網路型垃圾郵件過濾設備資通安全檢測技術規範
修正總說明

為更明確本技術規範之適用範圍及因應本會建置病毒樣本資料庫，提供測試樣本供實驗室對設備進行資通安全檢測之技術要求，爰修訂網路型垃圾郵件過濾設備資通安全檢測技術規範，作為辦理此類設備資通安全檢測之依據。主要修正重點分述如下：

一、概說(草案第 1 點)及適用範圍(草案第 2 點)-酌作文字修正，更明確說明設備之適用範圍。

二、安全等級(草案第 3 點) -酌作文字修正，更明確說明不同安全等級之差異性及測試項目。

三、技術要求(草案第 6 點)- 修訂書面審查及實機測試之審查類別、審查內容及審查標準。

網路型垃圾郵件過濾設備資通安全檢測技術規範

修正對照表

修正規定	現行條文	說明
1. 概說 網路型垃圾郵件過濾設備（以下簡稱垃圾郵件過濾設備）將內部網路(Internal Network)與外部網路(External Network)之間傳送的電子郵件，進行判讀，並依不同的安全策略設定規則，判定電子郵件是否為垃圾郵件，加以標註、刪除、保存或紀錄。	1.概說 網路型垃圾郵件過濾設備(以下簡稱垃圾郵件過濾設備)將傳送於內部網路(Internal Network)與外部網路(External Network)之間的電子郵件，進行判讀，並依不同的安全策略設定規則，判定電子郵件是否為垃圾郵件，加以標註、刪除、保存或紀錄。	酌作文字修正。
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郵件過濾設備，可支援至開放系統介面(OSI, Open System Interface)第七層(Layer 7)，依不同網路區域設定所屬之過濾策略管控傳遞郵件。本規範不適用安裝於電腦主機之純軟體郵件過濾軟體(Host-based Anti-Spam Software)。	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郵件過濾設備，可支援至開放系統介面(OSI, Open System Interface)第七層(Layer 7)，依不同網路區域設定所屬之過濾策略(policy)，以管控傳遞郵件；不適用安裝於電腦主機之純軟體郵件過濾軟體(Host-based Anti-Spam Software)。	酌作文字修正，明確說明設備之適用範圍。
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)。 3.1. 基礎型垃圾郵件過濾設備 基礎型設備安全功能測試項目包括郵件過濾、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。 3.2. 進階型垃圾郵件過濾設備 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郵件過濾及郵件內容反釣魚網址過濾；壓力測試項目包括最大同時連線數與最大建立連線速率；堅實測試項目包括異常流量；穩定測試項目包括真實	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)，進階型垃圾郵件過濾設備有比基礎型垃圾郵件過濾設備更加嚴格的技術要求。 3.1. 基礎型垃圾郵件過濾設備 指具有基礎之功能包括垃圾郵件過濾、安全記錄、操作管理等功能之垃圾郵件過濾設備。垃圾郵件過濾的準確率必需符合基礎型的規範。 3.2. 進階型垃圾郵件過濾設備 指具有基礎型垃圾郵件過濾設備功能外，還具有更準確的判斷率。	酌作文字修正，明確說明不同安全等級之差異性及測試項目。

修正規定	現行條文	說明
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 Anti-Spam Certification Testing Criteria Version 1.4-FinalDraft NSS UTM-Methodology-v2.0	4. 參考標準 ISO/IEC 15408 共同準則(Common Criteria for Information Technology Security Evaluation, CC) ICSA Anti-Spam Certification Testing Criteria Version 1.4-FinalDraft NSS UTM-Methodology-v2.0	未修正
5. 用語釋義 5.1. 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 5.2. 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。 5.3. 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。 5.4. 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。 5.5. 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。 5.6. 安全功能需求 (Security Functional Requirement, SFR) 指共同準則第二部份 (Common	5. 用語釋義 5.1. 網路型垃圾郵件過濾設備 (Networked Anti-Spam Device) 指在網路上以獨立硬體運作之垃圾郵件過濾設備，不同於安裝在個人電腦或伺服器上之垃圾郵件過濾軟體 (Host-Based Anti-Spam Software)。網路型垃圾郵件過濾設備對於在不同網路區域間所傳遞的電子郵件加以測試，並依網路管理人員的需求，設定不同的處理規則。 5.2. 內部網路(Internal Network) 指透過垃圾郵件過濾設備所保護的網路區域。 5.3. 外部網路(External Network) 指透過垃圾郵件過濾設備所區隔不可信任或非保護的網路區域。 5.4. 最大同時連線數 指垃圾郵件過濾設備能同時處理之 TCP 連線數最大值。 5.5. 吞吐量 指垃圾郵件過濾設備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)。 5.6. 最大連線建立速度 指垃圾郵件過濾設備能處理的 TCP 連線建立速度，通常的表示法為「TCP 連線數/每秒」。 5.7. 誤判率(False Positive Rate)	增訂專有名詞解釋及酌作文字修正。

修正規定	現行條文	說明
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。 5.7. 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。 5.8. 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。 5.9. 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。 5.10. 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。 5.11. 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。 5.12. 繞道 (Bypass) 指避開待測物安全功能檢查之技巧。(如：未經過身分鑑別，直接進入稽核功能介面)。 5.13. 最大同時連線數 指待測物能同時處理之 TCP 連線數最大值。 5.14. 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)。 5.15. 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	指垃圾郵件過濾設備將正常郵件判定為垃圾郵件的比例。 5.8. 漏判率(False Negative Rate) 指垃圾郵件過濾設備將垃圾郵件判定為正常郵件的比例。 5.9. 共同準則 為資通安全產品評估及驗證之標準之一，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、測試實驗室與驗證機關(構)評估及驗證資通安全產品安全性與功能性之依據。參考網址 http://www.commoncriteriaportal.org 5.10. 評估標的(Target of Evaluation, TOE) 指申請評估及驗證之產品及其相關使用手冊。 5.11. 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。 5.12. 安全標的(Security Target, ST) 指產品能符合保護剖繪(PP)或特定安全需求製作之規格文件。 5.13. 安全功能(TOE Security Functions, TSF) 指該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。 5.14. 安全功能需求(Security Functional Requirement, SFR) 指為定義於共同準則第二部(Common Criteria, Part 2)的安全相關需求條文，用以描述一產品之安全功能(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。	

修正規定	現行條文	說明
秒」。 5.16. 網路型垃圾郵件過濾設備 (Networked Anti-Spam Device) 指在網路上以獨立硬體運作之垃圾郵件過濾設備，不同於安裝在個人電腦或伺服器上之垃圾郵件過濾軟體 (Host-Based Anti-Spam Software)。網路型垃圾郵件過濾設備對於在不同網路區域間所傳遞的電子郵件加以測試，並依網路管理人員的需求，設定不同的處理規則。 5.17. 內部網路 (Internal Network) 指透過垃圾郵件過濾設備所保護的網路區域。 5.18. 外部網路 (External Network) 指非垃圾郵件過濾設備保護的網路區域。	5.15. 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。	
6. 技術要求 (詳如附件一)	6.技術要求 (詳如附件二)	修訂書面審查及實機測試之審查類別、審查內容及審查標準。

附件一

6. 技術要求

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**錯誤! 找不到參照來源。**)。

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	✓	✓
	安全功能需求	**錯誤! 找不到參照來源。**	設備規格說明書	✓	✓
安全功能設計	安全功能規格	**錯誤! 找不到參照來源。**	0 安全功能介面表	✓	✓
	設計安全性	**錯誤! 找不到參照來源。**	0 子系統描述與分類表		✓
	安全架構	**錯誤! 找不到參照來源。**	**錯誤! 找不到參照來源。**安全架構描述表	✓	✓

類別	項目	審查內容	檢附文件	基礎型	進階型
	安全指引	**錯誤！找不到參照來源。**	指引文件	✓	✓

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 (**錯誤! 找不到參照來源。**) 。

6.2.1.1. 設備規格說明

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)	✓	✓
		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。	✓	✓
		3.安全功能	應說明待測物之安全功能如何滿足本	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			規範之安全功能需求。		

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**錯誤! 找不到參照來源。**。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
安全標的	安全功能需求	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)	✓	✓
		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)	✓	✓
		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。	✓	✓
		4. 認證失	安全功能應具備以下認證失敗處理：	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		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。		
		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。	✓	✓
		6. 資料流控制	安全功能應具備根據以下資料屬性，對資料流進行控制、過濾等管理的能力： (1) 來源端位址或其他自行指定之來源格式 (2) 目的端位址及其他自行指定之目的格式 (3) 通訊協定 (4) 網路卡介面 (5) 服務型態 (6) 其他 (自行指定)	✓	✓
		7.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。	✓	✓
		8. 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	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			進行管理。 (4) 可變更待測物之登入失敗次數的最大值。 (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。		
		9. 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。	✓	✓
		10. 密碼操作	待測物應以密碼演算法保護遠端管理連線。	✓	✓
		11. 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。	✓	✓
		12. 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。	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			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。 B. 事件日期及時間。 C. 事件類型 D. 事件成功或失敗		
		13. 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。	✓	✓
		14. 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。	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			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。		

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 0 安全功能規格表，檢視安全功能規格之內容是否符合**錯誤! 找不到參照來源。**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	✓	✓

類別	項目	審查標準	基礎型	進階型
		(6) 執行的動作 (7) 錯誤訊息		

6.2.2.2. 設計安全性

本項書面審查內容依申請者提供之 0 設計安全性表，檢視設計安全性之內容是否符合**錯誤! 找不到參照來源。**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**錯誤! 找不到參照來源。**：

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		✓

6.2.2.3. 安全架構

本項書面審查內容依申請者提供之 0 安全架構表，檢視安全架構之內容是否符合**錯誤! 找不到參照來源。**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**錯誤! 找不到參照來源。**：

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**錯誤! 找不到參照來源。**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**錯誤! 找不到參照來源。**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**錯誤! 找不到參照來源。**：

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	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	✓	✓

類別	項目	審查標準	基礎型	進階型
設計		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 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)		

類別	項目	審查標準	基礎型	進階型
		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

測試待測物於面臨大量網路封包或連線時，安全功能是否能保持正常運作。

6.3.3. 堅實測試

測試待測物本身開啟服務或協定時，面臨針對待測物本身而來的不正常連線行為，是否能保持正常運作。

6.3.4. 穩定測試

將待測物置於真實網路流量下運作測試，是否有不穩定的狀況發生。

6.4. 實機測試類別之項目及判定標準

實機測試分為基礎型與進階型，皆包含安全功能測試、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	基礎型	進階型
安全功能測試	封包過濾	依 6.4.1.1.2. 進行測試，應具備下列過濾功能： 1. 應可阻擋設定之封包。 2. 應可通過設定之封包。	✓	✓
	流量內容統計	依 6.4.1.2.2. 進行測試，應正確記錄通過之流量內容，包含時間、傳輸速率 (bps) 、通訊協定及通訊埠號。	✓	✓
	安全事件紀錄	依 6.4.1.3.2. 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。	✓	✓
	安全管理	依 6.4.1.4.2. 進行測試，應具備下列管理功能： 1. 具備通行碼管理。 2. 具備通行碼輸入錯誤次數之上限設定，錯誤輸入超過上限次數後須封鎖管理介面一段時間。	✓	✓
	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。		✓
	流量控管規則	依 6.4.1.6.2. 進行測試，應可設定規則以控管網路流量。		✓
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。	✓	✓
	最大連線	依 6.4.2.2.2. 進行測試，當達到待測物規格		✓

類別	項目	判定標準	基礎型	進階型
	數	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。		
	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。		✓
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。	✓	✓
	遠端管理異常流量	依 6.4.3.2.2. 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。		✓
	非正常關機恢復	依 6.4.3.3.2. 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。	✓	✓
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。	✓	
		依 6.4.4.1.3. 進行測試，待測物應可持續 336 小時穩定運作。		✓

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. 封包過濾

6.4.1.1.1. 測試環境

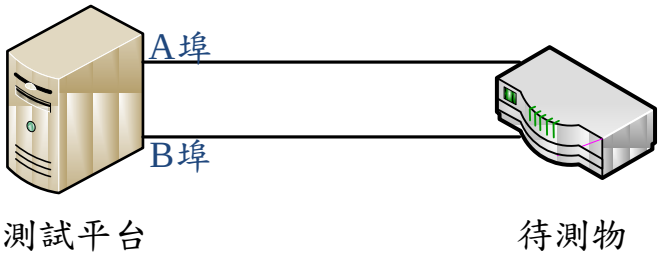

圖 1　封包過濾測試接續圖

(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 1，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) 開啟待測物之封包過濾功能。

(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。

6.4.1.1.2. 測試方法及標準

(1) 使用測試平台自 A 埠產生一來源 IP 位址為特定 IP 的封包，待測物開啟封包過濾功能，B 埠 無法收到測試封包。

(2) 使用測試平台自 A 埠產生一目的 IP 位址為特定 IP 的封包，待測物開啟封包過濾功能，B 埠無法收到測試封包。

(3) 使用測試平台自 A 埠產生一目的 IP 位址為特定 IP 的封包，待

測物關閉封包過濾功能，B 埠收到測試封包。

(4) 使用測試平台自 A 埠產生一目的 IP 位址為特定 IP 的封包，待測物關閉封包過濾功能，B 埠收到測試封包。

6.4.1.2. 流量內容統計

6.4.1.2.1. 測試環境

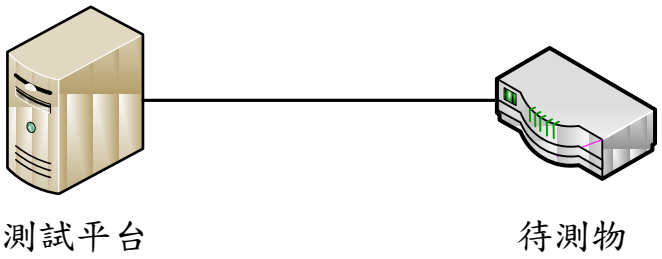

圖 2　流量內容統計測試接續圖

(5) 測試平台：可供測試人員連線至待測物之終端設備。

(6) 網路連接線：乙太網路線或光纖纜線。

(7) 連接待測物、測試平台與網際網路如圖 2。

(4) 開啟待測物之流量統計功能。

6.4.1.2.2. 測試方法及標準

由測試平台產生 1000MB 的網路流量 (包含 IPv4 及 IPv6 之混合流量)通過待測物，待測物的流量統計資訊應正確紀錄該流量。

6.4.1.3. 安全事件紀錄

6.4.1.3.1. 測試環境

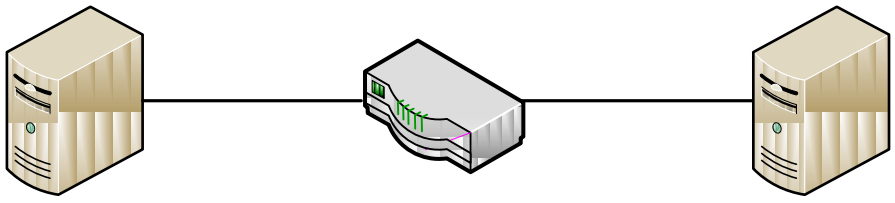

圖 3　安全事件紀錄接續圖

(1) 測試平台 A：可模擬終端使用者之測試儀器或程式。

(2) 測試平台 B：可產生病毒測試樣本並提供網路服務之測試儀器或程式。

(3) 連接待測物、測試平台 A 及測試平台 B 如圖 3。

(4) 開啟待測物之病毒防護及安全記錄功能。

(5) 由測試平台 A 連線至測試程式平台 B 並下載病毒檔案。

6.4.1.3.2. 測試方法及標準

當違反安全事件紀錄的網路流量通過待測物，待測物的流量統計資訊應正確紀錄違反安全規則之事件名稱、時間、來源 IP、目的 IP 及內容。

6.4.1.4. 安全管理功能

6.4.1.4.1. 測試環境 同 6.4.1.3.1.。

6.4.1.4.2. 測試方法及標準

(8) 由測試平台連線至待測物，確認待測物是否需要密碼才可進行設定，待測物應須輸入正確密碼才可進行管理設定。

(9) 嘗試輸入錯誤密碼，待測物是否檢查當超過最大錯誤次數時，會封鎖管理介面一段時間，避免遭受攻擊。

6.4.1.5. 備援管理 (適用進階型)

6.4.1.5.1. 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) 交換集線器 (Switch Hub)：匯集多條通訊纜線之裝置。
(3) 網路連接線：乙太網路線或光纖纜線。
(4) 開啟待測物之備援功能及安全功能。

(5) 連接測試平台、待測物、備援待測物及網際網路如圖 4。

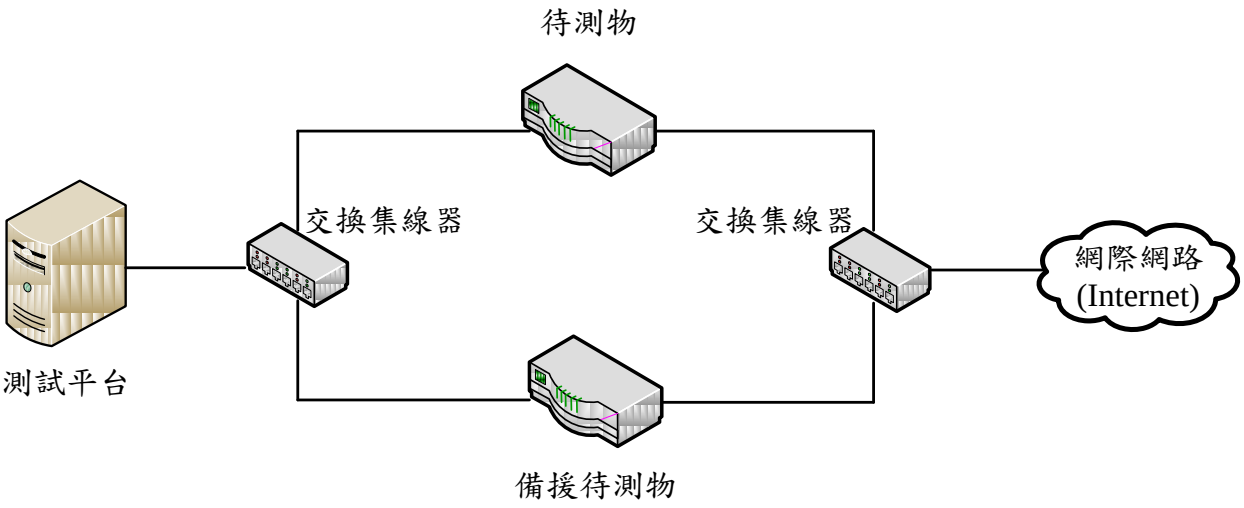

圖 4　備援測試接續圖

6.4.1.5.2. 測試方法及標準

測試平台產生網路流量經待測物傳送至網際網路，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安全功能，確保安全功能仍可正常運作。

6.4.1.6. 流量控管規則 (適用進階型)

6.4.1.6.1. 測試環境 同 6.4.1.2.1.。

6.4.1.6.2. 測試方法及標準

(1) 設定待測物之網路流量通過規則。

(2) 以測試平台產生符合規則之網路流量通過待測物，流量應正常通過待測物。

(3) 以測試平台產生不符合規則的網路流量通過待測物，流量應無法通過待測物。

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 1，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。

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

(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 2。
(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 2。
(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. 測試環境 無

6.4.3.3.2. 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

在一般使用者上線的真實運作之網路，以場測方式進行測試，或是將真實網路流量錄製後，再以重播之方式進行測試，測試環境同 6.4.4.1.1.。

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。

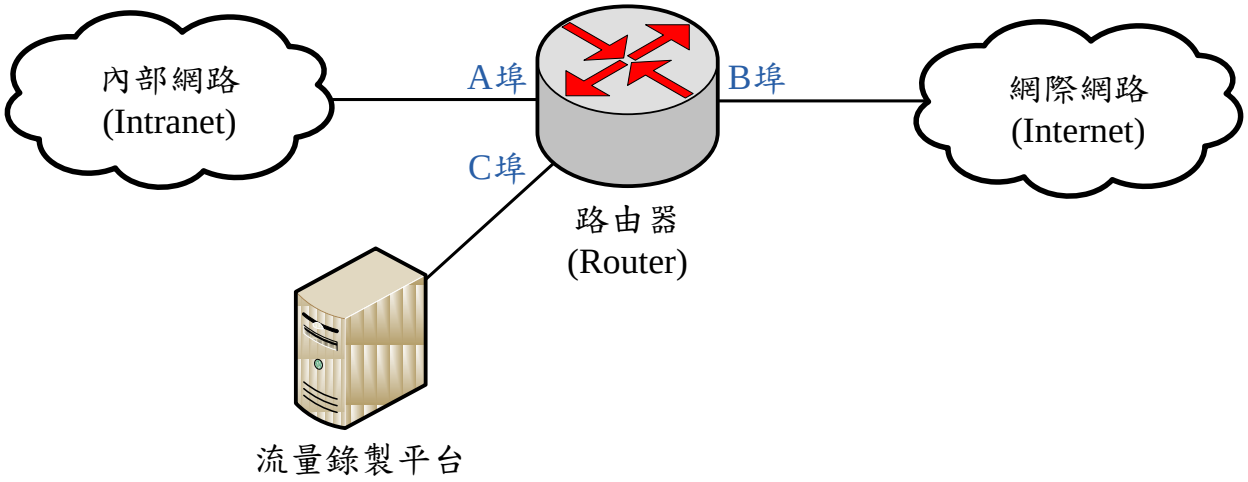

圖 5　流量錄製接續圖

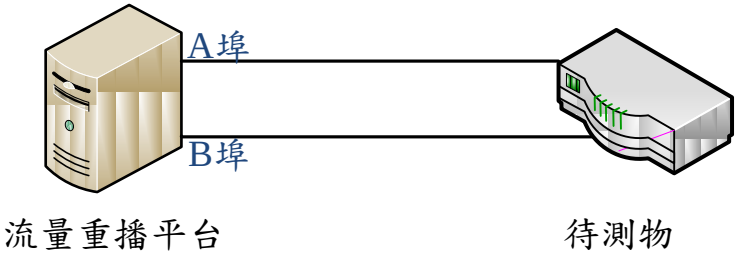

圖 6　流量重播接續圖

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) 流量最大同時連線數量在測試期間需達待測物規格說明處理能力最大值之 50%以上。

(4) 流量最大速度在測試期間需達待測物規格說明處理能力最大值之 50%以上。

(5) 流量內容包含至少 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 protocol, qqtv, pplive, qvod, flashcom, itunes, funshion

H. tps, http proxy

I. Others：sslvpn, nntp protocol, dns protocol, snmp protocol, dhcp protocol, mysql, ntp protocol

J. Web：http, http download, http video, http range get, https, http proxy

(6) 若以重播方式進行測試，所使用之流量必須包含最近 2 周內所錄製之流量。

6.4.4.1.3. 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

附件一、安全功能介面表

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*

附件二、子系統描述與分類表

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: ...*

附件三、安全架構描述表

項目	說明	
1.安全領域 Security Domain	**安全領域名稱**	**安全領域說明**
	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。*

項目	說明	
2.初始程序 Secure Initialization	**相關元件**	**初始程序說明**
	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。*

項目	說明		
3.自我保護 Self-Protection	**自我保護功能**	**與外部設備之關係**	**自我保護機制說明**
	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。*

項目	說明	
4.防止繞道 Non-Bypassibility	**防止繞道功能**	**防止繞道機制說明**
	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。*

附件二

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規範，實機測試標準主要參考 ICSA 與 NSS 等國際實驗室測試標準。

6.1. 書面審查類別

6.1.1. 安全標的

審查待測物之驗證範圍定義及安全功能(TSF)概述。

6.1.2. 安全功能設計

審查待測物之安全功能(TSF)，包含安全功能規格、安全設計、安全架構、安全指引、安全功能測試等說明。

6.2. 書面審查類別之項目及判定標準

應要求申請者依安全等級為基礎型或進階型需要，提供安全標的及安全功能設計類別之相關文件，如表 1。

表1 書面審查類別之項目及判定標準

類別	項目	判定標準	檢附文件	基礎	進階
安全標的	設備類型	詳如附表 1-1	設備之標識標籤、規格書或邏輯示意圖	V	V
	安全功能需求(SFR)	詳如附表 1-2-1	0、0 之資料	V	
		詳如附表 1-2-2			V
安全功能設計	安全功能規格	詳如附表 1-3	0 之資料，說明安全功能(TSF)執行的操作介面、執行方式及預期動作及錯誤訊	V	V

類別	項目	判定標準	檢附文件	基礎	進階
			息。		
	設計安全性	詳如附表 1-4	0 之資料，藉由描述子系統及其行為，以及與 SFR 執行之關係，說明其設計安全性。		V
	安全架構	詳如附表 1-5	0 之資料，針對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(需符合後續提供的指引手冊)。	V	V
	安全指引	詳如附表 1-6	指引文件	V	V

6.2.1. 安全標的

申請廠商提供送驗設備的基本資料、安全功能(TSF)範圍及該設備可執行的安全技術要求安全功能需求(SFR)。

6.2.1.1. 設備類型說明

本項書面審查內容與判定標準說明如附表 1-1：

附表1-1　設備類型之書面審查內容

項目	審查內容	判定標準
設備識別	設備應標示下列內容： 1. 名稱、廠牌、型號及版本 2. 申請者名稱(製造商、代理商) 3. 製造商名稱	檢附之設備標識標籤須符合審查內容
範圍與規格	5. 設備形式(硬體 hardware/韌體	檢附之設備規格書或邏

項目	審查內容	判定標準
	firmware/軟體 software) 6. 安全功能(TSF)之邏輯範圍，應包含安全稽核、密碼支援、用戶資料保護、身分認證/驗證、資料安全管理及安全功能保護。 7. 安全功能(TSF)之實體範圍，應包含安全功能(TSF)執行相關的設施、子系統。	輯示意圖須符合審查內容。

6.2.1.2. 安全功能需求(SFR)

本項書面審查內容將根據廠商所提供的 0 資料（進階設備另需提供 0 資料），檢視安全功能需求(SFR)的之執行內容是否符合附表 1-2-1 與附表 1-2-2 之判定標準：

附表1-2-1　安全功能需求之書面審查內容(基礎型)

項目	審查內容	判定標準
1.安全角色	1. 系統如何進行角色權限控管。 2. 不同的管理者角色各有何管理權限。	系統應維護被授權的管理者角色，並可配置對應的使用者。
2.使用者屬性定義	每位使用者的安全屬性如何個別維護。	設備安全功能(TSF)可提供維護每個使用者安全屬性之能力，安全屬性涵蓋： （1）使用者身份及鑑別資料 （2）被授權的系統角色 （3）其他(自行列舉)

項目	審查內容	判定標準
3.鑑別之時序	於身分鑑別之前後，准許使用者可執行哪些特定動作。	1. 在執行身分鑑別之前，設備安全功能(TSF)可執行的特定動作(自行列舉)。 2. 在執行身分鑑別之後，設備安全功能(TSF)可執行的特定動作(自行列舉)。
4.鑑別失敗處理	如何處理身分鑑別失敗： 1. 當使用者進行登入，設備安全功能(TSF)可偵測出連續鑑別失敗次數。 2. 連續鑑別失敗後，設備安全功能(TSF)鑑別系統應拒絕再次登入，直到採取特殊處置後，使系統回復可登入之狀態。	1. 自行指定 N 值，設備安全功能可偵測出連續鑑別失敗 N 次的能力。 2. 當使用者進行登入，連續鑑別失敗次數達到自行指定 N 值時，設備安全功能(TSF)鑑別系統應拒絕該使用者或外部系統再次登入，須採取特殊處置後，系統才回復可登入之狀態。 3. 定義執行以上安全功能需求(SFR)的介面名稱(需與功能規格對應)。
5.單次使用鑑別機制(Single-use authentication mechanisms)	設備對鑑別資料是否有單次使用鑑別機制	與遠端使用者或設備進行身份鑑別時，傳輸之鑑別資料應只單次使用(如鑑別資料加密、單次性密碼)，避免相關鑑別資料被惡意利用。
6.資料流控	系統是否具備資料	系統需根據以下資料屬性，對資料流進行

項目	審查內容	判定標準
制	流管理功能(如：管控過濾規則之實現功能)。	控制、過濾等管理： （1）來源端位址或其他自行指定之來源格式 （2）目的端位址及其他自行指定之目的格式 （3）應用程式協定 （4）其他(自行指定)
7.靜態屬性的初始化	系統是否具備預設的安全屬性(如預設郵件過濾規則等)	系統應提供垃圾郵件過濾設備預設規則(值)，且系統需允許被授權的管理者，選擇不同的預設規則(值)。
8.安全功能行為的管理	系統是否具備可以管理安全屬性的功能	系統應賦予被授權的管理者，有不同管理功能的使用權限如下： （1）系統啟動與關閉 （2）針對垃圾郵件過濾設備規則進行新增、刪除、修改與檢視 （3）針對使用者屬性進行新增、刪除、修改與檢視 （4）允許或禁止外部設備登入系統進行管理 （5）修改系統日期或時間 （6）備份、建立、刪除、清空或審查稽核紀錄 （7） 其他(自行指定)
9.殘餘資訊保護	垃圾郵件過濾設備在傳送使用者資料	垃圾郵件過濾設備在傳送使用者資料後，應具備避免殘餘資料外洩的功能

項目	審查內容	判定標準
	後是否避免殘餘資料的外洩	
10.密碼操作	系統如何使用密碼演算法保護系統管理之連線	系統需針對遠端管理通道進行加密，並提供採用之演算法，包含演算法所屬標準及其金鑰長度。
11.可靠時戳	系統是否提供可靠的時戳	系統需提供可靠的時戳並用於記錄稽核時間資訊。
12.稽核資料產生	是否依據定義之稽核事件等級產生稽核資料，並記錄於稽核資料庫	1.設備安全功能應提供下列可稽核事件的稽核紀錄： （1）稽核功能的啟動與關閉 （2）系統存取設備 （3）系統資料存取 （4）其他(自行指定) 2.每個稽核紀錄至少應具備下列資訊： （1）事件日期及時間 （2）事件型式 （3）主體識別碼及事件結果(成功或失效)。 3.針對第 1 項(1)~(3)所列舉的稽核事件，進行安全功能需求(SFR)與可稽核事件之對應。
13.稽核審查	設備是否具備審查稽核紀錄的功能	1. 設備安全功能可由被授權的管理者審核稽核紀錄 2. 稽核紀錄需可由人員辨讀

項目	審查內容	判定標準
14.可選取之稽核審查	於審查稽核紀錄時，是否能按條件選取要被審查之稽核資料	設備安全功能應依據以下事項，提供進行排序稽核紀錄的功能： （1）主機地址 （2）事件日期/事件時間 （3）網址範圍
15.稽核資料可用性之保證(Guarantees of audit data availability)	在非期望狀況發生時，設備是否能維護其稽核資料。	1. 設備安全功能應防止儲存的稽核紀錄被非授權使用者刪除 2. 設備安全功能應能保護儲存的稽核紀錄免於被非授權使用者竄改，或者儲存的稽核資料被非授權使用者竄改時能予以偵測。 3. 當系統發生稽核紀錄機制失效時(如：儲存空間已滿、設備故障或遭受攻擊)，設備安全功能應提供機制以維護已經儲存稽核紀錄之可用性。
16.稽核資料漏失之預防	設備如何因應稽核儲存空間耗盡時之狀況	當系統發生稽核紀錄儲存空間耗盡時，設備安全功能需執行下列兩項動作，以維持儲存稽核紀錄之功能： （1）每筆最新的稽核紀錄，必須從最舊的稽核紀錄開始覆蓋 （2）當稽核紀錄儲存空間耗盡時，必須提供系統告警

附表1-2-2　安全功能需求之書面審查內容(進階型)

項目	審查內容	判定標準
1.安全角色	1. 系統如何進行角色權限控管。 2. 不同的管理者角色各有何管理權限。	系統應維護被授權的管理者角色，並可配置對應的使用者。
2.使用者屬性定義	每位使用者的安全屬性如何個別維護。	設備安全功能(TSF)可提供維護每個使用者安全屬性之能力，安全屬性涵蓋： （1）使用者身份及鑑別資料 （2）被授權的系統角色 （3）其他(自行列舉)
3.鑑別之時序	於身分鑑別之前後，准許使用者可執行哪些特定動作。	1. 在執行身分鑑別之前，設備安全功能(TSF)可執行的特定動作(自行列舉)。 2. 在執行身分鑑別之後，設備安全功能(TSF)可執行的特定動作(自行列舉)。
4.鑑別失敗處理	如何處理身分鑑別失敗	1. 當使用者進行登入,設備安全功能(TSF)可偵測出連續鑑別失敗 N 次(自行指定 N 值)的能力。 2. 當使用者進行登入，連續鑑別失敗次數達到 N 次，設備安全功能(TSF)鑑別系統應拒絕該使用者或外部系統再次登入，直到採取特殊處置後，使系統回復可登入之狀態。
5.單次使用鑑別機制(Single-use	設備對鑑別資料是否有單次使用鑑別機制	與遠端使用者或設備進行身份鑑別時，傳輸之鑑別資料應只單次使用(如鑑別資料加密、單次性密碼)，避免相關鑑別資料被

項目	審查內容	判定標準
authentication mechanisms)		惡意利用。
6.資料流控制	系統是否具備資料流管理功能(如：管控過濾規則之實現功能)。	系統需根據以下資料屬性，對資料流進行控制、過濾等管理： （1）來源端位址或其他自行指定之來源格式 （2）目的端位址及其他自行指定之目的格式 （3）應用程式協定 （4）其他(自行指定)
7.靜態屬性的初始化	系統是否具備預設的安全屬性(如預設郵件過濾規則等)	系統應提供垃圾郵件過濾設備預設規則(值)，且系統需允許被授權的管理者，選擇不同的預設規則(值)。
8.安全功能行為的管理	系統是否具備可以管理安全屬性的功能	系統應賦予被授權的管理者，有不同管理功能的使用權限如下： （1）系統啟動與關閉 （2）針對垃圾郵件過濾設備規則進行新增、刪除、修改與檢視 （3）針對使用者屬性進行新增、刪除、修改與檢視 （4）允許或禁止外部設備登入系統進行管理 （5）修改系統日期或時間 （6）備份、建立、刪除、清空或審查

項目	審查內容	判定標準
		稽核紀錄 （7）其他(自行指定)
9.殘餘資訊保護	垃圾郵件過濾設備在傳送使用者資料後是否避免殘餘資料的外洩	垃圾郵件過濾設備在傳送使用者資料後，應具備避免殘餘資料外洩的功能
10.密碼操作	系統如何使用密碼演算法保護系統管理之連線	系統需針對遠端管理通道進行加密，並提供採用之演算法，包含演算法所屬標準及其金鑰長度。
11.可靠時戳	系統是否提供可靠的時戳	系統需提供可靠的時戳並用於記錄稽核時間資訊。
12.稽核資料產生	是否依據定義之稽核事件等級產生稽核資料，並記錄於稽核資料庫	1.設備安全功能應提供下列可稽核事件的稽核紀錄： （1）稽核功能的啟動與關閉 （2）系統存取設備 （3）系統資料存取 （4）其他(自行指定) 2.每個稽核紀錄至少應具備下列資訊： （1）事件日期及時間 （2）事件型式 （3）主體識別碼及事件結果(成功或失效)。 3.針對第 1 項(1)~(3)所列舉的稽核事件，進行安全功能需求(SFR)與可稽核事件之對應。

項目	審查內容	判定標準
13.稽核審查	設備是否具備審查稽核紀錄的功能	1. 設備安全功能可由被授權的管理者審核稽核紀錄 2. 稽核紀錄需可由人員辨讀
14.可選取之稽核審查	於審查稽核紀錄時，是否能按條件選取要被審查之稽核資料	設備安全功能應依據以下事項，提供進行排序稽核紀錄的功能： （1）主機地址 （2）事件日期/事件時間 （3）網址範圍
15.稽核資料可用性之保證(Guarantees of audit data availability)	在非期望狀況發生時，設備是否能維護其稽核資料。	1. 設備安全功能應防止儲存的稽核紀錄被非授權使用者刪除 2. 設備安全功能應能保護儲存的稽核紀錄免於被非授權使用者竄改，或者儲存的稽核資料被非授權使用者竄改時能予以偵測。 3. 當系統發生稽核紀錄機制失效時(如：儲存空間已滿、設備故障或遭受攻擊)，設備安全功能應提供機制以維護已經儲存稽核紀錄之可用性。
16.稽核資料漏失之預防	設備如何因應稽核儲存空間耗盡時之狀況	當系統發生稽核紀錄儲存空間耗盡時，設備安全功能需執行下列兩項動作，以維持儲存稽核紀錄之功能： （1）每筆最新的稽核紀錄，必須從最舊的稽核紀錄開始覆蓋 （2）當稽核紀錄儲存空間耗盡時，必

項目	審查內容	判定標準
		須提供系統告警
17.安全功能資料管理	是否准許被授權的使用者管理設備之安全功能資料。	設備安全功能(TSF)應限制由被授權使用者角色來執行以下功能： （1）查詢/新增系統與稽核資料 （2）查詢/修改其他安全屬性資料
18. 額外提供之安全技術	由廠商自行定義，如系統提供備援、策略控管等其他安全功能	設備安全功能實作之描述

6.2.2. 安全功能設計

申請廠商應提出安全功能需求(SFR)執行的設計文件、功能規格、安全架構、指引文件等資料供書面審查，以確保設備的安全功能(TSF)在特定的條件下能正確執行。

本項書面審查應提供以下設計文件：

6.2.2.1. 安全功能規格

應描述安全功能介面(TSFI)規格及安全功能(TSF)如何處理使用者所請求的服務。

功能規格內容需與前列的安全技術功能要求對應，並能和之後所需提供的設計安全性、安全架構及安全指引手冊的內容相符。

本項書面審查內容與判定標準說明如附表 1-3：

附表1-3 安全功能規格之書面審查內容

等級	審查內容	判定標準
基礎	提供資料應包含下列審查項目： (1)安全功能介面(TSFI)之目標與使用方法。 (2)每個安全功能介面(TSFI)與安全功能(TSF)有關的參數設定。 (3)針對安全功能介面(TSFI)，描述執行安全功能(TSF)的動作。 (4)針對安全功能介面(TSFI)，描述執行安全功能(TSF)動作所導致的直接錯誤訊息。 (5)所有安全功能需求(SFR)均能被安全功能介面(TSFI)完整實現。	需提供 0 資料，說明安全功能(TSF)執行的操作介面、執行方式及預期動作及錯誤訊息。
進階	提供資料除需包含基礎型內容外，並應提供以下訊息： (1)列出所有安全功能介面(TSFI)的參數 (2)描述每個安全功能介面(TSFI)的所有動作。 (3)功能規格應描述每個安全功能介面(TSFI)預期應有的安全執行結果與例外處理可能導致的所有直接錯誤訊息。	需提供 0 資料，說明安全功能介面(TSFI)的所有預期動作及錯誤訊息。

6.2.2.2. 設計安全性

本節適用於進階型設備驗證，依安全功能規格所對應的功能子系統(Subsystem)，提供以下訊息：

(1)子系統(列表)

(2)子系統的行為類型：

A.執行 SFR

B.支援 SFR

C.非涉 SFR

這些行為的敘述須與 6.2.2.1 的方式相同。

(3)子系統的行為描述應符合安全功能需求，包含以下內容：

A.所有安全功能運作的資訊。

B.與其他子系統間互動之資訊，該資訊足以識別不同子系統間的溝通以及傳遞資料的特性。

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

審查內容	判定標準
提供資料應包含下列審查項目： (1)應識別所有的安全功能(TSF)子系統。 (2)應描述每個子系統中屬於執行 SFR、支援 SFR 或非涉 SFR 的行為。 (3)應描述執行安全功能(TSF)子系統與其它子系統間的介面與溝通行為。 (4)所有行為均能對應到 6.2.2.1 安全功能規格中的介面。	需提供 0 資料，藉由描述子系統及其行為，以及與 SFR 執行之關係，說明其設計安全性。

6.2.2.3. 安全架構

安全架構分析應依據6.2.2.1安全功能規格及6.2.2.2設計安全性(進階型設備)之檢附文件，說明該設備能達成所描述的安全功能需求(SFR)。安全架構分析也將作為實機測試項目設計的參考。

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

審查內容	判定標準
提供資料應包含下列審查項目： (1)說明設備因執行安全功能(TSF)所區隔的安全領域。 (2)應描述各項安全功能(TSF)的安全初始程序。 (3)應描述各項安全功能(TSF)的自我保護機制。 (4)應描述安全功能(TSF)執行如何避免被繞道。	需提供 0 資料，針對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（需符合後續提供的指引手冊)。

6.2.2.4. 安全指引

內容須包括設備安全處理之訊息，以及人為疏失下可能造成錯誤的設定與作業程序。

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

審查內容	判定標準
提供資料應包含下列審查項目： (1)應定義可能的使用者角色。 (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. 可用的介面 C. 安全參數定義 D. 產生的安全事件 E. 應遵循的安全措施 (3)應描述於特殊權限操作時的安全環境要求，並提供適當的警告。 (4)應列舉設備操作時的所有運作模式。 (5)應列舉設備作業失敗(Failure)或人員操作錯誤產生的各種情況及處理方式。	1.指引文件內容中之介面、參數是否符合 6.2.2.1 的功能規格。 2.需提供設備使用時所需的安全環境，包括人員、實體、溝通等條件。 3.指引文件將做為實機測試的依據。

審查內容	判定標準
(6)應描述設備運作前的安全準備作業，包含設備安裝及啟動。 (7)應描述設備操作的安全環境設置，應包括以下項目： A. 設備使用目的(如針對使用者郵件進行過濾等) B. 實體環境安全(如設備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設備等) D. 連接安全(如設備與其他網路伺服器之連線安全等)	

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、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

測試待測物於面臨大量受測信件與連線時安全功能是否有受影響。

6.3.3. 堅實測試

測試待測物於開啟服務或協定的情況下，是否能夠處理不正常的連線行為，仍保持正常運作而不受影響。

6.3.4. 穩定測試

將待測物置於真實網路流量下運作測試，了解待測物在真實的網路流量下是否有不穩定的狀況發生。

6.4. 實機測試類別之項目及判定標準

實機測試分為基礎型與進階型，每個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 實機測試類別之項目及判定標準

類別	項目	判定標準	備註	基礎	進階
安全功能測試	郵件過濾	1.垃圾郵件應依規則被過濾，漏判率應低於 5% 2.正常郵件應依規則通過，誤判率應低於 0.008%	亦應符合附表 1-2-1、附表 1-2-2 之項目 6	V	
		1.垃圾郵件應依規則被過濾，漏判率應低於 3% 2.正常郵件應依規則通過，誤判率應低於 0.004%			V
	郵件內容反釣魚網址過濾	具備過濾郵件裡含有釣魚網址之功能			
	安全事件紀錄	應正確記錄違反安全規則的事件，包含時間與內容(來源/目的 IP、事件等)	亦應符合附表 1-2-1、附表 1-2-2 之項目 12、13、14、15、16	V	V
	安全管理	1. 具備通行碼管理 2.具備通行碼輸入錯誤次數之上限設定，超過上限次數後須封鎖管理介面一段時間。	亦應符合附表 1-2-1、附表 1-2-2 之項目 3、4	V	V
壓力	吞吐量	設備所負荷的吞吐量(Mbps		V	V

類別	項目	判定標準	備註	基礎	進階
測試		或 Gbps)達到設備規格說明之最大吞吐量時，安全功能應正常運作。			
	最大同時連線數	設備所負荷的同時連線數(TCP 連線數)達到設備規格說明之最大同時連線數時，安全功能應正常運作。			V
	最大建立連線速率	設備所負荷的連線建立速率(TCP 連線數/秒)達到設備規格說明之最大連線建立速率時，安全功能應正常運作。			V
堅實測試	阻斷式攻擊	攻擊發生時不應發生當機或重新啟動等情況，待攻擊結束後安全功能應正常運作。		V	V
	惡意流量	應可承受針對設備本身各項服務的惡意行為			V
	非正常關機復原	非正常關機後，應可於開機時恢復關機前之正常運作狀態		V	V
穩定測試	真實流量測試	與實際網路連線時，應可持續 168 小時正常運作。		V	
		與實際網路連線時，應可持續 336 小時正常運作。			V

6.4.1. 安全功能測試

6.4.1.1. 郵件過濾

6.4.1.1.1. 測試環境

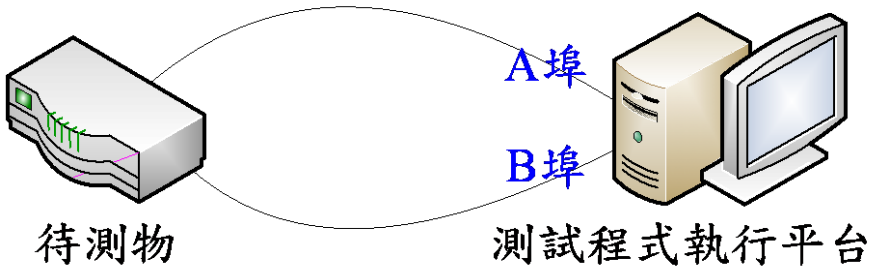

圖1　郵件過濾測試環境

6.4.1.1.2. 測試組態

(10)設定啟用垃圾郵件過濾功能。

(11)參數設定

A. 垃圾郵件數量：50,000。

B. 正常郵件數量：5,000。

6.4.1.1.3. 測試方法及標準

(12)開啟待測物規則，使用測試程式執行平台自 A 埠寄送或下載垃圾郵件，垃圾郵件應被阻擋、過濾、標記或紀錄。

(13)在啟用垃圾郵件過濾功能的狀況下，使用測試程式執行平台自 A 埠寄送或下載正常郵件，正常郵件不應被阻擋、過濾、標記或紀錄。

(14)垃圾郵件的漏判率(FNR)應小於 5%(基礎型)或 3%(進階型)。

(15)正常郵件的誤判率(FPR)應低於 0.008%(基礎型)或 0.004%(進階型)。

6.4.1.2. 郵件內容反釣魚網址過濾(進階等級)

6.4.1.2.1. 測試環境 同圖 1。

6.4.1.2.2. 測試組態

(16)啟用待測物郵件內容反釣魚網址過濾功能。

(17)參數設定

測試程式執行平台 A 透過 SMTP 通訊協定，寄出各類型惡意網址之網站連結，通過待測物後這類信件應被阻擋或過濾掉。

6.4.1.2.3. 測試方法及標準

由測試程式執行平台 A 透過 SMTP 通訊協定接放含有釣魚網址的郵件，待測物應過濾掉含有釣魚網站連結的惡意釣魚郵件，避免使用者因此而洩漏個人資訊或造成其它安全相關的危害。

6.4.1.3. 安全事件紀錄

6.4.1.3.1. 測試環境 同圖 1。

6.4.1.3.2. 測試組態

(1) 啟用待測物安全事件紀錄功能。透過待測物提供的 Web GUI 管理介面或 Console 管理介面進入待測物，找到待測物安全事件紀錄功能的對應設定位置，將待測物安全事件紀錄功能開啟。

(2) 參數設定

A.待測物參數：開啟垃圾郵件過濾功能。

B.流量產生參數：使用測試程式執行平台寄送垃圾郵件。

6.4.1.3.3. 測試方法及標準

由測試程式執行平台產生違反安全事件紀錄的流量通過待測物，待測物的流量統計資訊應正確紀錄違反安全事件紀錄發生的時間與內容。

6.4.1.4. 安全管理

6.4.1.4.1. 測試環境 同圖 1。

6.4.1.4.2. 測試組態 無。

6.4.1.4.3. 測試方法及標準

(18)由測試程式執行平台連線至待測物，確認待測物是否需要通行碼才可進行設定，待測物應須通行碼才可進行管理設定。

(19)嘗試輸入錯誤通行碼，檢查當超過最大錯誤次數時，待測物是否會封鎖管理介面一段時間，超過最大錯誤次數後待測物應封鎖管理介面一段時間，避免遭受攻擊。

6.4.2. 壓力測試

6.4.2.1. 吞吐量

6.4.2.1.1. 測試環境 同圖 1。

6.4.2.1.2. 測試組態

(20)開啟待測物之安全功能。

(21)參數設定

封包大小：64~1518 位元組。

6.4.2.1.3. 測試方法及標準

測試程式執行平台自 A 埠產生各種封包大小的流量送往 B 埠，過程中不能發生封包遺失，當待測物所負荷的吞吐量達到其規格說明之最大值時，其安全功能應能正常運作。

6.4.2.2. 最大同時連線數

6.4.2.2.1. 測試環境 同圖 1。

6.4.2.2.2. 測試組態

開啟待測物之安全功能。

6.4.2.2.3. 測試方法及標準

測試程式執行平台自 A 埠每秒建立一條 TCP 連線至 B 埠，過程中所有 TCP 連線皆建立成功且維持不斷線，當待測物所負荷的同時 TCP 連線數達到其規格說明之最大值時，其安全功能應能正常運作。

6.4.2.3. 最大連線建立速率

6.4.2.3.1. 測試環境 同圖 1。

6.4.2.3.2. 測試組態

開啟待測物之安全功能。

6.4.2.3.3. 測試方法及標準

測試程式執行平台自 A 埠建立 TCP 連線至 B 埠，過程中所有 TCP 連線皆建立成功且維持不斷線，TCP 連線建立速率持續加快直到待測物所負荷的 TCP 連線建立速率達到其規格說明之最大值時，其安全功能應能正常運作。

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

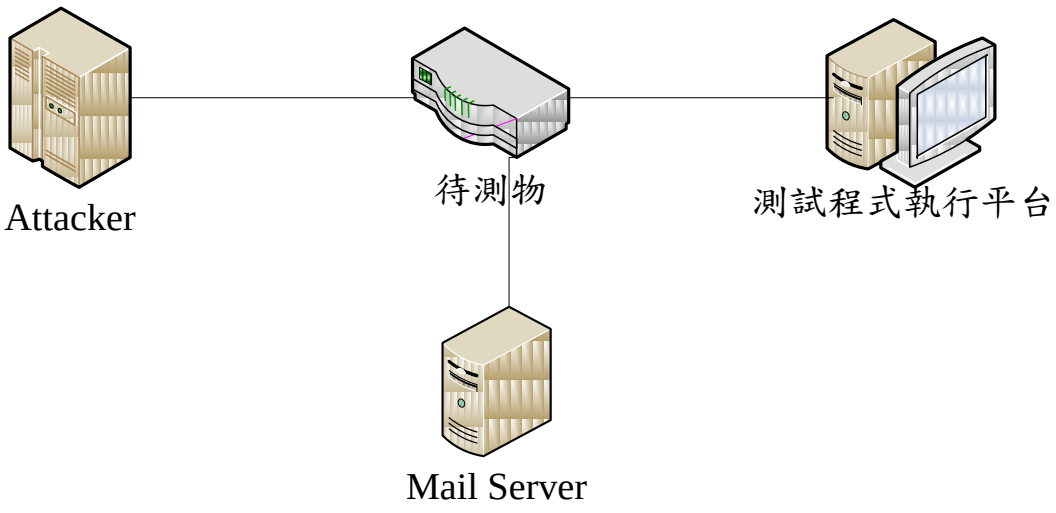

圖2　阻斷式攻擊測試網路拓樸

6.4.3.1.2. 測試組態

針對待測物提供服務的連接埠發動 SMTP flood 攻擊。

6.4.3.1.3. 測試方法及標準

自攻擊端分次依序各別送出大量 SMTP Request(Flag)的封包，送往待測物有開啟服務的連接埠。攻擊發生時待測物不應發生當機或重新啟動等情況，待攻擊行為結束後，由待測物測試程式存取待測物及郵件伺服器上所提供的服務，應能正常提供服務。

6.4.3.2. 惡意流量防禦

6.4.3.2.1. 測試環境

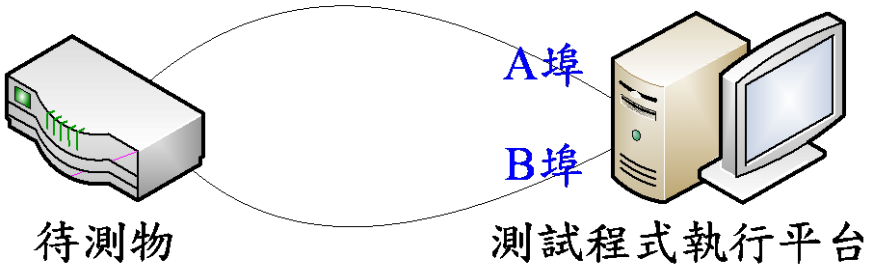

圖3　惡意流量防禦測試環境

6.4.3.2.2. 測試組態

啟用待測物遠端管理功能。透過待測物提供的 Console 管理介面進入待測物進行設定，開啟待測物 Web、Telnet 或 SSH 的管理功能。

6.4.3.2.3. 測試方法及標準

根據待測物所提供的遠端管理功能，選擇對應的服務攻擊程式(如待測物提供 Web 服務，則使用 HTTP 攻擊程式)，從外部網路對待測物

施加各項服務攻擊流量(如 HTTP 緩衝區溢位)，嘗試繞過待測物的通行碼保護取得管理權限，各項攻擊流量應無法順利取得待測物之管理權限，此外待測物各項服務應正常運作。

6.4.3.3. 非正常關機

6.4.3.3.1. 測試環境 無。

6.4.3.3.2. 測試組態 無。

6.4.3.3.3. 測試方法及標準

於待測物運作期間不正常移除電源，待測物於重新啟動後，應可正常恢復到失去電源前的最後正常狀態。

6.4.4. 穩定測試

6.4.4.1. 真實流量測試

6.4.4.1.1. 測試環境

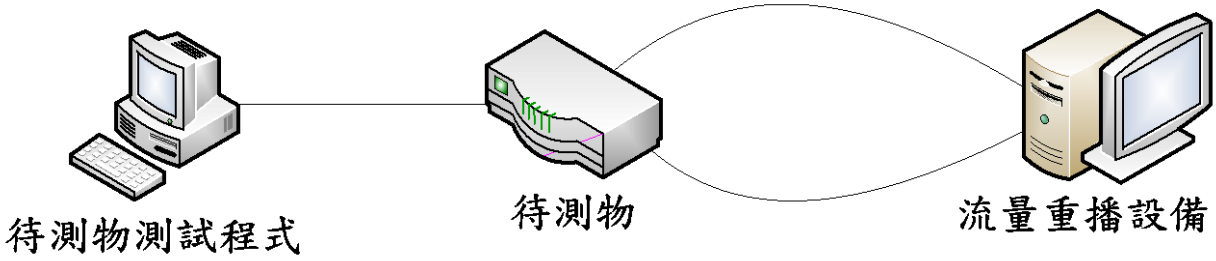

圖4 真實流量測試網路拓樸(重播方式)

6.4.4.1.2. 測試組態

(1) 啟用待測物規則。

(2) 參數設定

A. 流量產生自至少 100 位使用者同時上線的網路環境

B. 流量最大同時連線數量應至少達 10,000 條，平均同時連線數量應至少達 3,000 條，並可依待測物規格進行調整。

C. 流量最大速度應至少達100Mbps，平均速度至少達30Mbps，並可依待測物規格進行調整。

D. 流量內容包含至少 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, icq, qq
b. Email：gmail, hotmail, smtp protocol, pop3 protocol, imap protocol
c. File Transfer：ftp protocol, flashget, smb protocol
d. Game：garena, ms-directplay, facebook app
e. P2P：bittorrent protocol, edonkey, xunlei, fs2you, ed2k, ares, emule
f. Remote Access：windows remote desktop, telnet protocol, ssh protocol, vnc, Hamachi
g. Streaming：rtsp protocol, qqtv, pplive, qvod, flashcom, itunes, funshion
h. VoIP：skpye, skypeout, sip protocol
i. Web：http, http download, http video, http range get, https, http proxy
j. Others：sslvpn, nntp protocol, dns protocol, snmp protocol, dhcp protocol, mysql, ntp protocol

E. 流量內容包含 IPv4 及 IPv6。

F. 以重播方式進行測試所使用之流量其被錄製下來時的時間點與進行測試時的時間點兩者間隔不得超過 1 周

6.4.4.1.3. 測試方法及標準

透過場測(Field Trial)或是流量錄製與重播工具將流量導入待測物進

行測試，測試過程持續檢查待測物的網路是否暢通、網頁圖形使用者介面(Web GUI)設定功能是否可用、待測物沒有發生任何網路中斷或服務停止等狀況。

(1) 基礎型待測物需通過連續 168 小時的測試。

(2) 進階型待測物需通過連續 336 小時的測試。

附件 1 安全功能介面表

功能介面 TSFI	目的 Purpose	可執行的安全功能需求 SFR	操作方式 Method of Use	參數 Parameter	執行動作 Actions	錯誤訊息 Error Message
				基礎型填寫說明： *需提供此介面與安全功能相關之參數(內容應與指引文件相符)* *進階型填寫說明：* *需提供此介面的所有參數(內容應與指引文件相符)*	*基礎型填寫說明：* *需提供此介面與 SFR 的預期動作(內容應與設計文件對應)* *進階型填寫說明：* *需提供此介面的所有預期動作，包括非執行 SFR 的動作(內容應與設計文件對應)*	*基礎型填寫說明：* *需提供此介面與安全功能相關的錯誤訊息(內容應與指引文件相符)* *進階型填寫說明：* *需提供此介面的所有可能的錯誤訊息(內容應與指引文件相符)*

附件 2 子系統描述與分類表

名稱	子系統與 SFR 之對應			行為描述
	執行	支援	非涉	
				填寫說明： *需提供子系統行為資料如次：* *1.TSFI(須與 6.2.2.1 相符)* *2.描述與其他子系統之互動* *3.如為非涉，需敘明與安全功能無關之理由*
範例： Subsystem Audit		14.可選取之稽核審查		1.TSFI: TSFI_WebGUI, TSFI_CLI 2.與其他子系統之互動： (1) 從操作界面子系統獲得稽核紀錄選取條件 (2) 操作界面子系統回覆稽核紀錄選取條件參數

附件 3 安全架構描述表

項目	描述	
1.安全領域 Security Domain	**安全功能**	**領域說明**
	安全稽核	
	密碼支援	
	身分認驗證	
	資料安全管理	
填寫說明		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：安全稽核		安全稽核透過 TSFI_GUI 來執行，該 TSFI 同一時間只能執行單一功能之資料處理請求。
2.初始程序 Secure Initialization	**相關元件**	**程序說明**
填寫說明	操作設備的相關元件/環境	提供安全啟動該設備之相關元件起始步驟及安裝程序。
範例：	垃圾郵件過濾設備安裝	1.安裝於 Firewall 管轄之信任網路 2. 調整 Firewall 之 SMTP 導向與 DNS MX 設定

項目	描述		
		3. 設定預設條件，將預設條件納入政策中，篩選出要套用政策的郵件 4. 針對這些被篩選出的郵件執行動作以及附加動作	
3.自我保護 Self-Protection	**安全功能**	**與外部設備之介面**	**保護機制**
	安全稽核		
	身分認驗證		
	密碼支援		
	資料安全管理		
填寫說明		安全功能及其介面與外部設備之資料交換動作	需檢視介面是否提供實體上或邏輯上的保護機制，諸如： 1.通行碼保護 2.資料傳輸機制 3.特殊執行方式 4.特殊設備需求
範例：身分認驗證		以網路連結外部弱點資料庫、以TSFI_WEBGUI 介面進行身分認驗證	1.應輸入通行碼才能進入介面 2.資料傳輸機制：SSL 3.特殊執行方式：指紋辨識 4.特殊設備需求：指紋辨識器

項目	描述	
4.防止繞道攻擊 Bypass	**安全功能**	**防護機制**
	安全稽核	
	身分認驗證	
	密碼支援	
	資料安全管理	
填寫說明	1.列舉繞道攻擊之手法 2.說明防範作法，諸如：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：身分證驗證	以實體封鎖方式，防止利用維護介面繞道身分認證程序。	