式向國網中心申請SSL-VPN服務。連線申請經國網中心審查通過後，方可申請。
2. TWAREN SSL-VPN服務屬實驗性質之線路，TWAREN暫不與申請機構簽訂任何SLA(Service Level Agreement)，但TWAREN維運中心仍將會納入監控機制。
3. 申請機構連線成功後，須遵循台灣高品質學術研究網路(TWAREN)使用規範。

三、連線方式

如附錄所示

四、定義

1. 申請機構：欲申請TWAREN SSL-VPN服務之學校或研究機構
2. 審查單位：TWAREN核心管理團隊
3. Core Node：TWAREN主節點
4. GigaPOP：TWAREN區域網路中心(Point of Presence)

五、權責

1. 申請機構：提出需求、申請連線、提供連線申請書、提供連線工程資料、回報使用狀況
2. 維運單位：執行連線、監控、網頁及Mailing list資料更新
3. 審查單位：審查連線申請

六、作業內容

1. 連線需求：申請機構有連線之需求。
2. 告知客戶連線相關事宜：告知欲申請的連線單位關於他們的權利與義務，並提供「TWAREN 連線申請表格」給客戶。
3. 填寫申請表格：欲連線的機構需填寫連線申請表格，完成後寄至 TWAREN 執行小組。
4. 收件：由 TWAREN 執行小組檢查連線申請表格書的資料是否齊全正確，如否，告知申請機構如何修正。
5. 審查：審查單位依「TWAREN 使用政策」核可或拒絕此申請單位之申請，並將結果告知申請機構聯絡人。
6. 告知客戶：告知審查結果，是否需修改申請資料。
7. 與申請機構聯繫：申請通過後由審查單位通知 TWAREN 維運單位，與申請機構取得聯繫，提供更多技術上的資訊並確定連線時間。
8. 納入監控系統：連線成功後，由維運單位通知審查單位與申請單位，將申請的 SSL-VPN 服務納入網管監控系統。

七、相關表格

1. TWAREN 連線申請表格

八、相關文件

1. 台灣高品質學術研究網路 (TWAREN) 使用規範

附錄：

連線方式：

1. GigaPOP 學校連線方式：

欲使用國網 SSL-VPN 服務之 GigaPOP 學校須配合以下事項：

需提供貴校讓使用者認證之伺服器 IP，並配合國網 SSL-VPN 系統所支援之認證協定做所需之設定，目前國網 SSL-VPN 所支援之認證協定如下：

Local (IVE authentication)
LDAP
NIS
ACE
Active Directory/NT
Radius
Anonymous
SiteMinder
Certificate
SAML(Security Assertion Markup Language)

提供一段 IP Pool 供 Mobile User 使用

學校提供之 IP Pool 必須在貴校內可路由並可出 Internet

提供一組測試帳號待設定完畢我方可先行測試

我方設定完成並測試無誤後，並提供一帶有 IVE(Instant Virtual Extranet)識別字串的網址，學校之使用者可透過此網址 <https://sslvpn9.twaren.net/XXX> (XXX 為該學校的識別字串)，並輸入使用者名稱及帳號認證成功後即可使用此服務。

此服務所有流程如下：

Mobile User 先連往 <https://sslvpn9.twaren.net/XXX> (XXX 為該學校的識別字串)輸入帳號及密碼

SSL-VPN 會將此帳號密碼轉給貴校之認證伺服器做身份認證

認證成功並下載安裝完 Client Software 後會透過 DHCP Server 取得學校 IP

透過 VPLS 連回 GigaPOP 學校讀取學校圖書館資源或經由 TANet 連往 Internet

2. 連線單位學校連線方式：

欲使用國網 SSL-VPN 服務之連線單位學校須配合以下事項：

確定連線單位學校與 TWAREN 連線之方式是否為 Dark Fiber：

如是，則連線單位學校需與我方協調另一 Vlan ID 供 SSL-VPN 使用

如否，則連線單位學校需與電路商申請另一 Vlan ID 供 SSL-VPN 使用

需提供貴校讓使用者認證之伺服器 IP，並配合國網 SSL-VPN 系統所支援之認證協定做所需之設定，目前國網 SSL-VPN 所支援之認證協定如下：

Local (IVE authentication)

LDAP

NIS

ACE

Active Directory/NT

Radius

Anonymous

SiteMinder

Certificate

SAML(Security Assertion Markup Language)

提供一段 IP Pool 供 Mobile User 使用

學校提供之 IP Pool 必須在貴校內可路由並可出 Internet

提供一組測試帳號待設定完畢我方可先行測試

我方設定完成並測試無誤後，學校之使用者可連往

<https://sslvpn9.twaren.net/XXX> (XXX 為該學校的識別字串)，並輸入使用者名稱及帳號認證成功後即可使用此服務。

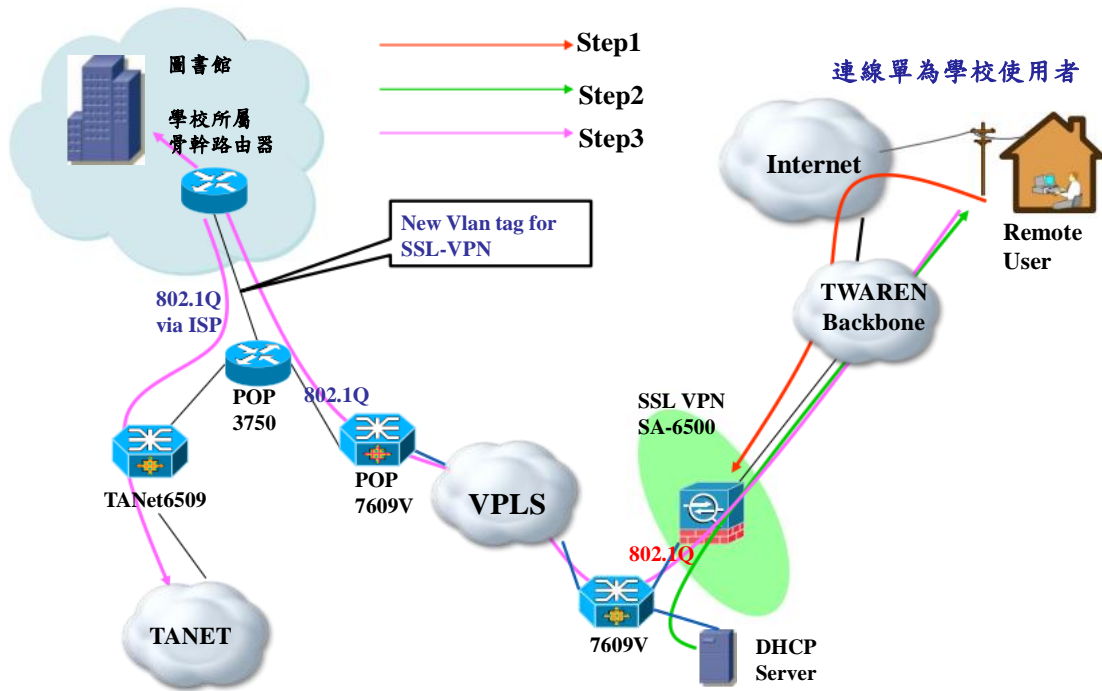
此服務所有流程如下：

Mobile User 先連往 <https://sslvpn9.twaren.net/XXX> (XXX 為該學校的識別字串)，並輸入帳號及密碼

SSL-VPN 會將此帳號密碼轉給貴校之認證伺服器做身份認證

認證成功並下載安裝完 Client Software 後會透過 DHCP Server 取得學校 IP

透過 VPLS 連回 GigaPOP 學校讀取學校圖書館資源或經由 TANet 連往 Internet



3. 非連線單位學校連線方式：

欲使用國網 SSL-VPN 服務之非連線單位學校須配合以下事項：

新增一條專線 (ISP 線路或 Dark Fiber) 進入 GigaPOP 學校機房，再連入 VPLS 網路

確定非連線單位學校進入 GigaPOP 學校機房為 Dark Fiber 或 ISP 線路：

如為 Dark Fiber，非連線單位學校需與我方協調一 Vlan ID 供 SSL-VPN 使用

如為 ISP 線路，非連線單位學校需告知此線路上之 Vlan ID

需提供貴校讓使用者認證之伺服器 IP，並配合國網 SSL-VPN 系統所支援之認證協定做所需之設定，目前國網 SSL-VPN 所支援之認證協定如下：

Local (IVE authentication)

LDAP

NIS

ACE

Active Directory/NT

Radius

Anonymous

SiteMinder

Certificate

SAML(Security Assertion Markup Language)

提供一段 IP Pool 供 Mobile User 使用

學校提供之 IP Pool 必須在貴校內可路由並可出 Internet

提供一組測試帳號待設定完畢我方可先行測試

我方設定完成並測試無誤後，學校之使用者可連往

<https://sslvpn9.twaren.net/XXX> (XXX 為該學校的識別字串)，並輸入使用者名稱及帳號認證成功後即可使用此服務。

此服務所有流程如下：

Mobile User 先連往 <https://sslvpn9.twaren.net/XXX> (XXX 為該學校的識別字串)，並輸入帳號及密碼

SSL-VPN 會將此帳號密碼轉給貴校之認證伺服器做身份認證

認證成功並下載安裝完 Client Software 後會透過 DHCP Server 取得學校 IP

透過 VPLS 連回 GigaPOP 學校讀取學校圖書館資源或經由 TANet 連往 Internet

