電信技術規範
檢驗規範

資通安全 0012 (IS0012-0)
訂定日期 101 年 2 月 29 日
通傳技字第 10043040220 號

網頁應用防火牆
資通安全檢測技術規範

技術規範(草案)

國家通訊傳播委員會
中華民國101年2月

目　次

圖　次

表　次

附　件

網頁應用防火牆資通安全檢測技術規範

1. 概說

網頁應用防火牆 (Web Application Firewall, WAF)，用於保護伺服器端之網頁應用程式，避免遭受網際網路各種惡意攻擊。

2. 適用範圍

本規範適用於獨立式硬體架構，並使用嵌入式韌體或專屬軟體之防火牆，可掃描、阻擋或過濾網路應用層通訊協定之網頁應用攻擊。

3. 安全等級

本規範之設備安全等級分為基礎型 (Basic) 與進階型 (Advanced)。

基礎型網頁應用防火牆

基礎型設備安全功能測試項目包括異常/攻擊偵測、網頁應用程式迴避攻擊抵禦、安全事件紀錄及安全管理；壓力測試項目包括吞吐量；堅實測試項目包括阻斷式攻擊及非正常關機復原；穩定測試項目包括真實流量長時間測試。

進階型網頁應用防火牆

進階型設備除基礎型設備之測試項目外，另增加安全功能測試項目包括備援管理；壓力測試項目包括最大同時連線數及最大建立連線速率；堅實測試項目包括異常流量；穩定測試項目包括真實流量長時間測試。

4. 參考標準

ISO/IEC 15408 共同準則 (Common Criteria for Information Technology Security Evaluation, CC)
ICSA Web Application Firewall Certification Criteria
NSS Web Application Firewall Certification Methodology

5. 用語釋義

共同準則 (Common Criteria, CC)

為國際資通安全產品評估及驗證之標準 (ISO/IEC 15408)，依其定義之評估保證等級 (Evaluation Assurance Level，簡稱 EAL) 判定產品之安全等級，EAL 共有 7 個等級，最低等級為 EAL 1，最高等級為 EAL 7，提供申請者/贊助者、檢測實驗室與驗證機關 (構) 評估及驗證資通安全產品安全與功能性。參考網址 http://www.commoncriteriaportal.org

評估標的 (Target of Evaluation, TOE)

指申請資通安全評估及驗證之產品及其相關使用手冊。

保護剖繪(Protection Profile, PP)

指滿足資通安全產品評估標的 (TOE) 製作之安全基本需求文件。

安全標的 (Security Target, ST)

指資通安全產品能符合保護剖繪 (PP) 或特定安全需求製作之規格文件。

安全功能 (TOE Security Functions, TSF)

指資通安全產品用於實現安全標的 (ST) 所要求安全功能需求 (Security Functional Requirement, SFR) 之相關功能。

安全功能需求 (Security Functional Requirement, SFR)

指共同準則第二部份 (Common Criteria, Part 2) 所定義之安全相關需求條文，用以描述一資通安全產品之安全功能 (TSF) 所需滿足的各項要求。此要求條文會被引用於保護剖繪及安全標的中，用以具體陳述該產品功能的安全方面的需求。

角色 (Role)

指預先定義之規則，以描述使用者與待測物間的操作權限。

5.1. 指引文件 (Guidance Documentation)

指描述待測物之遞送、安裝、運作、管理及使用等相關文件。

5.2. 安全功能介面 (TOE Security Functions Interface, TSFI)

為評估標的 (TOE) 用於實現安全功能需求 (SFR) 之對外溝通介面。

安全領域 (Security Domain)

指一個主動式個體 (人或機器) 被授權存取的資源集合，為安全架構的屬性之一。

自我保護 (Self-Protection)

指安全功能本身無法被無關的程式碼或設施破壞，為安全架構的屬性之一。

防止繞道 (Non-Bypassibility)

指防止避開待測物安全功能檢查之技巧。(如：未經過身分鑑別，無法進入稽核功能介面)。

最大同時連線數

指待測物能同時處理之 TCP 連線數最大值。

5.3. 吞吐量 (Throughput)

指待測物處理網路流量的速度，通常的表示法為「Mbps」（每秒一百萬位元）或「Gbps」（每秒十億位元）。

最大連線建立速度

指待測物能處理的 TCP 連線建立速度，通常的表示法為「TCP 連線數/每秒」。

緩衝區溢位攻擊 (Buffer Overflow)

指惡意使用者利用程式設計漏洞，輸入超過預定長度的字串，以任意的語法插入程式碼中，造成緩衝區溢位，可能使程式異常停止、執行任意程式碼或取得系統權限等影響。

資料隱碼攻擊 (Injection)

指惡意使用者利用網頁應用程式執行外部程式或指令，如資料庫的語法或作業系統相關的指令；來進行新增、刪除或修改的動作，進而控制整個網頁應用程式。目前常見的攻擊手段主要是以 SQL 資料隱碼攻擊為主。

跨站腳本攻擊 (Cross-Site Scripting)

指惡意使用者利用網頁應用程式的安全漏洞，將惡意程式碼注入到網頁(如：HTML 或 Javascript 等)上，使網頁瀏覽者下載或執行惡意程式碼。可能造成竊取資訊塊 (Cookie)、影響網頁瀏覽或竊取個人資訊等。

破解認證機制 (Broken Authentication and Session Management)

指惡意使用者竊取合法使用者的資訊塊或竊聽其帳號密碼等封包資料，來破解網站的身分認證機制。

網頁程式參數竄改 (Parameter Tampering)

指惡意使用者利用網站處理使用者輸入的漏洞，傳送網頁非法的參數值，以提升操作權限或取得機密資料。

隱藏欄位竄改 (Hidden Field Tampering)

指惡意使用者竄改 HTTP Request 隱藏參數欄位的值，以改變網頁內容。(如：修改拍賣網站的商品價錢，以低價購入該商品。)

資訊塊中毒 (Cookie Poisoning)

指惡意使用者修改資訊塊獲得用戶未授權的資訊，以盜取用戶身份，進而取得該用戶帳號的權限。

無效請求 (Invalid Request)

指伺服器無法辨認 HTTP 請求時，會回傳「無效請求」，一般發生於用戶端送出的 HTTP 請求格式不符合要求。

強迫瀏覽攻擊 (Forceful Browsing)

指以窮舉法 (Exhaustive Search) 來產生不同的網址，存取不允許被瀏覽的伺服器端網頁或資料。

資訊洩漏 (Information Leakage)

網頁應用程式設計不良，致無意中洩漏機密資訊，使得惡意使用者可收集相關資訊。

傳輸層保護不足 (Insufficient Transport Layer Protection)

未使用安全的傳輸層通訊協定 (TLS/SSL) 或加密金鑰強度不足。

HTTP 阻斷服務攻擊 (HTTP Denial of Service)

指惡意使用者利用 HTTP 協定之攻擊程式，持續且大量對網頁伺服器要求建立連線，造成伺服器無法正常提供服務或降低效能。

網址編碼 (URL Encoding) 逃脫技巧

依 RFC 1738 規定，URL 由 ASCII 字元所組成，如欲使用其他字元，則須編碼成「%xx」的格式，其中 xx 代表兩個 16 進位數字，如「空白」會編碼成「%20」。惡意使用者可利用 URL 編碼逃脫技巧，以躲避網頁應用防火牆之偵測，如「cgi-bin」與「%63%67%69%2d%62%69%6e」於 URL 表示法中語意相同，但網頁應用防火牆可能因字串不同而無法正確偵測。

雙斜線 (Double Slashes) 逃脫技巧

URL 表示法中，連續的「/」只會被視為單一「/」。惡意使用者可利用多個「/」躲避網頁應用防火牆之偵測，如「//cgi-bin//xxx.cgi」與「/cgi-bin/xxx.cgi」於 URL 表示法中語意相同，但網頁應用防火牆可能因字串不同而無法正確偵測。

反向走訪 (Reverse Traversal) 逃脫技巧

作業系統「..」意指上一層目錄，惡意使用者可利用「http://xxx/yyy/../」之語法，

如「/cgi-bin/xxx.cgi」替換為「/cgi-bin/yyy/../xxx.cgi」，以躲避網頁應用防火牆偵測。

自我引用目錄 (Self-reference Directories) 逃脫技巧

作業系統 '.'意指目前目錄，惡意使用者可利用「http://xxx/./」之語法，如「/cgi-bin/phf」替換為「/./cgi-bin/./phf」，以躲避網頁應用防火牆偵測。

過早請求終止 (Premature Request Ending) 逃脫技巧

URL 語法如包含 %0d%0a 字串時，%0d 代表 Carriage Return (CR)，等同於 enter，%0a 代表 Line Feed，等同於換行。惡意使用者可利用 URL 加入 %0d%0a，使原 URL 被折解成多段，以躲避網頁應用防火牆偵測。

參數隱藏 (Parameter Hiding) 逃脫技巧

網頁應用防火牆可能會忽略 URL 語法中「?」後傳遞參數的檢查，惡意使用者可利用參數隱藏技巧，如 GET /index.htm?param=/../cgi-bin/some.cgi HTTP/1.0，以躲避網頁應用防火牆偵測。

HTTP 格式異常 (HTTP Mis-formatting) 逃脫技巧

依 RFC 1945 規定，HTTP 係以 <space> 分隔 HTTP request 每一個參數，目前多數的網頁伺服器可用 <tab> 代替 <space> 解析 HTTP request，但網頁應用防火牆的惡意特徵碼可能以「參數 +<space>」的方式進行比對。惡意使用者可將 <space> 替換成 <tab>，以躲避網頁應用防火牆偵測。

長網址 (Long URLs) 逃脫技巧

網頁應用防火牆可能只檢查 HTTP request 前幾個 bytes，惡意使用者可利用長 URL 逃脫技巧，如 GET /xxx <lots of characters> xxx/…/cgi-bin/some.cgi HTTP/1.0，以躲避網頁應用防火牆偵測。

DOS/Win 目錄語法 (DOS/Win directory syntax) 逃脫技巧

Internet Information Server (IIS) 或 DOS/Windows 伺服器會自動將 HTTP 協定之分隔資料夾「\」符號轉為「/」符號，但網頁應用防火牆可能只檢查 HTTP

協定之分隔資料夾「/」符號。惡意使用者可利用「\」符號，如 /cgi-bin\some.cgi，以躲避網頁應用防火牆偵測。

空值處理 (NULL Method Processing) 逃脫技巧

空值 (null) 於 C 語言內建的字串處理函式中表示一個字串的結尾。網頁應用防火牆若使用 C 語言內建的字串處理函式讀入字串，遇到空值字元即可能提前結束處理。惡意使用者可於 HTTP request 中夾帶空值字元，如 GET%00 /cgi-bin/some.cgi HTTP/1.0，以躲避網頁應用防火牆偵測。

檔名大小寫差別 (Case Sensitivity) 逃脫技巧

DOS/Windows 系統將檔名大小寫視為相同，網頁應用防火牆可能將檔名大小寫視為不相同。惡意使用者可將「/cgi-bin/some.cgi」替換成「/CGI-BIN/SOME.CGI」，以躲避網頁應用防火牆偵測。

連線切割 (Session Splicing) 逃脫技巧

網頁應用防火牆之惡意特徵碼可能只針對單一封包進行比對。惡意使用者可將 HTTP request 拆解成多個封包傳遞，如「GET / HTTP/1.0」拆解成 「GE」、「T 」、「/」、「 H」、「T」、「TP」、「/1」及「.0」，以躲避網頁應用防火牆偵測。

5.4. 漏判 (False Negative)

指待測物對網路攻擊行為應能判定而未判定。

5.5. 誤判 (False Positive)

指待測物對非網路攻擊行為判定為攻擊行為。

6. 技術要求

本規範技術要求包括書面審查及實機測試。書面審查標準主要參考共同準則，實機測試標準主要參考 ICSA 與 NSS 等國際實驗室之測試標準。

6.1. 書面審查類別

6.1.1. 安全標的

審查待測物之設備規格及安全功能需求。

6.1.2. 安全功能設計

審查待測物之設計安全性、安全架構及安全指引。

6.2. 書面審查類別之項目及判定標準

申請者應依基礎型或進階型之安全等級，提供符合該等級之安全標的及安全功能設計類別相關文件（如表 1）。

表1 書面審查之類別、項目及審查內容

類別	項目	審查內容	檢附文件	基礎型	進階型
安全標的	設備規格	附表 1-1	設備規格說明書	Π	Π
	安全功能需求	附表 1-2	設備規格說明書	Π	Π
安全功能設計	安全功能規格	附表 1-3	附件一、安全功能規格表	Π	Π
	設計安全性	附表 1-4	附件二、子系統描述與分類表		Π
	安全架構	附表 1-5	3 安全架構描述表		Π
	安全指引	附表 1-6	指引文件	Π	Π

6.2.1. 安全標的

申請者應提供待測物之設備規格說明書，包含設備規格（附表 1-1）及該設備可執行的安全功能需求 (附表 1-2)。

6.2.1.1. 設備規格

本項書面審查內容依申請者提供之設備規格說明書，檢視設備規格是否符合附表 1-1 設備規格之書面審查內容：

附表1.1 設備規格之書面審查內容

類別	項目	子項目	審查標準	基礎型	進階型
安全標的	設備規格	1.設備識別	應標示下列內容： 1. 名稱、廠牌、型號及版本 2. 申請者名稱 (製造商或代理商) 3. 製造商名稱 4. 設備形式 (硬體、韌體或軟體)	Π	Π
		2.範圍	應說明下列內容： 1. 待測物之實體範圍：包含待測物外觀、尺寸、主要零組件及執行必須之相關週邊設施。 2. 待測物之邏輯範圍：包含待測物安全功能以及功能之間相互關係。	Π	Π
		3.安全功能	應說明待測物之安全功能如何滿足本規範之安全功能需求。	Π	Π

6.2.1.2. 安全功能需求 (SFR)

本項書面審查內容依申請者提供之設備規格說明書，檢視安全功能需求 (SFR) 之執行內容是否符合附表 1-2 安全功能需求之書面審查內容。

附表1.2 安全功能需求之書面審查內容

類別	項目	子項目	審查標準	基礎型	進階型
安全	安全	1. 安全角色	安全功能應具備及設定以下安全角色： (1) 經授權的管理者 (2) 其他 (自行列舉)	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
標的	功能需求	2. 使用者屬性定義	安全功能應具備以下使用者屬性定義： (1) 使用者身份識別 (Identity) (2) 使用者被設定的角色屬性 (3) 其他 (自行列舉)	Π	Π
		3. 認證時序	安全功能應具備以下認證時序： (1) 列舉使用者身分認證前，可執行的安全功能 (如 DHCP, Show Status 等)。 (2) 完成使用者身分認證後，始可執行被授權的安全功能。	Π	Π
		4. 認證失敗處理	安全功能應具備以下認證失敗處理： (1) 可偵測出認證連續失敗次數。 (2) 當使用者進行登入，連續認證失敗次數達到指定值時，應拒絕該使用者再次登入，經採取特殊處置後，始可重新登入。	Π	Π
		5. 單次使用認證機制	待測物對使用者進行身份認證時，其認證資料 (如加密金鑰或登入密碼) 僅限單次使用，以避免認證資料被重複使用。	Π	Π
		6. 攻擊阻擋	安全功能應具備阻擋以下各式網頁應用程式攻擊的能力： (1) 緩衝區溢位攻擊 (Buffer Overflow) (2) 資料隱碼攻擊 (Injection) (3) 跨站腳本攻擊 (Cross-Site Scripting) (4) 破解認證機制 (Broken Authentication and Session Management) (5) 網頁程式參數竄改 (Parameter Tampering) (6) 隱藏欄位竄改 (Hidden Field Tampering) (7) 資訊塊中毒 (Cookie Poisoning) (8) 無效請求 (Invalid Request) (9) 強迫瀏覽攻擊 (Forceful Browsing) (10) 資訊洩漏 (Information Leakage) (11) 傳輸層保護不足 (Insufficient Transport	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
			Layer Protection) (12) HTTP 阻斷服務攻擊 (HTTP Denial of Service)		
		7. 逃脫技巧偵測	安全功能應具備以下逃脫技巧偵測： (1) 網址編碼 (URL Encoding) 逃脫技巧 (2) 雙斜線 (Double Slashes) 逃脫技巧 (3) 反向走訪 (Reverse Traversal) 逃脫技巧 (4) 自我引用目錄 (Self-reference Directories) 逃脫技巧 (5) 過早請求終止 (Premature Request Ending) 逃脫技巧 (6) 參數隱藏 (Parameter Hiding) 逃脫技巧 (7) HTTP 格式異常 (HTTP Mis-formatting) 逃脫技巧 (8) 長網址 (Long URLs) 逃脫技巧 (9) DOS/Win 目錄語法 (DOS/Win directory syntax) 逃脫技巧 (10) 空值處理 (NULL Method Processing) 逃脫技巧 (11) 檔名大小寫差別 (Case Sensitivity) 逃脫技巧 (12) 連線切割 (Session Splicing) 逃脫技巧	Π	Π
		8.初始化安全屬性	安全功能應具備以下初始化安全屬性： (1) 應提供預設之安全屬性，如預設之阻擋規則(值) 等。 (2) 允許被授權的管理者，變更不同的安全屬性。	Π	Π
		9. 安全功能行為管理	安全功能應具備以下安全功能行為管理： (1) 可啟動及關閉待測物。 (2) 可允許及禁止管理者或設備登入待測物進行管理。 (3) 如待測物具備遠端管理功能時，可限制管理者自特定網址 (IP Address) 登入待測物進行管理。 (4) 可變更待測物之登入失敗次數的最大值。	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
			(5) 當使用者登入待測物失敗次數超過最大值致無法登入時，待測物應具備恢復使用者登入之管理功能。 (6) 可對待測物之安全規則進行新增、刪除、修改與檢視。 (7) 可對待測物之使用者屬性進行新增、刪除、修改與檢視。 (8) 可修改待測物之系統時間。 (9) 可備份、建立、刪除、清空或瀏覽待測物之稽核紀錄 (Audit Trail)。 (10) 可備份待測物之安全規則及使用者安全屬性。 (11) 可將待測物組態復原至備份組態。		
		10. 殘餘資訊保護	當待測物處理通過之資料封包，應清除或覆蓋可再使用的系統資源 (如資料暫存區) 之殘餘資訊，或其他保護機制。	Π	Π
		11. 密碼操作	待測物應以密碼演算法保護遠端管理連線。	Π	Π
		12. 可信賴之時戳	待測物應具備可信賴之時戳 (Reliable Timestamp)，正確記錄稽核資料的日期及時間。	Π	Π
		13. 稽核紀錄	安全功能應具備以下稽核紀錄： (1) 待測物應依下列事件類型產生其稽核紀錄，並存於資料庫中： A. 啟閉稽核功能。 B. 存取稽核資料。 C. 使用者登錄成功或失敗、登錄權限變更及恢復。 D. 變更安全屬性。 E. 變更系統時間。 (2) 每筆稽核紀錄至少包含下列資訊： A. 事件識別碼。	Π	Π

類別	項目	子項目	審查標準	基礎型	進階型
			B. 事件日期及時間。 C. 事件類型 D. 事件成功或失敗		
		14. 稽核紀錄之查詢	安全功能應具備以下稽核紀錄之查詢： (1) 可由被授權的管理者查詢各種稽核紀錄（含事件之稽核紀錄）。 (2) 稽核紀錄應以適合管理者理解之方式呈現。 (3) 可依設定條件查詢稽核紀錄。	Π	Π
		15. 稽核紀錄可用性之保證	安全功能應具備以下稽核紀錄可用性之保證： (1) 應確保已儲存的稽核紀錄不被非授權使用者刪除。 (2) 當非授權使用者嘗試竄改已儲存的稽核紀錄時，應偵測並記錄之。 (3) 當發生稽核紀錄儲存設備之空間用盡、故障或遭受攻擊時，應維持儲存稽核紀錄之功能。其中空間即將用盡時，除提供系統警告外，並應至少提供下列一種處置方式： A. 另存稽核紀錄：將需要保存的稽核紀錄另存至其他儲存設備。 B. 刪除稽核紀錄：將不需要保存之稽核紀錄予以刪除。 C. 覆蓋稽核紀錄：新增之稽核紀錄覆蓋最舊的稽核紀錄。	Π	Π
		16. 資訊流屬性控管	安全功能應具備以下資訊流屬性及控管： (1) 安全規則之資訊流屬性如下： A. 主體屬性 (如來源端及目的端網路位址 (IP Address) 等)。 B. 訊息屬性 (如通訊埠、通訊協定或應用程式等)。 (2) 至少提供下列其中一種安全規則之資訊流控管： A. 依安全規則允許或拒絕資訊流。 B. 身分認證後，依安全規則進行資訊流管制。	Π	Π

6.2.2. 安全功能設計

申請者應提供待測物安全功能規格、設計安全性、安全架構及安全指引等文件，以確保安全功能 (TSF) 能正確執行。

6.2.2.1. 安全功能規格

本項書面審查內容依申請者提供之附件一、安全功能規格表，檢視安全功能規格之內容是否符合附表 1-3 安全功能規格之書面審查內容。

附表1.3 安全功能規格之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能設計	安全功能規格	安全功能介面應實現安全功能需求，應說明安全功能介面 (TSFI)以下規格： (1) 安全功能介面名稱 (2) 目的 (3) 可實現的安全功能需求 (4) 操作方式 (5) 參數 (6) 執行的動作 (7) 錯誤訊息	Π	Π

6.2.2.2. 設計安全性

本項書面審查內容依申請者提供之附表二、設計安全性表，檢視設計安

全性之內容是否符合附表 1-4 設計安全性之書面審查內容。

本項書面審查內容與判定標準說明如附表 1-4：

附表1.4 設計安全性之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能設計	設計安全性	應說明如何以子系統組成安全功能規格之安全功能介面，並說明安全功能子系統以下規格： (1) 子系統名稱 (2) 目的 (3) 子系統隸屬之安全功能介面 (4) 子系統行為說明		Π

6.2.2.3. 安全架構

本項書面審查內容依申請者提供之 3 安全架構表，檢視安全架構之內容是否符合附表 1-5 安全架構之書面審查內容。

本項書面審查內容與判定標準說明如附表 1-5：

附表1.5 安全架構之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能設計	安全架構	應依據 6.2.2.1 安全功能規格及 6.2.2.2 設計安全性之檢附文件，說明待測物安全架構如何滿足安全功能需求 (SFR)，並作為實機測試項目設計的參考。針對		Π

類別	項目	審查標準	基礎型	進階型
		安全功能介面及子系統，提出安全架構的設計概念與操作安全建議，也需符合後續提供的指引文件。安全架構應說明下列項目： (1) 待測物因執行安全功能所區隔的安全領域。 (2) 安全功能的安全初始程序。 (3) 安全功能的自我保護機制。 (4) 安全功能執行如何避免被繞道。		

6.2.2.4. 安全指引

本項書面審查內容依申請者提供之指引文件，檢視文件內容是否符合附表 1-6 安全指引之書面審查內容。

本項書面審查內容與判定標準說明如附表 1-6：

附表1.6 安全指引之書面審查內容

類別	項目	審查標準	基礎型	進階型
安全功能設計	安全指引	(1) 應定義每個使用者角色 (2) 應提供每個使用者角色於執行安全功能 (TSF) 時之相關說明，包括： A. 週邊設備及安全設定 B. 允許使用的介面	Π	Π

類別	項目	審查標準	基礎型	進階型
		C. 安全參數定義 D. 可能產生的安全事件 E. 應遵循的安全措施 (3) 應說明於特殊權限操作時的安全環境要求，並提供適當的警告 (4) 應列舉待測物操作時的所有運作模式 (5) 應列舉待測物作業失敗 (Failure) 或人員操作錯誤產生的各種情況及處理方式 (6) 應說明待測物運作前的安全準備作業，包含待測物安裝及啟動方式 (7) 應說明待測物操作的安全環境設置，應包括以下項目： A. 待測物使用目的 (如針對伺服器進行網路協定管制作業等) B. 實體環境安全 (如待測物需置於有門禁管制的環境等) C. 人員安全 (如僅有授權人員能存取待測物等) D. 連接安全 (如待測物與其他網路伺服器之連線安全等) (8) 指引文件將做為實機測試的依據。		

6.3. 實機測試類別

實機測試包含安全功能測試、壓力測試、堅實測試及穩定測試。

6.3.1. 安全功能測試

測試待測物所具有安全防護相關功能。

6.3.2. 壓力測試

當大量網路流量通過待測物時，測試待測物是否保持正常運作。

6.3.3. 堅實測試

當待測物遭受網路攻擊時，測試待測物是否保持正常運作。

6.3.4. 穩定測試

當待測物置於真實網路流量的環境中，測試待測物是否保持正常運作。

6.4. 實機測試之類別、項目及判定標準

實機測試分為基礎型與進階型，包含安全功能測試、壓力測試、堅實測試及穩定測試四個類別。實機測試項目及標準如表 2。

表2 實機測試之類別、項目及判定標準

類別	項目	判定標準	基礎	進階
安全功能測試	攻擊阻擋	1. 漏判測試： 依 6.4.1.1.3. (1) 進行測試，漏判率應小於或等於 10%。 2. 誤判測試： 依 6.4.1.1.3. (2) 進行測試，不能發生誤判。	Π	
		1. 漏判測試： 依 6.4.1.1.3. (1) 進行測試，漏判率應		Π

類別	項目	判定標準	基礎	進階
		小於或等於 5%。 2. 誤判測試： 依 6.4.1.1.3. (2) 進行測試，不能發生誤判。		
	逃脫技巧偵測	依 6.4.1.2.3. 進行測試，不能誤判或漏判，並能產生相關訊息。	Π	Π
	安全事件紀錄	依 6.4.1.3.3 進行測試，應正確記錄違反安全規則之事件名稱、時間、來源 IP、目的 IP 及內容。	Π	Π
	安全管理	依 6.4.1.4.2. 進行測試，應具備下列管理功能： (1) 管理待測物之通行碼。 (2) 輸入通行碼錯誤之次數限制及管制。	Π	Π
	備援管理	依 6.4.1.5.2. 進行測試，備援待測物應於規定時間內接替失效之待測物。		Π
壓力測試	吞吐量	依 6.4.2.1.2. 進行測試，當待測物所負荷的吞吐量達到其規格說明之最大值時，不能發生封包遺失且待測物安全功能應正常運作。	Π	Π
	最大連線數	依 6.4.2.2.2. 進行測試，當達到待測物規格說明之最大連線數時，不能發生斷線且待測物安全功能應正常運作。		Π
	最大連線建立速率	依 6.4.2.3.2. 進行測試，當達到待測物規格說明之最大連線建立速率時，不能發生斷線且待測物安全功能應正常運作。		Π
堅實測試	阻斷式攻擊	依 6.4.3.1.2. 進行測試，當攻擊流量低於或等於待測物規格說明之吞吐量最大值時，安全功能應正常運作。	Π	Π

類別	項目	判定標準	基礎	進階
	遠端管理異常流量	依 6.4.3.2.3. 進行測試，待測物遠端管理介面對服務/協定異常流量應保持正常運作。		Π
	非正常關機復原	依 6.4.3.3.1. 進行測試，待測物應可復原到非正常關閉電源前的最後狀態。	Π	Π
穩定測試	真實流量	依 6.4.4.1.3. 進行測試，待測物應可持續 168 小時穩定運作。	Π	
		依 6.4.4.1.3. 進行測試，應可持續 336 小時穩定運作。		Π

6.4.1. 安全功能測試

檢視待測物之安全功能需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.4.1.1. 攻擊阻擋

6.4.1.1.1. 測試環境

(1) 測試平台：可產生攻擊測試樣本之測試儀器或程式。
(2) 伺服器：具有網頁應用程式弱點之伺服器。
(3) 網路連接線：乙太網路線或光纖纜線。
(4) 連接測試平台、待測物及伺服器如圖 1。
(5) 開啟待測物之安全功能。

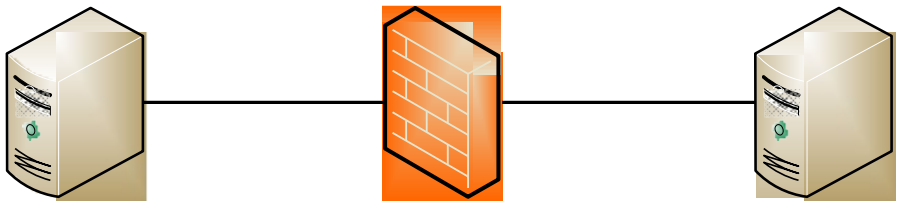


圖1　攻擊阻擋測試接續圖

6.4.1.1.2. 測試樣本

以附表 1-2 之項目 6 為依據，由測試平台產生至少 100 個攻擊測試樣本，測試樣本必須涵蓋附表 1-2 之項目 6 所列網頁應用程式攻擊類型半數以上。

6.4.1.1.3. 測試方法及標準

依圖 1 建置具有網頁應用程式弱點之伺服器，測試平台利用測試樣本測試待測物，待測物必須正確偵測及阻擋攻擊，且不能誤判正常的網路存取連線。

(1) 漏判測試方法及標準

基礎型待測物之漏判率應小於或等於 10%；進階型待測物之漏判率應小於或等於 5%。

(2) 誤判測試方法及標準

對伺服器進行 100 次以上的正常網頁存取 (包含：登入、認證、下載及上傳等動作)，基礎型與進階型待測物均不能有誤判的情況發生。

6.4.1.1. 逃脫技巧偵測

驗證待測物能夠偵測與阻擋套用逃脫技術應用下所產生的網頁攻擊。

6.4.1.1.1. 測試環境 同 6.4.1.1.1.。

6.4.1.1.2. 測試樣本

將 6.4.1.1.2.之攻擊樣本套用附表 1-2 之項目 7 表列之各種逃脫技巧，由測試平台產生抵禦迴避攻擊之測試樣本。

6.4.1.1.1. 測試方法及標準

(1) 當偵測攻擊時，不能誤判或漏判。

(1) 當偵測到攻擊時，應產生對應的警示訊息。

(2) 如攻擊被成功解碼後，應提供正確的攻擊名稱。

6.4.1.2. 安全事件紀錄

6.4.1.2.1. 測試環境

(1) 測試平台：可產生攻擊測試樣本之測試儀器或程式。
(2) 伺服器：具有網頁應用程式弱點之伺服器。
(3) 將測試平台、待測物及伺服器依圖 1 架設測試環境。
(4) 透過待測物提供的 Web GUI 管理介面或終端管理介面進入待測物，找到待測物安全紀錄功能的對應設定位置，將待測物安全紀錄功能開啟。

6.4.1.2.2. 測試樣本

以測試平台產生之違反防護規則的網路流量作為測試樣本。

6.4.1.2.3. 測試方法及標準

由測試平台產生違反安全事件的流量通過待測物，待測物的流量統計資訊應正確記錄違反安全規則之事件名稱、時間、來源 IP、目的 IP 及內容。

6.4.1.3. 安全管理功能

6.4.1.3.1. 測試環境 同 6.4.1.1.1.。

6.4.1.3.2. 測試方法及標準

(1) 由測試平台連線至待測物，確認待測物是否需要通行碼才可進行設定。待測物必須輸入正確之通行碼才能進行管理設定。

(2) 嘗試輸入錯誤通行碼，檢查當錯誤超過最大容忍次數時，是否會鎖定待測物之管理功能。輸入錯誤超過最大容忍次數後，待測物應鎖定一段時間以避免遭受攻擊。

6.4.1.4. 備援管理 (適用進階型)

6.4.1.4.1. 測試環境

(1) 測試平台：可產生攻擊測試樣本之測試儀器或程式。
(2) 伺服器：具有網頁應用程式弱點之伺服器。
(3) 交換集線器 (Switch Hub)：匯集多條通訊纜線之裝置。
(4) 網路連接線：乙太網路線或光纖纜線。
(5) 開啟待測物之備援功能及防火牆功能。

(6) 連接測試平台、待測物、備援待測物及伺服器如圖 2。

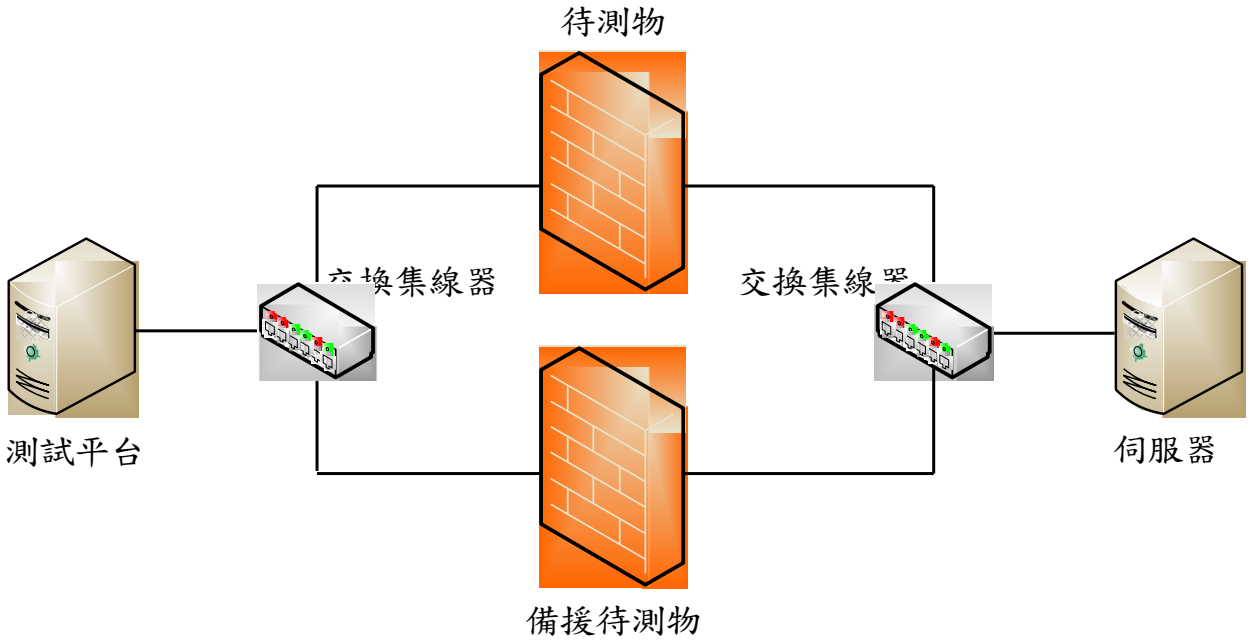


圖2　備援測試接續圖

6.4.1.4.2. 測試方法及標準

測試平台產生網路流量經待測物傳送至伺服器，至少 30 秒後，將待測物電源移除使之失效，備援待測物應於 10 秒內自動接替待測物啟動防火牆功能，確保伺服器仍可正常運作。

6.4.2. 壓力測試

6.4.2.1. 吞吐量測試

6.4.2.1.1. 測試環境

(1) 測試平台：可產生網路封包之測試儀器或程式。
(2) 測試平台 A 埠：模擬用戶端送收網路封包。
(3) 測試平台 B 埠：模擬伺服器端送收網路封包。
(4) 網路連接線：乙太網路線或光纖纜線。
(5) 連接測試平台及待測物如圖 3，其中乙太網路線或光纖線路連接數量依待測物運作模式 (如 Proxy 或 Transparent Mode) 決定。
(6) 代理模式 (Proxy Mode)：乙太網路線或光纖線路連接數量為一條，測試平台 A 埠及 B 埠為同一連接埠。
(7) 通透模式 (Transparent Mode)：乙太網路線或光纖線路連接數量為兩條，測試平台 A 埠及 B 埠為獨立的兩個連接埠。
(8) 開啟待測物之安全功能。

(9) 測試平台產生大小為 64、570、594 及 1518 位元組之網路封包，將其依 IMIX 之比例 57%、7%、16%及 20%混合，時間至少 60 秒。

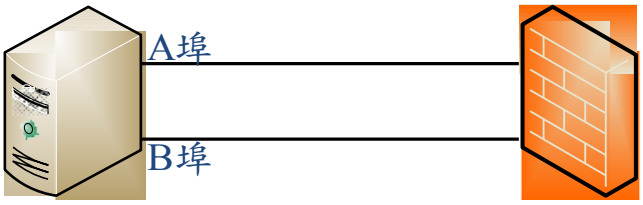


圖3　吞吐量測試接續圖

6.4.2.1.2. 測試方法及標準

測試平台建立自 A 埠經待測物至 B 埠之網路連線後，傳送不同大小之封包。當待測物所負荷的吞吐量達到其規格說明之最大值時，不能發生封包遺失且待測物安全功能應正常運作。

6.4.2.2. 最大連線數

6.4.2.2.1. 測試環境　同 6.4.2.1.1.。

6.4.2.2.2. 測試方法及標準

測試平台每秒建立一條自 A 埠經待測物至 B 埠之連線。當達到待測物規格說明之最大連線數時，不能發生斷線且待測物安全功能應正常運作。

6.4.2.3. 最大連線建立速率

6.4.2.3.1. 測試環境　同 6.4.2.1.1.。

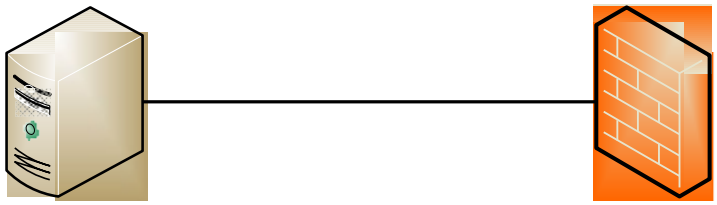
6.4.2.3.2. 測試方法及標準

測試平台建立自 A 埠經待測物至 B 埠之連線，並逐漸提高連線建立速率，當達到待測物規格說明之最大連線建立速率時，不能發生斷線且待測物安全功能應正常運作。

6.4.3. 堅實測試

6.4.3.1. 阻斷式攻擊

6.4.3.1.1. 測試環境



測試平台　　待測物

圖4　阻斷式攻擊測試接續圖

(1) 測試平台：可產生大量網路流量之測試儀器或程式。
(2) 網路連接線：乙太網路線或光纖纜線。
(3) 連接測試平台及待測物如圖 4。
(4) 開啟待測物之安全功能。
(5) 測試平台針對待測物的服務連接埠，發動阻斷式攻擊。

6.4.3.1.2. 測試方法及標準

測試平台送出大量的網路流量，持續 600 秒攻擊待測物開啟的連接埠，並阻斷其服務。當攻擊流量低於或等於待測物規格說明之吞吐量最大值時，安全功能應正常運作。

6.4.3.2. 遠端管理異常流量

6.4.3.2.1. 測試環境

(1) 測試平台：可產生大量網路流量之測試儀器或程式。
(2) 網路連接線：乙太網路線或光纖纜線。
(3) 連接測試平台及待測物如圖 4。
(4) 開啟待測物之安全功能。
(5) 透過待測物提供的終端管理介面進入待測物進行設定，開啟待測物之遠端管理功能。

6.4.3.2.2. 測試樣本

以測試平台產生之服務或協定異常流量至少 10 種作為測試樣本。

6.4.3.2.3. 測試方法及標準

測試平台送出測試樣本至待測物，待測物之遠端管理功能應正常運作。

6.4.3.3. 非正常關機恢復

6.4.3.3.1. 測試方法及標準

待測物運作期間不正常關閉電源時，經重新啟動後，待測物應可復原到非正常關閉電源前的最後狀態。

6.4.4. 穩定測試

6.4.4.1. 真實流量

6.4.4.1.1. 測試環境

(1) 流量錄製平台：錄製網路封包。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接流量錄製平台、路由器、內部網路及網際網路如圖 5。

(4) 路由器將往來 A、B 兩埠的網路封包複製一份後，經 C 埠送至流量錄製平台，流量錄製平台將網路封包錄製成為檔案儲存。

(5) 流量重播平台：將預先錄製之真實流量檔案還原成網路封包送至待測物。

(6) 連接流量重播平台與待測物如圖 6。

(7) 網路封包來源 IP 位址如屬內部網路，流量重播平台將網路封包經 A 埠送至待測物；反之，來源 IP 位址如屬網際網路，則網路封包經 B 埠送至待測物。

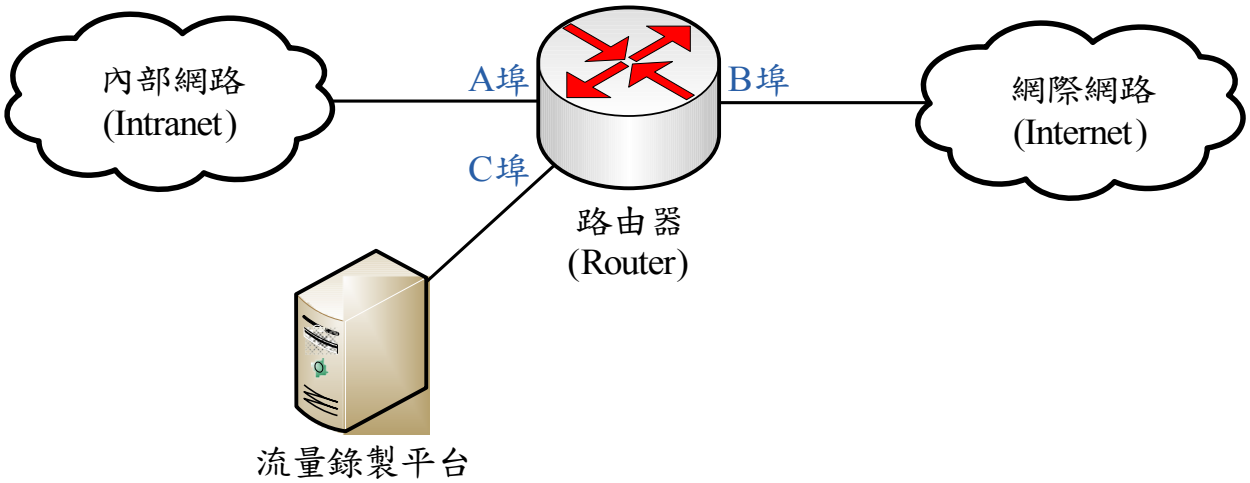


圖5　流量錄製接續圖

圖6　流量重播接續圖

6.4.4.1.2. 測試樣本

測試樣本必須滿足以下要求：

(1) 應從真實網路環境錄製。

(2) 具備至少 100 位使用者同時上線之網路流量。

(3) 應為該待測物送測前 2 周內所錄製之網路流量。

(4) 須達該待測物規格說明之最大連線數 50% 以上。

(5) 須達該待測物規格說明之吞吐量最大值 50% 以上。

(6) 包含至少 10 種應用類型，每一種應用類型至少包括一個應用項目，全部之應用項目須達 50 個以上。舉例如下：

A. Chat： msn、yahoo messenger、qq、xmpp 及 aol-icq。

B. Email：gmail、smtp、pop3、imap 及 webmail。

C. File Transfer：ftp、flashget 及 smb。

D. Game：garena、facebook app 及 steam。

E. P2P：gnutella、edonkey、bt、xunlei、fasttrack、ares、kazaa 及 ed2k。

F. Remote Access：windows remote desktop、telnet、ssh 及 vnc。

G. Streaming：rtsp、qqtv、pplive、ppstream、qvod、flashcom、itunes、rtp 及 shoutcast。

H. VoIP：skype 及 sip。

I. Web：http、https、http download、http video 及 http range get。

J. Others：hopster、softether、dns、snmp、oracle 及 ms-sql。

6.4.1.1.1. 測試方法及標準

(1) 基礎型待測物須進行連續 168 小時測試；進階型待測物須進行連續 336 小時測試。

(2) 測試過程待測物不能發生下列不穩定之情況：

A. 當機。

B. 重新開機。

C. 連線不正常中斷。

D. 安全功能失效。

附件

附件1、　　安全功能規格表

安全功能介面名稱 TSFI	目的 Purpose	安全功能介面可實現之安全功能需求 SFR	操作方式 Method of Use	參數 Parameter	執行動作 Actions	錯誤訊息 Error Message
列出所有安全功能介面。	說明各安全功能介面之安全功能目的。	說明各安全功能介面如何實現附表 1-2 所列之安全功能需求。	說明如何使用各安全功能介面。	說明各安全功能介面所有參數及其意義。	說明各安全功能介面如何運作及其執行細節。	說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。
範例： *TSFI_CLI*	*範例：* *提供命令列模式操作介面*	*範例：* *SFR_安全管理：提供安全管理功能*	*範例：* *以 ssh 連接待測物，即提供命令列模式操作介面*	*範例：* *ID & password*	*範例：* *可下達管理命令操作待測物*	*範例：* *連接失敗* *認證失敗*

附件2、　　設計安全性表

子系統名稱 **Subsystem**	**目的** **Purpose**	**子系統隸屬之安全功能介面** **TSFI**	**子系統行為說明** **Behavior Description**
列出各安全功能介面之子系統。	說明各子系統之安全功能目的。	說明各子系統隸屬於附件一所列之安全功能介面。	說明各子系統行為如下： (1) 如何實現安全功能介面的功能。 (2) 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。
範例： *Subsystem_ssh*	*範例：* *提供 ssh 服務*	*範例：* *TSFI_CLI*	*範例：* *(1) 提供 TSFI_CLI 命令列模式操作介面* *(2) 與其他子系統之互動：* *(A) Subsystem_auth: 傳遞認證資訊給 Subsystem_auth，並由回覆訊息確認認證是否成功* *(B) Subsystem_terminal: ...*

附件3、　　安全架構表

項目	說明	
1.安全領域	安全領域名稱	安全領域說明

項目	說明	
Security Domain	列出各安全功能介面對應之安全領域 *範例：* *TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection*	在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 *範例：* *透過 TSFI_GUI 來執行管理功能石，該 TSFI 同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。*
2.初始程序	**相關元件**	**初始程序說明**

項目	說明		
Secure Initialization	操作待測物的相關元件/環境 *範例：* *待測物網路連接程序*	提供安全啟動待測物之相關元件起始步驟及安裝程序。 *範例：* *1. 從端口標記為 0/0（ethernet0/0 接口）連接一個 RJ-45 電纜到交換機或路由器 Trust 安全區。* *2. 從端口標記為 0/1（ethernet0/1 接口）連接一個 RJ-45 電纜到交換機或路由器中的 DMZ 安全區。*	
3.自我保護	**自我保護功能**	**與外部設備之關係**	**自我保護機制說明**

項目	說明		
Self-Protection	列出各安全功能介面對應之自我保護機制 *範例：* *TSFI_WEB:* *自我保護 1:身分驗證* *自我保護 2:遠端連線加密*	說明安全功能及其介面與外部設備之資料交換動作 *範例：* *遠端以瀏覽器連線待測物進行管理功能時，以 TSFI_WEB GUI 介面進行身分認驗證*	需說明安全功能介面提供實體上或邏輯上的自我保護機制 *範例：* *1. 應輸入通行碼才能進入介面。* *2. 資料傳輸機制：TLS/SSL。* *3. 特殊執行方式：指紋辨識。* *4. 特殊設備需求：指紋辨識器。*
4.防止繞道	**防止繞道功能**	**防止繞道機制說明**	

項目	說明	
Non-Bypassibility	列出各安全功能對應之防止繞道機制 *範例：* *TSF_Authentication 身分驗證功能*	1. 列舉可能繞道之手法 2. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 *範例：* *可能直接以維護介面不經身份認證操控待測物。* *防範作法：以實體封鎖方式，防止利用維護介面繞道身分認證程序。*