

全國農業金庫股份有限公司

111年度網頁應用程式防火牆規格及特別條款

全國農業金庫股份有限公司(以下稱本公司)採購網頁應用程式防火牆(以下稱本案設備)1臺,其規格及特別條款規定如下:

甲、規格

壹、一般規定

- 一、得標廠商應檢具原廠(含在臺分公司)之合法授權代理或經銷證明文件,並於驗收時提供原廠(含在臺分公司)之原廠連帶保固保證書。
- 二、得標廠商需提供本案設備網路佈線工程。
- 三、投標廠商應按投標金額 5%之現金、金融機構簽發之本票或支票、銀行保付支票、郵政匯票繳納押標金,得標後押標金轉為履約保證金,履約保證金經履約完成無待解決事項後轉為保固保證金,保固期滿且無待解決事項後無息發還保固保證金,未得標者無息退還。
- 四、得標廠商應提供 2022 年 1 月 1 日(含)以後製造之新品。
- 五、規格稱"以上"、"以下"、"以內"、"至少"、"高於"、"低於" 俱含本數。

貳、設備規格

一、網頁應用程式防火牆(Imperva X2520)

- 1、網頁應用程式防火牆閘道器支援之處理效能(System Throughput)需可具備處理第七層 http 500Mbps(含)以上，為硬體式獨立主機(Hardware Appliance)架構，並使用嵌入式或專屬作業系統。
- 2、為確保設備斷電及故障時網路流量仍可通過，不影響網站服務的正常運作，內建網卡需具備 bypass(fail-open)功能，不需依賴外部模組達到 Bypass，以防止單點失效影響 Web 服務。
- 3、網頁應用程式防火牆閘道器具備雙電源、雙硬碟備援機制。
- 4、設備需提供 SSL 硬體加速
- 5、設備需支援以 L2 Inline Bridge、Transparent Reverse Proxy、Reverse Proxy 及 Sniffing(Mirror)模式佈署。
- 6、使用 layer 2 透通式(Inline bridge)和 Transparent Reverse Proxy 佈署模式，不需於設備 Web 流量通過之網路埠設定 IP，也不需於設備內設定 VLAN 即可達到此需求，須提供 2 組(含)以上實體網路橋接區段(bridge segment)，區段內皆不需設定 IP 以防止設備遭受攻擊。
- 7、可針對 OWASP Top 10 攻擊事件提供防禦與偵測。
- 8、具備網站行為自動學習功能，自動學習 URL、Cookie、Parameter name、Parameter type、Parameter value length、網頁使用者帳號、Session 及 HTTP Method，提供正面列表防禦機制(Profile)，並支援 Virtual Host 虛擬主機功能，學習之結果可由管理者手動調整與手動切換學習模式或防護模式，且也可以目錄為單位鎖定(lock)該學習功能。
- 9、須可針對多網段、IP 範圍進行排程掃描是否有主機具備 HTTP、HTTPS 服務，並可針對掃描探測結果，將具備針對掃描探測結果，將具備 HTTP、HTTPS 服務之 IP 自動產生保護網站列表進行防護。
- 10、阻斷方式可設定針對攻擊來源之 Session、User Name 或 Source IP，且可定義欲阻擋該攻擊來源 Session、User Name 或 Source IP 的時間(秒)。
- 11、設備需提供自動更新功能(可設定排程每日、每週或每月執行)，其更新內容需包括政策定義、特徵碼、報表範本。
- 12、提供設備 1 年保固。

二、網頁應用程式防火牆管理系統(IMPERVA SecureSphere VM150)

- 1、提供 CLI (Command Line Interface)、SSH 命令列管理介面與 Web 管理介面。
- 2、支援多重管理者機制，可以依據不同的管理者角色給予不同的權限及管理設備範圍。
- 3、須提供事件管理中心介面，讓管理者查詢即時監控之訊息，並提供篩選功能，定義呈現之範圍及條件。
- 4、系統告警功能提供異常行為及完整過程訊息分析功能，包含來源 IP、發生時間、目的端 IP、事件描述(Alert Description)、事件內容(Details)等資訊，並可進行條件過濾(filter)。
- 5、提供告警事件收斂彙整管理技術，將類似之事件集中為一項，以減少管理者之負擔。
- 6、系統告警(Alert)資訊可透過 email、SNMP、OS Command 及 Syslog 等機制通知相關管理者或第三方系統。
- 7、提供 Web 介面，可同時管理多部閘道器設備，統一管理各閘道器之事件訊息與運作狀態。
- 8、Web 管理介面需以 HTTPS 方式加密連線。
- 9、可集中管理所有被監控目標之設定、政策、報表，並可自動派送至各閘道器設備。
- 10、須提供管理者作業之工作稽核記錄(System Event)，包括管理者登入/登出、修改設定、產製/修改報表等工作記錄，且管理者本身無法對此記錄做任何修改。為安全考量，須提供密碼強度限制的相關設定，如密碼長度、是否需大小寫混合、有效期限…等。
- 11、所有 log 及稽核資料須能備份匯出，並可支援多種匯出方式：FTP、HTTP file transfer、NFS、Mount file system、SCP…etc.。匯出的資料須提供加密或驗證技術。
- 12、需提供 NTP 校時功能，可與上層時間伺服器對時，確保事件時間準確性。
- 13、具備特徵碼更新機制，可立即生效不影響系統運作，並可派送至各閘道器。
- 14、具備自動隱藏或移除告警、報表中敏感性資料之功能，使用者可自訂敏感性資料欄位或物件。
- 15、需具備原廠更新（可設定排程每日、每週或每月執行）特徵碼機制，

無需手動介入操作即可自動更新。

- 16、需具備手動更新機制，防止因資安政策無法使本系統對外連線時，可手動更新特徵碼。
- 17、原廠提供更新之內容，包括政策定義、特徵碼、報表範本、資料庫弱點掃描項目。
- 18、需可提供惡意 IP 情資資料庫，並定期自動更新。
- 19、須內建報表系統，可正常顯示中文，所有報表產出都可在設備內獨立完成，不需另行匯出資料至其他的報表模組以產生報表。
- 20、可依使用者需求自行調整報表格式（可自行新增或刪除顯示於報表之欄位及設定報表產出之條件），可調整欄位顯示順序，並可設定第一排序(sorting)欄位及第二排序欄位，以產出符合使用者需求之報表。
- 21、可設定報表以一次性產出、或週期性(每日、每週、每月或可設定每多少分鐘)產出，並可設定報表產出後自動以 Email 方式寄送給相關管理者。
- 22、產出之報表格式可以選擇匯出為 Acrobat Format (PDF)、Comma Separated Values (CSV)等格式。
- 23、須具備符合 SOX、PCI、HIPPA、ISO27001 規範的報表。
- 24、政策、白名單、黑名單、報表等設定，需可排程自動備份轉存。
- 25、提供管理系統 1 年訂閱授權。

乙、特別條款

壹、本案設備之維護工作應由得標廠商承擔，若得標廠商非為設備供應商，須於簽約前取得設備供應商或其在臺分公司之書面承諾，支援硬體的維護工作。

貳、得標廠商對於本案系統同意履行以下 14 款情事：

- 一、得標廠商提供本公司使用之本案系統，如有第三者主張得標廠商所提供本公司使用之本案系統有侵犯專利權或著作權時，本公司同意儘速以書面通知得標廠商，得標廠商應負責為本公司提出抗辯或和解談判，所有經法院判決確定或成立和解應由本公司負擔之費用、損害賠償及本公司因此所支付之費用（含委聘律師酬金）、所受之損害等均由得標廠商負擔。
- 二、得標廠商應訂定其聘僱人員之相關管理規定，並將維護（修）人員名冊（含簽章）函送本公司備查，且對其操守行為負責，如有異動時亦同。
- 三、得標廠商因履行契約應辦事項所知悉一切有關本公司及本公司客戶之相關資料及內容，應採取必要之安全措施，得標廠商及其員工均應保守秘密不得洩漏，否則如致本公司遭受損害應由得標廠商負賠償責任；契約終止時亦同。
- 四、得標廠商因履行契約應辦事項所應負之損害賠償責任以直接實際損害為限，且以契約總價款為賠償上限。但有關人身傷害（包含死亡）、物之毀損、專利權及著作權之損害、得標廠商之故意或重大過失造成之損害賠償則不在此限。
- 五、得標廠商同意金融監督管理委員會、中央銀行、中央存款保險公司、行政院農業委員會農業金融局或依農業金融法第7條規定之機關及本公司得取得契約應辦事項相關資料或報告，及進行金融檢查或稽核，或得要求其於期限內提供相關資料或報告。
- 六、得標廠商履行契約不得違反法令強制或禁止規定、公共秩序及善良風俗，對本公司經營、管理及客戶權益，不得有不利之影響，並應遵守農業金融法、銀行法、洗錢防制法、個人資料保護法、消費者保護法、中華民國銀行商業同業公會全國聯合會訂定之相關業務規章或自律公約及其他法令之規定。
- 七、得標廠商應依本公司同意之標準作業程序，執行消費者權益保障、風

險管理、內部控制及內部稽核制度。契約如有履行不能、履行困難或履行困難之虞者，得標廠商應即通知本公司。

八、得標廠商若有違反契約約定情事發生，除契約另有約定外，本公司得於通知得標廠商後終止或解除契約。本公司於主管機關命為終止或解除契約時亦同。

九、得標廠商履行契約應辦事項，對外不得以本公司名義為之，亦不得進行不實廣告。

十、得標廠商應建立消費者爭端解決機制，包含解決時程、程序及補救措施。

十一、得標廠商非經本公司事先書面同意，不得將契約應辦事項複委託。

十二、得標廠商對契約應辦事項若有重大異常或缺失應立即通知本公司。

十三、得標廠商不得於本公司提供之設備上做任何不當作業之行為及植入非法或足以損害正常作業與保密之功能，否則如致本公司遭受損害，應由得標廠商負賠償責任，於維護期間受委託機構須配合本公司定期資安檢測作業(如弱點掃描)，所檢測出之風險弱點項目，應配合本公司要求於期限內進行修正完成，本公司不另行付費。

十四、得標廠商須符合本公司現有各項系統管理作業規定及安全管理規範。

參、報價

一、得標廠商以新臺幣為報價基礎，且分別依下表列出價格：

單位：元

項次	名稱	數量	單價	金額
1	Imperva X2520	1	000	000
2	IMPERVA SecureSphere VM150 Management(訂閱制 1年)	1	000	000
合 計				000

*以上報價應依規格內容報價(含稅)。

肆、交貨、安裝及測試

一、得標廠商須於簽約次日起 4 個月內將本案設備於本公司指定地點完成交貨、安裝、測試並提出經本公司簽認之測試報告，如逾所訂期限，

得標廠商應依照下列公式計付違約金予本公司：

$$\text{違約金} = \text{契約總價款} \times 0.1 \% \times \text{逾期日數}$$

- 二、上述作業，如逾期超過 30 天仍未完成時，除仍應依前述規定計付違約金外，本公司得通知解除契約，並沒入履約保證金。上述逾期違約金之累計總額以契約總價款之 20% 為上限。

伍、驗收及付款

- 一、得標廠商於本公司指定地點完成交貨、安裝、測試，由本公司派員辦理驗收，驗收合格後，支付契約總價款。
- 二、得標廠商須提供設定操作手冊(書面及電子檔)及教育訓練計畫(書面電子檔)，並於驗收時一併交付。
- 三、得標廠商須提供原廠(含在臺分公司)之原廠連帶保固保證書。

陸、維護及保固

- 一、得標廠商必須提供本案設備之技術工程師週一至週五上班日待命維修之服務，以維護本案設備之正常運作，如於非上班日遇有硬體損壞需更換零件之情事，則最遲須於次一上班日完成維修恢復運作。
- 二、得標廠商對於本案設備，維護及保固應至少包含下列事項：
 - 1、提供必要之檢查、清潔、調整或更換零件等預防保養服務，以維持本案設備之正常運作功能。
 - 2、本公司發現本案設備故障時應通知得標廠商進行檢修，得標廠商維護人員應於收到通知後 4 小時內（含交通時間）到達現場。
 - 3、為檢修之必要，得暫以同類型設備無償提供本公司代用。於此情形，該本案設備視為已回復正常運作。惟得標廠商仍應於 3 日內將本案設備回復正常運作或更換功能不低於本案設備之備品。
 - 4、得標廠商應負責本案設備之韌體，需依本公司要求更新至最新版本。
 - 5、得標廠商應負責本案硬體問題排除及技術支援。

三、得標廠商對於本案設備，於本案完成全案正式驗收之次日起，負責維護及保固 1 年。保固期滿後，本公司得視實際需要與得標廠商簽訂維護契約，其每年設備硬體維護費率如下：

- 1、項次一：「Imperva X2520」每年維護費率為該項次契約總價款 8%。
- 2、項次二：「IMPERVA SecureSphere VM150 Management」為訂閱制項目，保固期滿後，依該項次契約單價每年訂閱。
- 3、以上兩項得標廠商不得拒絕簽約。若本公司要求簽訂維護契約而得標廠商未於保固期間屆滿前與本公司簽訂維護契約，則保固期間自動延長至維護契約生效日止。

柒、技術移轉

得標廠商應免費提供與本案相關技術移轉及教育訓練課程：

教育訓練課程時數至少 4 小時以上

捌、得標廠商應對本案契約內容充分瞭解，並依本公司之解釋切實執行辦理。