防火牆服務採購規範

一、服務介紹

防火牆服務由立約服務供應商提供一部(Unified threat management, UTM)整合式威脅管理網路防火牆設備，協助政府機關建置該設備、更新防禦情資、維護防火牆設備並進行該設備資安政策管理，於網路閘道內提供：防火牆、VPN、入侵偵測與防禦(Intrusion Detection and Prevention，IDS/IPS)等資訊安全防護功能。另提供威脅告警與定期產生服務記錄報表，提供給政府機關作為網路資訊安全的管理依據。

政府機關可根據連外頻寬與網路處理流量需求，選擇所需要的網路整體處理效能，包含：300Mbps、500Mbps 與 1Gbps 的不同等級之防火牆服務。

二、服務說明

1. 服務範圍

本項目服務標的為服務供應商所建置之網路防火牆設備，提供一次到場安裝服務與每年一次到場計劃性維護服務，日常服務作業將以遠端進行設定、防禦情資更新、系統更新、防火牆政策管理與設備維護等作業事項。

本服務自供應商完成網路防火牆設備建置後，提供 36 個月的維運服務，服務期滿供應商應於 1 個月內將設備取回，逾期機關得自行處置前開設備。

2. 現行網路架構檢視

針對機關提供的網路架構圖進行安全性弱點檢視，依據網路架構安全設計、備援機制設計、網路設備管理、伺服器主機設備、網路存取管控、IP 網段配置、既有防火牆政策(Policy Rules)與開啟通訊埠位(Port)等資訊，檢視網路拓樸設計邏輯是否合宜、主機網路位置及通訊埠位是否適當及現有防護政策是否足夠等，用以設定新部署之網路防火牆政策。

3. 網路防火牆部署

立約商應於政府機關訂購單通知之次工作日起算 30 個日曆天內，檢視政府機關現有網路架構與環境需求，提出網路防火牆設備部署建議報告，並與機關協調設備部署時間。部署工作應包含：網路防火牆設備安裝、網段部署設定、防火牆政策設定與系統調校及導入等工作。

若機關若有調整網路防火牆設備部署之需求，最多每年不得超過 1 次，並列

入到場計劃性維護服務之中，機關若超過計劃性維護服務的部分，則不屬本服務範圍。

4. 網路防火牆維護

(1) 網路防火牆系統更新

依據防火牆設備原廠提供之新版系統軟體或韌體時程，與機關協調設備系統更新之計劃性維護作業時間，並彙整記錄於每月服務報告。

(2) 防禦情資資料庫更新

立約商應於服務期間提供防火牆設備原廠的防禦情資使用授權，並依據設備原廠提供之最新防禦情資，定期更新防禦資料庫與設備設定，並彙整記錄於每月服務報告。

(3) 防火牆政策維護與管理

依據以下作業需求：

(a) 防火牆告警與威脅

(b) 機關使用的 IP 網段或伺服器主機 IP 位置等政策異動

(c) 機關的資安威脅預警

由立約商配合提出計劃性維護作業與進行防火牆政策更新與事件處理等作業，並彙整記錄於每月服務報告。

5. 防火牆告警與事件處理

立約商針對防火牆偵測的資安威脅與告警，進行事件處理或防火牆政策調整，並彙整記錄於每月服務報告。

6. 服務監控

提供每月網路防火牆服務監控報告，提供報告內容需包含以下項目：

(1) 網路流量統計記錄

(2) 網路資安威脅統計記錄

(3) 網路資安告警記錄

7. 服務要求

維護時間應於使用機關之辦公日（依行政院人事行政總處公布之上班日為準）每日上午 8 時 30 分至下午 5 時 30 分，不含例假日。

立約商應於接獲使用機關電話、傳真或書面維護作業需求後，於 2 小時以電話、Email、簡訊或其他書面方式回覆機關維護作業計劃，並於 1 個工作

天以內完成系統更新與防火牆政策管理維護作業，如需配合機關日常業務進行，另外約定之維護計畫作業時間則不在此限制內。

全年設備故障次數、總時間與搶救時限要求,全年故障次數不可超過 5 次，故障總時間不可超過 104 小時，每次須於 1 個工作天內完成修復，唯計劃性維護作業不列入故障總時間及次數之中。

政府機關或廠商因天災或事變等不可抗力或不可歸責於契約當事人之事由，致未能依時履約者，得展延履約期限。

三、網路防火牆功能規格

本服務需具備防火牆政策管理、IDS/IPS 入侵偵測與防禦、IPSec VPN、SSL VPN、雲端沙箱、不當網頁過濾與應用程式控管及韌體更新服務等功能，部署設備需符合以下規格：

1. 防火牆防護能力需通過第三方資訊安全機構防火牆檢測認證如 NSS Labs 、 ICSA Labs 等。
2. 網路防火牆防護效能
   (1) UTM 整合式威脅管理處理流量可達 300 Mbps。
   (2) UTM 整合式威脅管理處理流量可達 500 Mbps。
   (3) UTM 整合式威脅管理處理流量可達 1Gbps。
3. VPN 效能
   (1) 1Gbps 之防火牆服務具備可同時建立 32 條 VPN 連線。
   (2) 500Mbps 之防火牆服務具備可同時建立 16 條 VPN 連線。
4. 網路防火牆具備 2 個以上 10/100/1000 自動偵測超高速乙太網路介面的 WAN 埠介面，以及內建 4 個以上 10/100/1000 自動偵測超高速乙太網路介面，每埠可自行定義為 LAN 或 DMZ。
5. 支援多個不同安全網域（Security Zone），不同安全網域網段連通，需經防火牆政策（Firewall Policy）控管。
6. 支援 IDS/IPS 入侵偵測與防禦、Anti-Virus 網路防毒、Content Filtering 異常網頁過濾、與應用程式控管等資安防護功能。
7. 支援雲端智慧沙箱服務，協助模擬分析未知威脅，找出惡意程式與病毒特徵碼，提升零時差攻擊防禦能力減少資安攻擊事件。
8. 支援 IPSec VPN、SSL VPN，並符合 SHA-2（512-bit）標準之封包認證功能與 3DES 及 AES（256-bit）之加、解密演算標準。
9. 具備使用者認證功能（User Authentication）
10. 支援 IPv4 與 IPv6 網路路由功能。

11. 具備雙韌體映像檔（Dual Firmware Image）。

12. 支援標準 19 吋機架安裝設計。

13. 符合 FCC Part 15（Class A）、CE EMC（Class A）及 BSMI 安規及電磁檢測標準。

四、廠商應配合事項及交付項目

1、網路防火牆部署建議報告

如服務說明要求

2、每月提供網路防火牆服務報告，至少包含：

(1) 摘要說明
(2) 執行情形
如服務說明要求。
(3) 執行建議
針對各項服務內容，提出改善建議
(4) 結論。

五、服務人員資格

參與網路防火牆服務人員應具備資訊網路、防火牆系統之維護技能，以確保服務水準。需求技能條件說明如下：

1、網路管理：接受過 CCNA (Cisco Certified Network Associate) 或其他類似網路管理相關課程訓練證明。

2、防火牆維護：具備防火牆設備原廠認證資格，以確保立約廠商具有網路資安與防火牆維護服務之能力。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關同意後始得服務。

服務人員需年滿 18 歲以上，身體健康無法定傳染病，體能符合適用機關資安服務工作需求，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。

六、機關配合事項

1. 機關須配合提供既有網路拓樸架構、使用 IP 網段、伺服器主機位置、VLAN 資訊及網路建置所必須資訊，並安排相關人員受訪確認機關網路環境。

2. 提供群組原則(Group Policy)、既有防火牆政策(Policy Rule)與開啟通訊埠(Port)的資訊，以供服務廠商設定建置防火牆政策維護。

3. 機關須提供適當環境配合安裝建置網路防火牆設備。

4. 機關如欲集中納管設備系統日誌，政府機關必須提供集中管理的日誌伺服器(Syslog Server)相關設定資訊，由服務廠商設定網路防火牆的日誌管理伺服器。