TaiwanPlus 防火牆招標規範

一、 設備規格

A.每台防火牆規格如下: (共計採購兩台)

1.1. 具獨立主機採硬體式設備(Hardware Appliance)架構，並使用專屬作業系統。

1.2. 需提供佐證文件或測試數據，提供應用程式辨識與控制整體處理效能需達 2.9 Gbps。

1.3. 提供最大連線數可達 300,000 筆，每秒新增連線數可達 50,000 筆。

1.4. 具備 IPSec VPN 功能，加密演算法支援 3DES(Data Encryption Standard 與 AES(Advanced Encryption Standard) 128 位元、192 位元、256 位元，效能須達 2.1 Gbps。

1.5. 需具備 8 埠(含)以上 10/100/1000 乙太網路埠。

1.6. 支援動態路由功能 BGP, OSPFv2/v3, RIP, IGMPv1/v2/v3, PIM-SM, PIM-SSM 等路由協定。

1.7. 可擴充第二備援電源，提供 100–240 VAC 輸入電壓。

1.8. 提供 120GB 儲存容量。

1.9. 具備檢視原則規則使用狀況分析工具，以協助將以連接埠(L4)的規則轉移成以應用程式(L7)的規則。

1.10. 具備各版本設定檔檢測功能，對設定檔正式套用前進行檢測，並提供設定異動與差異性分析資訊。

1.11. 防火牆設備具備資安事件記錄儲存與關聯性分析功能，並能依照需要自訂報表，無須外掛任何報表軟體，即可製作報表提供分析之用。

1.12. 針對 SSL 加密連線資料進行資安檢測(包括使用 TLS 1.3 和 HTTP/2 通訊協定的流量)，亦可設定將解密後資料以複製(SSL Port Mirror)提交第三方系統進行稽核、存查等各種需求之分析。

1.13. 提供威脅防護功能包括入侵偵測防禦(IPS)、應用程式控制(APCL)、防毒(Anti-Virus)、防間諜程式(Anti-Spyware)，並能防止使用者與駭客中繼站(C&C)的連線行為，阻斷可疑連線但不影響正常網路運作，且效能全開須達 1.6 Gbps。

1.14. 惡意軟體防護需具備酬載式(Payload)偵測與串流式(Stream)偵測方式。

1.15. 提供超過 60 種良性及惡意內容類別，並可根據網站內容、功能和安全性分類。

1.16. 提供 URL 過濾使用雲端式內嵌機器學習分析實際的 Web 流量，並即時分類及封鎖各種惡意 URL。

1.17. 提供雲端沙箱功能，具自動偵測及防禦未知的惡意軟體威脅。

1.18. 提供 IPsec/SSL/無用戶端 VPN (Clientless VPN)，與支援行動裝置 VPN 的連線。
1.19. 提供 DNS Security 功能，透過雲端數據庫即時偵測進行 DNS 查詢。
1.20. 根據類別設定政策以進行封鎖、警示或 Sinkhole 處理，包括 C2、動態 DNS、惡意軟體、新註冊的網域、網路釣魚、灰色軟體、寄放網域、Proxy 規避。
1.21. 投標防火牆產品設備品牌須通過 NSS Labs NGFW 及 NSS Labs NGIPS 等國際第三方實測安全認證。

B.每台 L2 網路交換器規格如下：(共計採購兩台)

1.22. 具備 8 埠(含)以上 100M/1G BaseT 乙太網路埠。
1.23. 須提供三年(含)以上保固。

二、 其他

2.1 得標商負責所有與本案相關設備(包含本單位現有設備)的安裝設定。如有任何費用產生，由得標廠商支付。
2.2 本案所有新購之軟硬體產品須提供原廠或原廠授權代理商之新品證明。

三、 履約期限

3.1 立約商應於簽約日次日起 120 日曆天內完成交貨、安裝、測試並報請驗收。逾期每遲延一日，應分別按契約總價千分之一逐日計課逾期違約金，上限為契約總價百分之二十。
3.2 為兼顧採購時間彈性與製播持續營運，得標廠商須於得標後七個日曆天內，提供替代產品協助防護本會日常傳輸需求及資訊安全至本次採購設備上線防護為止。(目前對接端 TAIWANPLUS 使用 PA-850 機型，建議使用同樣機型確保傳輸穩定與快速切換佈署。)

四、 保固與維護

4.1 立約商於全案驗收合格日起保固三年。保固期間內免費負責標的物之維修、保養換件等維護工作及正常使用狀況下發生故障免費修理與更換非消耗性零組件。若標的物在保固期間內軟硬體有缺點(BUG)，立約商應負責維修或更新改善，並不得索取任何費用。
4.2 立約商應於驗收後提供原廠或原廠授權代理商連帶保固三年切結書。
4.3 本案自驗收合格日之次日起，立約商提供軟硬體三年 7*24 保固與維護，須於 2 小時內提供電話除錯服務，叫修後 4 小時內到府服務，如無法於 24 小時內修復完畢，立約商須無條件提供相容同等級以上之備品。

4.4 若立約商未依上述時限排除故障，又無替代故障設備之措施時，每逾一日按契約價金總額千分之二計算逾期違約金，本會得逕自保固保證金扣抵，並連續處罰至故障完全排除為止。

4.5 保固期間內系統有任何異常，包含硬體損壞與軟體不正常運作，立約商需提供免費維修及更換料件服務。

4.6 保固期內，倘公視基金會因業務需要，需進行設備關機、移機等工作，立約商應無條件派員技術配合處理，因異動產生之材料費用，由本會負擔。

4.7 除特別註明不同保固時間之項目外，立約商需在保固期間內提供免費負責標的物之維修、保養換件等之維護工作，及在正常操作情況下發生故障免費修理與更換零組件。若標的物在保固期間內軟硬體有缺點(BUG)，立約商應負責維修或更新改善，並不得索取任何費用。

4.8 全系統操作手冊廠商應不定期無償更新。

五、 驗收

5.1 原廠或原廠授權代理商之新品證明，如係進口貨應另附海關進口證明文件。

5.2 提供所有軟硬體設備 3 年之立約商保固與維護之保固切結書及原廠或原廠授權代理商保固證明書。該切結書及證明書必須隨附購案中各項電腦系統軟硬體之個別廠商證明文件作為附件。

5.3 依本會需求及本規範規定之手冊及電子檔。

六、 其他規範事項

6.1 得標廠商資格:

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件：

（一） 凡在政府機關登記合格，且不得為中國企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員不得為陸籍人士。

（二） 本案服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他經銷商執行。

6.2 業務保密安全責任:

（一） 得標廠商基於本案需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影（音）及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任，並簽定保密協議書。

（二） 得標廠商對特別以文字標示或口頭明示為機密資料者，非經本會書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，得標廠商應負完全責任。

（三） 得標廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由得標廠商自訂)。
（四） 契約終止時，得標廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本會或經本會同意後銷毀。
（五） 履約期間造成保密及安全事件，得歸咎於得標廠商之責任時，得標廠商應負所有法律及賠償責任。
（六） 本會對得標廠商保留實地稽核權，以確保得標廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

6.3 配合事項:

（一） 得標廠商須無償配合提供：本會災難演練、主管機關或行政院災防演習之遠端技術協助或諮詢服務。
（二） 需無償配合本會依 ISO 27001 之指定的第三方外部稽核或查核，進行實地或書面訪查作業，如有違反資通安全法規情事依合約條款處理，並不得續約。
（三） 廠商應遵守行政院所頒訂之各項資訊安全規範及標準，並遵守機關資訊安全管理及保密相關規定。此外機關保有對廠商執行稽核的權利。
（四） 廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。
（五） 廠商提供服務，如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。
（六） 基於法令及合約需求，本會得要求實施定期或不定期稽查，以監督專案內各項安全管理執行情形。
（七） 契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還之，並保留執行紀錄。

七、 教育訓練(免費提供):

設備安裝完成後，即可進行教育訓練，課程內容必須包括系統操作與維護，並於報請驗收前完成。立約商準備教育訓練計畫，並提供合格教師在指定之時間及地點進行教育訓練課程，課程至少 8 小時以上之專業訓練，並得視使用單位需要延長及增加梯次，立約商並不得另外要求收費。師資人員及其他相關衍生性之所有費用皆由立約商自行負擔。