僑務委員會「SSL VPN 網路通訊安全閘道系統」簡介

壹、前言

本會當前僑務工作重點在提供多元化的服務，項目包括僑民及僑團聯繫服務、僑民文教工作推展、僑民經濟事業輔助、僑生回國升學輔導、僑民證照服務、函授教育、新聞傳播與海外文宣等。為推展各項僑務工作，本會於海外各主要華人聚居地區均已派駐僑務秘書於當地協助辦理僑民服務相關工作。

本會僑務秘書因工作需要必須利用海外當地電腦經由網際網路連接本會內部伺服主機，以執行本會各項應用系統。為提升本會公務資料安全，本會目前提供 IPSec VPN（虛擬私有網路設備）作為僑務秘書連接本會內部應用系統伺服主機之入口，並全程進行加密作業以防止資料遭到竊取。

由於 IPSec VPN 之安裝與使用手續太過繁雜，且使用者分布全球造成後續維護工作十分不便，對本會派駐海外僑務秘書之日常工作推展造成影響。因此，本會規劃導入 SSL VPN 網路通訊安全閘道系統以解決上述問題。

相較於舊型 IPSec VPN 的缺點眾多，SSL VPN 具備以下優點：

一、使用容易－使用者個人電腦僅需具備支援 HTTPS 協定之瀏覽器（如微軟 Internet Explorer）即可使用，使用者不必自行安裝任何軟體或改變任何網路組態設定，一切交由電腦系統自動處理。

二、安全性佳－SSL VPN 之架構本身是一個代理伺服器角色，使用者的電腦並不會直接進入本會內部網路系統，其基本架構就比 IPSec VPN 更安全。使用者端除了經過帳號密碼檢查確認安全無虞方可與 SSL VPN 設備連線外，未來甚至可以結合個人金鑰（如內政部核發之「自然人憑證」、USB 憑證、I-Key…等）或其他身分認證機制做到更安全的存取管理。

三、簡化管理－可以與本會現有使用者認證機制（包括 Microsoft Active Directory、Novell eDirectory）整合，不必另行管理一套使用者帳號認證系統，好處是簡化日常管理程序，以及降低管理人力需求。

四、網路架構相依性低－使用者端不論是採用何種網路架構或 IP 組態，只要可以正常上網瀏覽網頁就可以使用 SSL VPN 設備連線使用本會資訊系統，減少本會駐外人員的使用障礙。

貳、專案說明

本系統導入期間為一個月（日曆天），在此期間內陸續完成下列工作：

一、裝機：本會規劃購置 SSL VPN 網路通訊安全閘道系統兩套並設定爲 HA (High Availability)架構，以便建立負載平衡及備援的機制；該系統規劃安置於防火牆內以加強資訊安全防護能力。

二、帳號認證測試：於本系統設定使用者帳號認證機制配合本會現有微軟 Windows Server 2003 Active Directory 目錄系統進行帳號認證作業，以確保使用者帳號之一致性，讓使用者不必再另外記憶一組帳號。

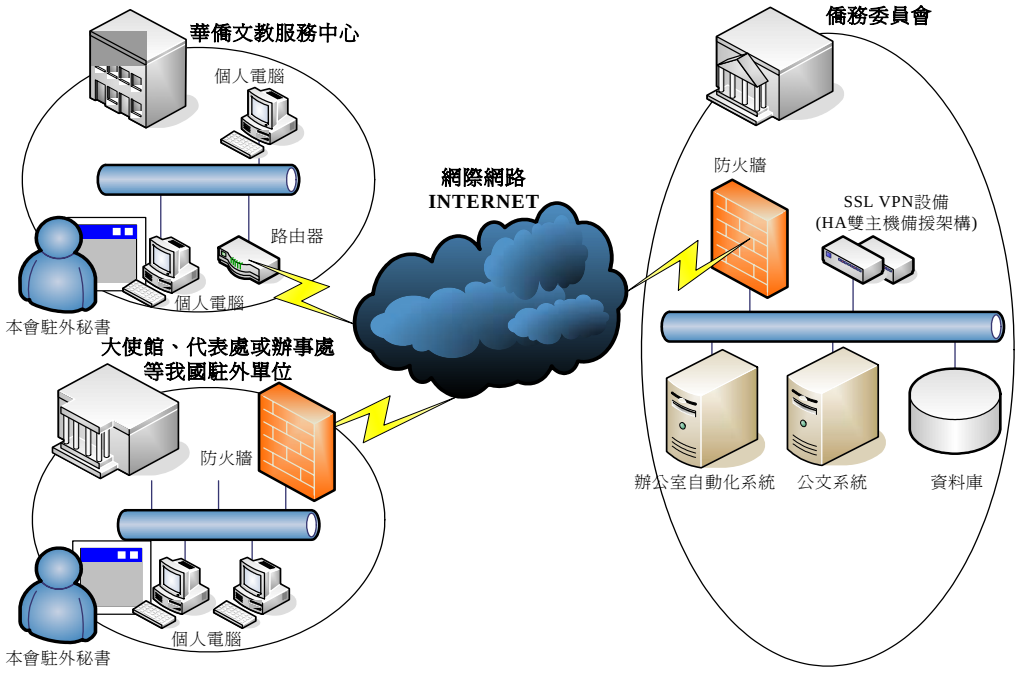
三、應用系統連線測試：於本系統設定登入成功之使用者可以使用本會各應用系統（如辦公室自動化系統、海外電子公文系統以及僑團情系統等），但是各應用系統內部各項子功能之使用權限仍由應用系統本身控管。

四、電子郵件系統測試：於本系統設定本會電子郵件系統連線及認證資料後進行測試作業，測試作業內容爲以本系統連線並收發電子郵件是否順利。

五、會內同仁實際上線測試：邀請本會資訊科同仁與部分駐外秘書實際利用本系統上線測試，以確認本系統可以於使用者實際使用環境正常運作。

測試結果各項功能均能符合本會需求，目前本系統已經通過驗收程序，正在與舊有 IPSec VPN 進行平行作業，預計將於 94 年 9 月 1 日正式全面改用 SSL VPN 網路通訊安全閘道系統。

參、系統架構



肆、效益

本系統啓用後之效益爲：

一、本會駐外秘書不必再爲原有 IPSec VPN 的眾多問題煩惱了，只要電腦可以正常上網，就可以使用 SSL VPN 連線至本會進行日常工作。

二、SSL VPN 之安全性遠遠優於 IPSec VPN，本會資訊人員不必再擔心可能來自 IPSec VPN 方面的資安威脅。

三、SSL VPN 之帳號認證作業可以和本會現有目錄系統整合，不必像 IPSec VPN 一樣必須另外維護一套帳號認證系統，大幅減少本會資訊人員的工作負擔。

伍、未來可能發展

一、建立本會同仁於第二辦公處所（或在家）上班支援機制：由於近年來國際間陸續發生禽流感、豬鍊球菌感染等傳染性高之疾病，世界各國正嚴陣以待，陸續加強本身防疫體系之完整以及採購相關藥物增加安全庫存以預防高危險傳染疾病再次橫行。爲預防類似 SARS 之疾病再度肆虐以致同仁出席率降低甚至無法上班，導致本會無法維持正常運作。因此未來可將 SSL VPN 使用者範圍陸續擴增至本會同仁，並自本會各單位選出種子學員參與測試計畫，以協助本會建立本會建立遠端作業機制及標準程序。

二、建立電腦機房設備遠端管理機制：以 SSL VPN 配合導入 IP based KVM 系統，可建立本會電腦機房設備遠端管理機制，以提供本會資訊人員可以 24 小時隨時查看並處理電腦機房之各項問題，並可保證連線過程資料的安全，防止未經授權者進入。

陸、結語：導入 SSL VPN 以後，對於本會各項工作之推動均有極大之幫助，確實達到以資訊科技加強本會服務工作之目的。

（本文由僑務委員會 提供）