高速核心防火牆
設備規格與需求

一、 核心防火牆＊2 台

每台規格如下:

1.1 提供 8 個(含)以上 10 Gigabit SFP+ Ethernet 埠。

1.2 提供與防火牆同廠牌 4 個(含)以上 QSFP+網路模組及與防火牆同廠牌 2 個(含)以上 40G QSFP+ GBIC。

1.3 提供 2 個(含)以上 1100 瓦電源供應器，具備熱抽取式功能。

1.4 防火牆效能：須達每秒 80Gbps(含)以上。

1.5 啟動防火牆及應用程式管控效能：須達每秒 27Gbps(含)以上。

1.6 啟動防火牆及應用程式管控及入侵防禦效能：須達每秒 26Gbps(含)以上。

1.7 硬體 TLS 解密效能：須達每秒 6.5 Gbps(含)以上。

1.8 提供入侵成功指標(IoC)，聚合相關威脅事件，如入侵事件或 CNC 連線行為等，供管理人員判讀。

1.9 提供進階威脅防護，檢測、阻擋、追蹤、分析和修復等功能，以保護免受持續的惡意軟體攻擊亦可整合與防火牆同廠牌端點防護。

1.10 提供雲端沙箱或與防火牆同廠牌沙箱硬體設備整合，傳送未知檔案與雜湊值進行檢測。

1.11 提供應用程式控制:包含應用程式、IP 地理位址、使用者、網站，可自定義應用程式和網址的檢測政策。

1.12 所有軟硬體提供五年原廠保固，次工作日人工零件到場標準保固，驗收後需開立原廠或原廠授權代理商五年保固證明書。

二、 防火牆虛擬化管理平台

每台(套)規格如下:

2.1 提供自動化入侵防禦政策調整和影響評估。

2.2 虛擬管理平台提供 10 台(含)以上同廠牌防火牆設備管理授權與最多 10,000,000(含)以上入侵防禦事件。

2.3 提供多項資安功能整合策略管理功能，在單一策略中設定防火牆存取、應用程序控制、威脅預防、進階惡意程式保護。

2.4 提供與防火牆同廠牌威脅情報，和支援從 STIX/TAXII 第三方威脅情報平台中提取和關聯威脅。

2.5 提供報表範本且可自定義報表格式，提供圖形化監控網路行為和硬體效能，來維運系統正常運作。

2.6 虛擬管理平台提供攻擊發生前、發生時、發生後，整個事件的統一管理。

A. 發生前:提供檢視網路中正在運行的應用程式，以便本會可以看到需要保護的內容。創建防火牆規則，並控制在本會的環境中使用超過 4000 種商業和自定義應用程式。

B. 發生時:定義入侵防禦級別，網址信譽規則和進階惡意軟體防護等級，甚至在必要時將可疑檔案發送到整合與防火牆同廠牌沙箱。

C. 發生後:產生攻擊感染的所有設備的圖形，輕鬆創建自定義規則以阻止攻擊進行的能力，對惡意軟體進行詳細分析，以安全地對其進行修復。

2.7 虛擬管理平台提供自動收集、整理和顯示有關網路環境中的威脅資訊、使用者名稱、應用程式、檔案傳輸方式、命令與控制能力的伺服器 IP address、服務主機(作業系統版本、應用程式版本、漏洞資訊)、端點設備資訊(網路設備、行動裝置、印表機、VoIP 電話)等資訊。

2.8 虛擬管理平台支援 API 整合。

A. 從虛擬管理平台將事件傳送到安全信息和事件管理（SIEM）解決方案。

B. 使用第三方數據(主動掃描的漏洞管理資料或操作系統資訊)增加防火牆虛擬管理平台資料庫。

C. 啟動由用戶定義的關聯規則的工作流程和修復步驟。

三、 其他

3.1 擴充本會現有 HP 交換器，須提供 4 個(含)以上 HPE 5930/5940 原廠 40GbE QSFP 埠(多模)。

3.2 本案須將資料做分流，multicast 流量與 unicast 流量分開，unicast 流量需經過本案採購的核心防火牆，且防火牆須為 HA 架構。

3.3 本案相關設備需與本單位現有的軌跡儲存系統整合。

3.4 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。

3.5 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。

3.6 本案為兩層式架構的第二層， 原第一層架構防火牆品牌為 Checkpoint，為了避免無意義的同品牌二次掃描，本案不可使用 Checkpoint 品牌之產品。

四、 履約期限

4.1 立約商應於簽約日次日起 270 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。

4.2 為兼顧採購時間彈性與營運安全，得標廠商須於得標後三個月內，提供替代產品協助防護本會資訊安全至本次採購設備上線防護為止。

五、 保固與維護

5.1 立約商於全案驗收合格日起保固五年。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。

5.2 立約商應於驗收後提供原廠或原廠授權代理商連帶保固五年切結書。

5.3 立約商需於報請驗收時，提供「保固維護計畫書」，並經由公視基金會核可。計劃內容須提供完整保固計畫，以附註條款及本招標規範中保固項目相關條文為主要內容。

5.4 本案自驗收合格日之次日起，立約商提供軟硬體五年 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。

5.5 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。

5.6 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。

5.7 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。

5.8 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。

5.9 全系統操作手冊廠商應不定期無償更新。

六、 規格審查合格標準

為確保公視基金會權益，本案採二階段進行：

6.1 第一階段為書面審查，投標廠商須將符合招標規範擬採用之設備填入規格審查表，並依各項設備所列之規格逐條答覆，且須檢附相關佐證資料(產品型錄、技術手冊及原廠之相關技術文件)，並劃線標示對應之規格項目編號，俾利公視基金會審查。審查結果有一項不合格，即為不合格標，廠商不得參加次一階段之實機測試。

6.2 第二階段為實機測試，為確保投標廠商所提供之設備能完全符合公視基金會未來的應用與運作需求，投標廠商須提供本次投標之設備，依公視基金會所定之測試計畫書(附件一)項目於規定時間內完成相關測試，任何項目測試不合格及等同規格未合格，不得參予價格標開標程序。

七、 驗收

立約商應於測試合格後依據契約規範規定提供下列文件及經本會核准之測試計畫書向本會申請報驗：

7.1 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。

7.2 提供所有軟硬體設備 5 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。

7.3 依本會需求及本規範規定之手冊及電子檔。

八、 其他規範事項

8.1 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，並於服務建議書專章詳述：

（一） 凡在政府機關登記合格，且不得為陸資企業(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。

8.2 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。

8.3 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。

8.4 交付與時程:

（一） 投標時須檢附設備建置建議書「設備建置建議書」供審查。

（二） 得標後二個月內交付「工作計畫書」，工作計畫書應以得標廠商投標時之「設備建置建議書」為基礎，並依本會需求作修改。內容除包括對本專案之執行敘述，含專案管理、組織、人力、工作項目、時程說明及品質管理流程。

8.5　建議書製作規定:

A. 服務建議書格式

（一）　紙張:宜用 A4 規格

（二）　繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面及目錄，封面上註明投標廠商名稱、投標廠商地址、本案名稱及日期，裝訂線在左側。

（三）　目次：應標示各章節之出處頁碼。

（四）　投標廠商投標建議書之份數為一式三份。

B.　服務建議書內容

（一）　專案概述

1. 專案名稱
2. 專案目標
3. 專案時程

（二）　投標廠商說明

1. 投標廠商簡介
2. 公司營運狀況，包含參與人員名單、能力證明及投標廠商經驗說明。

（三）　專案工作規劃

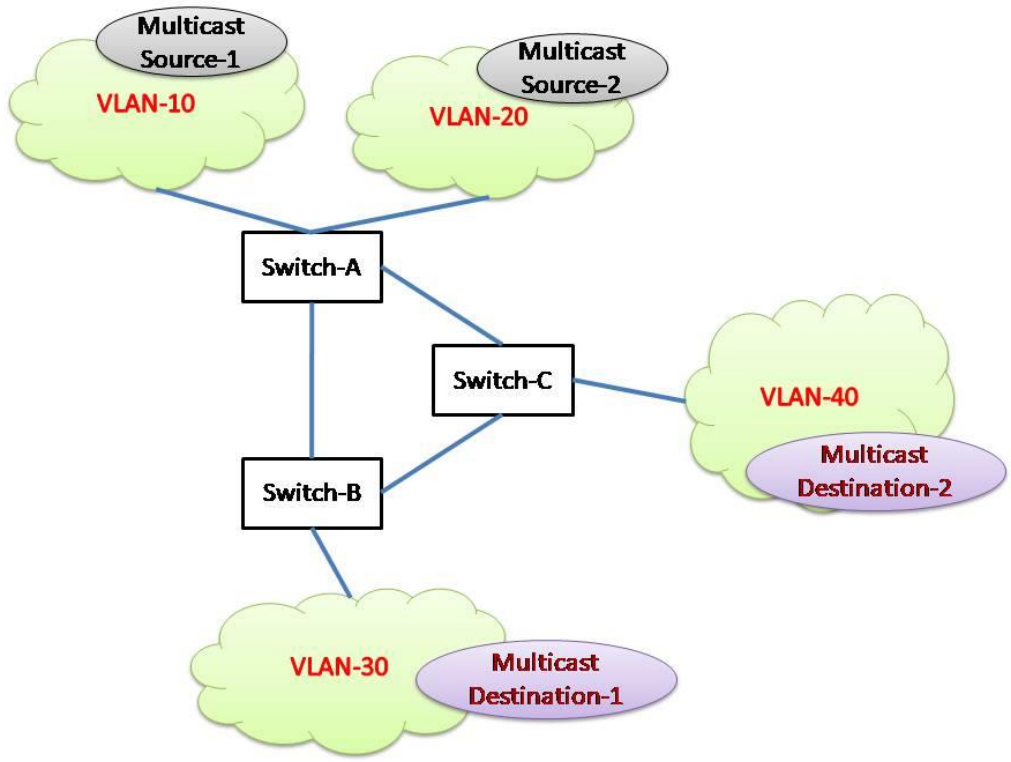
（四）　專案組織與管理

1.　人力配置、資格及管理
2.　專案時程規劃
3.　專案管理規劃
4.　交付文件項目

8.6　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，並於報請驗收日起 30 個日曆天內完成。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。

附件一 測試計畫書



■ LAB 環境描述：(如上圖)

- 4 個不同的 VLAN，分別串接到 3 台 switch
- VLAN-10 & VLAN-20 內有 multicast source(產生器)；VLAN-30 & VLAN-40 內有 multicast destination(接收器)

■ LAB 測試說明：

所有 LAB 設備(switch & multicast 設備)由廠商自行準備，唯 switch 設備須為本會現有使用廠牌型號(HP 5130)。

1. Multicast Source-1 的 multicast 流量(資料)，可以同時傳送到 Multicast Destination-1 & Multicast Destination-2。
2. VLAN-10 的 Multicast Source-1 的 multicast 封包直接從 Switch-A 走到 Switch-B 的 VLAN-30，(同時)且 Multicast Source-1 的 unicast 封包從 Switch-A 走到 Switch-C 再走到 Switch-B 的 VLAN-30。
   (同時)且 Multicast Source-2 的 multicast & unicast 封包直接從 Switch-A 走到 Switch-B 的 VLAN-30。

■ 測試項目及結果：

第 1 題: 可以在 2 個 multicast destination 看到 multicast source 傳送出來的資料(畫面, 影像, 聲音.....)。本會將會以工程部提供之專業影像觀測設備進行驗證，執行中該影像觀測設備之畫面不能發生 LAG 或出現錯誤警訊，否則將判定不合格。(若有疑慮部分將由本會專業影像工程人員判定，廠商不得有異議。)

□合格　　□不合格　　備註:

第 2 題:

在 switch 做一個 mirror port, 透過 sniffer 這類的軟體, 觀看下列條件是否全部符合。須全部符合才算合格。

Switch-C 應該如下:

1. 可以看到 VLAN-10 的 unicast traffic

□合格　　□不合格　　備註:

2. 不可以看到 VLAN-10 的 multicast traffic

□合格　　□不合格　　備註:

3. 不可以看到 VLAN-20 的 unicast traffic

□合格　　□不合格　　備註:

4. 不可以看到 VLAN-20 的 multicast traffic

□合格　　□不合格　　備註:

Switch-B 應該如下:

1.可以看到 VLAN-10 & VLAN-20 所有 traffic(包含 unicast & multicast)

□合格　　□不合格　　備註: