

防毒閘道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，爰修訂防毒閘道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。

防毒閘道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 防毒閘道設備 (Anti-Virus Gateway) 用於偵測與防護電腦病毒、蠕蟲及特洛伊木馬等惡意程式。	1.概說 防毒閘道器(Anti-Virus Gateway)使用於偵測與防護病毒、蠕蟲和特洛伊木馬等惡意程式。<u>並整合監控識別、自動升級或資料恢復等功能。</u>	酌作文字修正。
2. 適用範圍 本規範適用於硬體架構，提供 URL 過濾功能亦可對電子郵件病毒、間諜程式及檔案型電腦病毒進行即時阻絕、警告通知或隔離。<u>本規範不適用安裝於電腦主機之防毒軟體。</u>	2.適用範圍 本規範適用於硬體架構，提供 URL 過濾、<u>監控、網頁病毒</u>，郵件病毒，間諜程式及檔案病毒的即時阻絕，警告通知及隔離。<u>不適用安裝於電腦主機之防毒軟體。</u>	酌作文字修正，明確說明設備之適用範圍。
3. 安全等級 本規範適用基礎型 (Basic) 與進階型 (Advanced) 之防毒閘道設備。 3.1. 基礎型防毒閘道設備 <u>基礎型設備安全功能測試項目包括病毒偵測、線上更新、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。</u> 3.2. 進階型防毒閘道設備 <u>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病毒偵測、運作模式切換及惡意網址過濾等；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流量長時間測試。</u>	3. 安全等級 本規範適用基礎等級(Basic)與進階等級(Advanced)之防毒閘道器，<u>進階等級之防毒閘道器有比基礎等級更加嚴格的技术要求。</u> 3.1. 基礎等級防毒閘道器 <u>指具有如偵測病毒、蠕蟲、釣魚程式、木馬程式、隱形程式線上更新、安全事件紀錄、安全管理功能等安全功能之防毒閘道器。</u> 3.2. 進階等級防毒閘道器 <u>指具有基礎等級防毒閘道器安全功能外，須有惡意網址過濾、運作模式管理等安全功能與需求。</u>	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。
4. 參考標準 ISO/IEC 15408 共同準則(Common Criteria for Information Technology Security Evaluation, CC)	4. 參考標準 ISO/IEC 15408 共同準則(Common Criteria for Information Technology Security Evaluation, CC)	未修正

修正規定	現行條文	說明
ICSA Gateway Anti-Virus V 4.1 NSS UTM-Methodology-v2.0	ICSA Gateway Anti-Virus V 4.1 NSS UTM-Methodology-v2.0	
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 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. 用語釋義 5.1. 防毒閘道器 指在網路上以獨立硬體運作之防毒系統，不同於安裝在個人電腦上本機端防毒軟體。 5.2. 角色(Role) 指一組預先定義的規則，用來建立操作者與送驗設備使用權限的關係。 5.3. 安全領域(Security Domain) 指一個主動式個體(包括人、機器)被授權存取的資源集合，為安全架構的屬性之一。 5.4. 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。 5.5. 繞道(Bypass) 指以非安全功能之方式去執行設備安全功能需求(SFR)的動作。(例如：未經過身分鑑別，直接進入稽核功能介面) 5.6. 病毒程式 指能自我複製及執行的電腦程式，導致受感染電腦無法正常運作。 5.7. 蠕蟲程式 指一種能夠自我複製的電腦程式，其不須附在其他程式內，且不須使用者操作也能自我複製或執行，並可發動分散式阻斷服務攻擊，影響其他電腦的正常使用。 5.8. 特洛伊木馬 指一種後門程式，駭客可透過此類型程式用來盜取其他使用者的個人資料，或從遠端控制他人電腦。 5.9. 釣魚程式 指駭客於偽造網站中置入該程式，目的是誘導使用者在該網站輸入個人資	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
<u>5.7. 角色 (Role)</u> 指預先定義之規則，<u>以描述使用者與待測物間的操作權限。</u> <u>5.8. 指引文件 (Guidance Documentation)</u> 指描述待測物之遞送、安裝、運作、管理及使用等相關文件。 <u>5.9. 安全功能介面 (TOE Security Functions Interface, TSFI)</u> 為評估標的 (TOE) 用於實現安全功能需求 (SFR) 之對外溝通介面。 <u>5.10. 安全領域 (Security Domain)</u> 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。 <u>5.11. 自我保護 (Self-Protection)</u> 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。 <u>5.12. 繞道 (Bypass)</u> 指<u>避開待測物安全功能檢查之技巧。</u> (如：未經過身分鑑別，直接進入稽核功能介面)。 <u>5.13. 最大同時連線數</u> 指待測物能同時處理之 TCP 連線數最大值。 <u>5.14. 吞吐量 (Throughput)</u> 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)。 <u>5.15. 最大連線建立速度</u> 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」。 <u>5.16. 防毒閘道設備</u> 指在網路上以獨立硬體運作之防毒系統，不同於安裝在個人電腦上本機端之防毒軟體。	料。 <u>5.10. 隱形程式(Rootkit)</u> 隱藏惡意行程的軟體，進而竊取電腦資料不被發現。 <u>5.18. 安全功能介面 (TOE Security Functions Interface, TSFI)</u> 為評估標的(TOE)用於實現安全功能需求(SFR)之對外溝通介面。 <u>5.11. 共同準則(Common Criteria for Information Technology Security Evaluation, CC)</u> 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、檢測實驗室與驗證機關(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 <u>5.12. 防毒系統保護剖繪(US Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments)</u> 指美國政府機關採購防毒系統之設備技術參考指引。 <u>5.13. 評估標的(Target Of Evaluation, TOE)</u> 指申請評估及驗證之產品及其相關使用手冊。 <u>5.14. 保護剖繪(Protection Profile, PP)</u> 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。 <u>5.15. 安全標的(Security Target, ST)</u> 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。 <u>5.16. 安全功能(TOE Security Functions, TSF)</u>	

修正規定	現行條文	說明
5.17. <u>電腦病毒 (Computer Virus)</u> 指能自我複製及執行的電腦程式，導致受感染電腦無法正常運作。 5.18. <u>蠕蟲病毒 (Computer Worm)</u> 指一種能夠自我複製的電腦程式，其不須依附其他程式，且不須使用者操作也能自我複製或執行，並可發動分散式阻斷服務攻擊，影響其他電腦的正常使用。 5.19. <u>特洛伊木馬 (Trojan Horse)</u> 指一種特定的後門程式，駭客可透過此類型之程式來盜取其他使用者的個人資料，或從遠端控制<u>受害電腦</u>。 5.20. <u>釣魚程式 (Phishing)</u> 指駭客於偽造網站中誘導使用者在該網站輸入個人資料之<u>程式</u>。 5.21. <u>隱形程式 (Rootkit)</u> 隱藏惡意行程的軟體，進而竊取電腦資料不被發現。 5.22. <u>防毒系統保護剖繪(US Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments)</u> 指美國政府機關採購防毒系統之設備技術參考指引。 5.23. <u>漏判 (False Negative)</u> <u>指待測物對網路攻擊行為應能判定而未判定。</u> 5.24. <u>誤判 (False Positive)</u> <u>指待測物對非網路攻擊行為判定為攻擊行為。</u>	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。 5.17. 安全功能需求(Security Functional Requirement, SFR) 指<u>為定義於共同準則第二部(Common Criteria, Part 2)的安全相關需求條文</u>，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。	
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

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	✓	✓
	安全功能需求	附表 1-2	設備規格說明書	✓	✓
安全功能設計	安全功能規格	附表 1-3	0 安全功能規格表	✓	✓
	設計安全性	附表 1-4	0 設計安全性表		✓
	安全架構	附表 1-5	0安全架構表		✓
	安全指引	附表 1-6	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（附表 1-2）。

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
安全標準的	安全功能需求	1.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。 B. 事件日期及時間。 C. 事件類型 D. 事件成功或失敗	✓	✓
		2.使用者身分關聯	安全功能應能將每個可稽核事件與引發該事件之使用者進行關聯。	✓	✓
		3.稽核審查	安全功能應具備以下稽核審查： (1) 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	✓	✓
		4.受限制之稽核審查	安全功能應禁止未經授權使用者瀏覽稽核紀錄。	✓	✓
		5.可選取之稽核審查	安全功能應具備以下可選取之稽核審查： (1) 事件日期與時間 (2) 事件類型 (3) 主體識別碼	✓	✓
		6.稽核資料	設備安全功能應防止非授權人員透過安全功能介	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		儲存保護	面竄改或刪除稽核資料。		
		7.稽核資料漏失之預防	當系統發生稽核紀錄儲存空間耗盡時，除提供系統告警外，安全功能應具備以下可選取之稽核資料漏失之預防，以維持儲存稽核紀錄之功能： (1) 忽略新增之系統資料 (2) 保護被授權使用者所選擇的系統資料 (3) 每筆最新的系統資料必須從最舊的系統資料開始覆蓋 (4) 告警管理者儲存空間剩餘使用時間 (5) 告警管理者儲存空間剩餘可記錄筆數 (6) 告警管理者儲存空間剩餘百分比	✓	✓
		8.防毒措施	安全功能應具備以下防毒措施： (1) 清除病毒 (2) 隔離病毒 (3) 監控企圖透過遠端 TCP、UDP 或 SMTP 協定進行非授權之程序	✓	✓
		9.防毒告警	安全功能應具備以下防毒告警： (1) 偵測到病毒時，應發出警示訊息，內容應包含病毒資訊與處置措施 (2) 應持續提供警示訊息，直到使用者與管理者有所回應	✓	✓
		10.密碼操作	安全功能應提供演算法產生簽章，包含演算法所屬標準及其金鑰長度，以確保病毒特徵檔之完整性。	✓	✓
		11.安全功能行為的管理	安全功能應具備以下安全功能行為的管理： (1) 稽核 (2) 即時病毒偵測	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		12.安全功能資料管理	安全功能應具備以下安全功能資料管理，提供管理者設定查詢、更改或刪除下列事項： (1) 病毒被偵測後所需進行的動作 (2) 病毒特徵檔 (3) 稽核紀錄	✓	✓
		13.管理功能規格	安全功能應具備以下管理功能規格： (1) 設定偵測功能啟用或關閉 (2) 設定運作模式 (3) 更新病毒碼 (4) 回應警示訊息 (5) 瀏覽稽核紀錄	✓	✓
		14.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) 經授權的系統管理者 (3) 其他（自行列舉）	✓	✓

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	✓	✓

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	設計安全	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：	／	✓

類別	項目	審查標準	基礎型	進階型
設計	性	(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 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	✓	✓

類別	項目	審查標準	基礎型	進階型
		(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	病毒偵測	1. 漏判測試： 依 6.4.1.1.3. (1) 進行測試，漏判率須小於 5%。	✓	
		2. 誤判測試： 依 6.4.1.1.3. (2) 進行測試，不可發生誤判。		
		1. 漏判測試： 依 6.4.1.1.3. (1) 進行測試，漏判率亦須小於 3%。		✓
		2. 誤判測試： 依 6.4.1.1.3. (2) 進行測試，不可發生誤判。		
	線上更新	依 6.4.1.2.2. 進行測試，應可透過網路進行線上更新特徵碼資料。	✓	✓
	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	✓	✓

類別	項目	判定標準	基礎	進階
		管理介面一段時間。		
	運作模式 切換	依 6.4.1.5.2. 進行測試，具備可切換運作模式 (路由模式或透通橋接模式)。		✓
	惡意網址 過濾	依 6.4.1.6.2. 進行測試，具備過濾惡意網址之功能。		✓
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。	✓	✓
	最大同時 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。		✓
	最大連線 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 機復原	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 測試	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		✓

類別	項目	判定標準	基礎	進階
		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. 病毒偵測

6.4.1.1.1. 測試環境

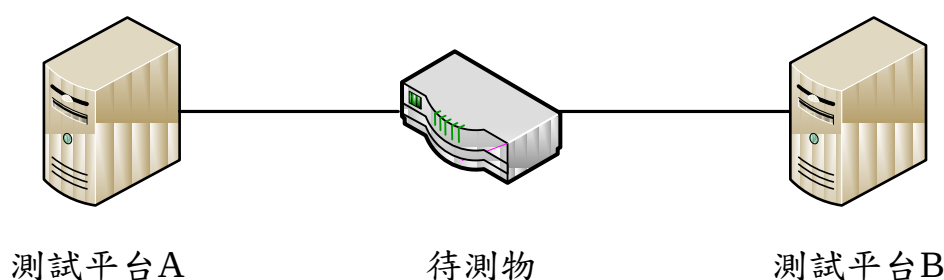


圖1 病毒偵測接續圖

- (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) 網路連接線：乙太網路線或光纖纜線。
- (4) 連接測試平台 A、待測物及測試平台 B 如圖 1。
- (5) 開啟待測物支援通訊協定（如 HTTP、FTP、SMTP、POP3 及 IMAP 等）之掃毒功能。

6.4.1.1.2. 測試樣本

A. 病毒測試樣本

- (a) 基礎型測試樣本：自國家通訊傳播委員會病毒樣本資料庫擷取待測物送測前一個月公告之病毒清單為測試樣本。
- (b) 進階型測試樣本：自國家通訊傳播委員會病毒樣本資料庫

擷取待測物送測前一個月至前三個月公告之病毒清單為測試樣本。

B. 無病毒測試樣本

以測試儀器或程式產生無病毒之測試樣本，樣本數量至少五千筆。

6.4.1.1.3. 測試方法及標準

(6) 漏判測試方法及標準

分別開啟 HTTP、FTP、SMTP、POP3 及 IMAP 通訊協定情況下，測試平台 A 模擬使用者經由待測物，連上測試平台 B，存取對應通訊協定之服務，並下載病毒測試檔案。基礎型待測物對於基礎型病毒測試樣本之漏判率須小於 5%；進階型待測物對於進階型病毒測試樣本之漏判率亦須小於 3%。

(7) 誤判測試方法及標準

分別開啟 HTTP、FTP、SMTP、POP3 及 IMAP 通訊協定情況下，測試平台 A 模擬使用者經由待測物，連上測試平台 B，存取對應通訊協定之服務，下載無病毒測試檔案，不可有檔案被待測物判定為病毒。

6.4.1.2. 線上更新

6.4.1.2.1. 測試環境

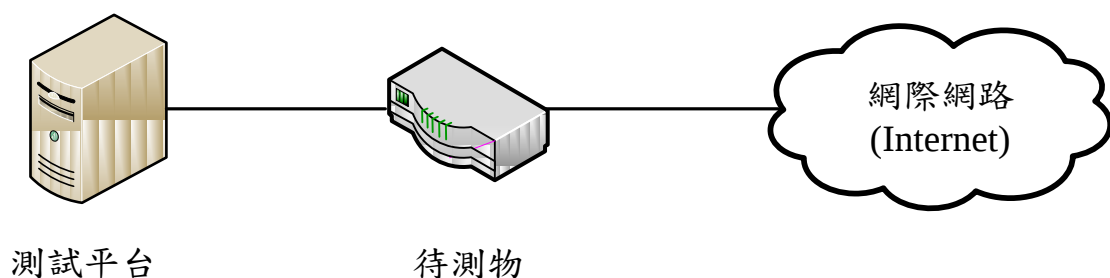


圖2 線上更新測試環境接續圖

- (1) 測試平台：可供測試人員連線至待測物之終端設備。
- (2) 網路連接線：乙太網路線或光纖纜線。
- (3) 連接待測物、測試平台與網際網路如圖 2。
- (4) 開啟待測物之線上更新功能（自動更新或手動更新）。

6.4.1.2.2. 測試方法及標準

- (8) 以測試平台開啟待測物之自動更新功能，確認待測物可自動更新掃毒引擎與特徵碼。
- (9) 以測試平台開啟待測物之手動更新功能，並設定每 5 分鐘自動更新，確認待測物可自動更新掃毒引擎與病毒特徵碼。
- (10) 以測試平台開啟待測物之手動更新功能，並設定每 60 分鐘自動更新，確認待測物可自動更新掃毒引擎與病毒特徵碼。
- (11) 以測試平台開啟待測物之手動更新功能，並設定每周一、三及五之凌晨 5 點自動更新，確認待測物可自動更新掃毒引擎與病毒特徵碼。

6.4.1.3. 安全事件紀錄

6.4.1.3.1. 測試環境

- (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 1。
- (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

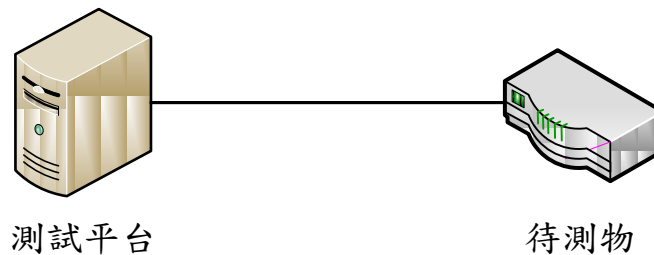


圖3 安全管理功能測試接續圖

- (1) 測試平台：可供測試人員連線至待測物之終端設備。
- (2) 網路連接線：乙太網路線或光纖纜線。
- (3) 連接待測物與測試平台如圖 3。

6.4.1.4.2. 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。

6.4.1.5. 運作模式切換 (適用進階型)

6.4.1.5.1. 測試環境

- (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) 網路連接線：乙太網路線或光纖纜線。

(4) 連接測試平台 A、待測物及測試平台 B 如圖 1。

(5) 將待測物運作模式由閘道模式 (Gateway Mode) 切換成通透模式 (Transparent Mode) 或由通透模式切換成閘道模式。

6.4.1.5.2. 測試方法及標準

由測試平台 A 經由待測物連線至測試平台 B，透過支援之通訊協定下載病毒檔案，待測物應正確偵測病毒且應阻擋或刪除該病毒檔案。

6.4.1.6. 惡意網址過濾 (適用進階型)

6.4.1.6.1. 測試環境

(1) 測試平台：可供測試人員連線至待測物之終端設備。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接待測物、測試平台與網際網路如圖 2。

(4) 啟用待測物惡意網址過濾功能。

(5) 測試平台透過 HTTP 通訊協定，瀏覽各類型惡意網址之網站。

6.4.1.6.2. 測試方法及標準

由測試平台透過 HTTP 通訊協定，瀏覽各類型之惡意網站，待測物應阻擋瀏覽惡意網站之網頁內容。

6.4.2. 壓力測試

6.4.2.1. 吞吐量

6.4.2.1.1. 測試環境



圖4 壓力測試接續圖

- (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 4。
- (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 (適用進階型)

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. 最大連線速率 (適用進階型)

6.4.2.3.1. 測試環境 同 6.4.1.4.1.。

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 3。
- (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 3。
- (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

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. 真實流量測試

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

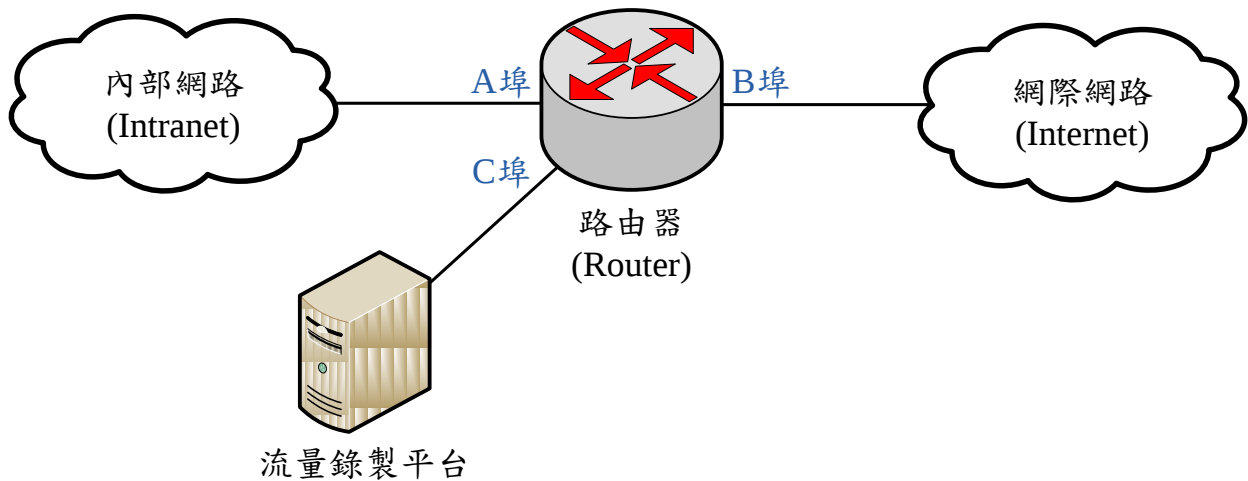


圖5 流量錄製接續圖



圖6 流量重播接續圖

- (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。

6.4.4.1.2. 測試樣本

測試樣本必須滿足以下要求：

- (1) 具備至少 100 位使用者同時上線的網路流量。
- (2) 若以重播方式進行測試，應為該待測物送測前 2 周內所錄製之網路流量。
- (3) 網路流量之最大同時連線數於測試期間必須達待測物規格說明處理能力最大值之 50% 以上。
- (4) 網路流量於測試期間必須達待測物吞吐量最大值之 50% 以上。
- (5) 網路流量內容包含至少 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、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。

6.4.4.1.3. 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

附件二、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: ...

附件三、安全架構表

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	附件 1、附件 2 之資料	V	
		詳如 0			V
安全功能設計	安全功能規格	詳如附表 1-3	附件 1 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息。	V	V
	設計安全性	詳如附表 1-4	附件 2 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	附件 3 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	V	V

類別	項目	判定標準	檢附文件	基礎	進階
			建議(需符合後續提供的指引手冊)。		
	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基本資料、安全功能(TSF)範圍及該設備可執行的安全功能需求(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)	檢附之設備標識標籤須符合審查內容

項目	審查內容	判定標準
	3. 製造商名稱	
範圍與規格	1. 設備形式(硬體 hardware/韌體 firmware/軟體 software) 2. 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。 3. 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。	檢附之設備規格書或邏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附件 1 資料（進階設備另需提供附件 2 資料），檢視安全功能需求(SFR)之執行內容是否符合附表 1-2-1 與 0 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
----	------	------

項目	審查內容	判定標準
1.稽核資料產生 (Audit data generation)	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(TSF)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（自行列舉） 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.針對本判定標準第 1 點(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。
2.使用者身分關聯(User Identity)	設備是否能建立稽核事件與使用者的關聯	設備安全功能(TSF)應能夠將每個可稽核事件與引發該事件之使用者進行關聯。

項目	審查內容	判定標準
Association)		
3.稽核審查 (Audit review)	設備是否具備審查稽核紀錄的功能	1. 設備安全功能(TSF)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
4.受限制之稽核審查 (Restricted audit review)	稽核紀錄是否僅由被識別的使用者進行審查，並排除其他使用者讀取的可能。	設備安全功能(TSF)應禁止未經授權使用者瀏覽稽核紀錄
5.可選取之稽核審查 (Selectable audit review)	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，提供進行搜尋及排序稽核紀錄的功能： (1) 事件日期與時間 (2) 事件類型 (3) 主體識別碼
6.稽核資料儲存保護(Protected Audit Trail)	如何防止非授權人員竄改或刪除稽核資料。	設備安全功能(TSF)應防止非授權人員透過安全功能介面竄改或刪除稽核資料。

項目	審查內容	判定標準
Storage)		
7.稽核資料漏失之預防 (Prevention of audit data loss)	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，除提供系統告警外，設備安全功能應執行下列動作之一，以維持儲存稽核紀錄之功能： (1)忽略新增之系統資料 (2)保護被授權使用者所選擇的系統資料 (3)每筆最新的系統資料必須從最舊的系統資料開始覆蓋 - 當系統發生稽核紀錄儲存空間耗盡前，應以下列資訊之一告警管理者： (1)儲存空間剩餘使用時間 (2)儲存空間剩餘可記錄筆數 (3)儲存空間剩餘百分比
8.防毒措施 (Anti-Virus)	設備如何進行病毒偵測。	設備安全功能(TSF)應偵測病毒，並執行下列措施之一：

項目	審查內容	判定標準
Actions)		(1) 清除病毒 (2) 隔離病毒 (3) 其他(自行列舉) 2. 設備安全功能(TSF)應監控企圖透過遠端 TCP、UDP、SMTP 協定進行非授權之程序。
9.防病毒告警 (Anti-Virus Alerts)	設備如何進行告警	1. 設備安全功能(TSF)偵測到病毒時，應發出警示訊息，內容應包含病毒資訊與處置措施。 2. 設備安全功能(TSF)應持續提供警示訊息，直到使用者與管理者有所回應。
10.密碼操作 (Cryptographic Operation)	系統如何確保病毒特徵檔之完整性	設備安全功能(TSF)應提供演算法產生簽章，包含演算法所屬標準及其金鑰長度，以確保病毒特徵檔之完整性。
11.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	設備安全功能(TSF)應提供管理員可啟用或關閉下列功能：

項目	審查內容	判定標準
(Management of security functions behavior)	能	(1)稽核 (2)即時病毒偵測
12.安全功能資料管理 (Management of TSF data)	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)應提供管理者設定查詢、更改或刪除下列事項： (1)病毒被偵測後所需進行的動作 (2)病毒特徵檔 (3)稽核紀錄
13.管理功能規格 (Specification of Management Functions)	如何提供額外的管理功能。	設備安全功能(TSF)應提供下列管理功能之一： (1)設定偵測功能啟用或關閉 (2)設定運作模式 (3)更新病毒碼 (4)回應警示訊息 (5)瀏覽稽核紀錄
14.安全角色	是否能規定設備能	1. 設備安全功能應維護以下安全角

項目	審查內容	判定標準
(Security roles)	識別之安全角色。	色： (1) 被授權管理者 (2) 被授權的系統管理者 (3) 其他(自行列舉) 2. 設備安全功能(TSF)應可定義使用者與其安全角色之關聯

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.稽核資料產生 (Audit data generation)	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(TSF)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(自行列舉) 2.每個稽核紀錄至少應具備下列資訊： (1) 事件日期及時間

項目	審查內容	判定標準
		(2) 事件型式 (3) 主體識別碼及事件結果(成功或失效)。 3.針對本判定標準第 1 點(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。
2.使用者身分關聯(User Identity Association)	設備是否能建立稽核事件與使用者的關聯	設備安全功能(TSF)應能夠將每個可稽核事件與引發該事件之使用者進行關聯。
3.稽核審查(Audit review)	設備是否具備審查稽核紀錄的功能	1. 設備安全功能(TSF)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
4.受限制之稽核審查(Restricted audit review)	稽核紀錄是否僅由被識別的使用者進行審查，並排除其他使用者讀取的可	1. 設備安全功能(TSF)應禁止未經授權使用者瀏覽稽核紀錄 2. 定義執行安全功能需求(SFR)的介面名稱(需與功能規格對應)

項目	審查內容	判定標準
	能。	
5.可選取之稽核 審查 (Selectable audit review)	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，提供進行搜尋及排序稽核紀錄的功能： (1) 事件日期與時間 (2) 事件類型 (3) 主體識別碼
6.稽核資料儲存 保護(Protected Audit Trail Storage)	如何防止非授權人員竄改或刪除稽核資料。	設備安全功能(TSF)應防止非授權人員透過安全功能介面竄改或刪除稽核資料。
7.稽核資料漏失 之預防 (Prevention of audit data loss)	設備如何因應稽核儲存空間耗盡時之狀況	1. 當系統發生稽核紀錄儲存空間耗盡時，除提供系統告警外，設備安全功能應執行下列動作之一，以維持儲存稽核紀錄之功能： (1) 忽略新增之系統資料 (2) 保護被授權使用者所選擇的系統資料

項目	審查內容	判定標準
		(3)每筆最新的系統資料必須從最舊的系統資料開始覆蓋 2. 當系統發生稽核紀錄儲存空間耗盡前，應以下列資訊之一告警管理者： (1)儲存空間剩餘使用時間 (2)儲存空間剩餘可記錄筆數 (3)儲存空間剩餘百分比
8.防毒措施 (Anti-Virus Actions)	設備如何進行病毒偵測。	1. 設備安全功能(TSF)應偵測病毒，並執行下列措施之一： (1) 清除病毒 (2) 隔離病毒 (3) 其他(自行列舉) 2. 設備安全功能(TSF)應監控企圖透過遠端 TCP、UDP、SMTP 協定進行非授權之程序。
9.防毒告警 (Anti-Virus)	設備如何進行告警	1. 設備安全功能(TSF)偵測到病毒時，應發出警示訊息，內容應包含

項目	審查內容	判定標準
Alerts)		病毒資訊與處置措施。 2. 設備安全功能(TSF)應持續提供警示訊息，直到使用者與管理者有所回應。
10.密碼操作 (Cryptographic Operation)	系統如何確保病毒特徵檔之完整性	設備安全功能(TSF)應提供演算法產生簽章，包含演算法所屬標準及其金鑰長度，以確保病毒特徵檔之完整性。
11.安全功能行為的管理 (Management of security functions behavior)	系統是否具備可以管理安全屬性的功能	設備安全功能(TSF)應提供管理員可啟用或關閉下列功能： (1) 稽核 (2) 即時病毒偵測
12.安全功能資料管理 (Management of TSF data)	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)應提供管理者設定查詢、更改或刪除下列事項： (1) 病毒被偵測後所需進行的動作 (2) 病毒特徵檔

項目	審查內容	判定標準
		(3)稽核紀錄
13.管理功能規格 (Specification of Management Functions)	如何提供額外的管理功能。	設備安全功能(TSF)應提供下列管理功能之一： (1)設定偵測功能啟用或關閉 (2)設定運作模式 (3)更新病毒碼 (4)回應警示訊息 (5)瀏覽稽核紀錄
14.安全角色 (Security roles)	是否能規定設備能識別之安全角色。	1. 設備安全功能應維護以下安全角色： (1) 被授權管理者 (2) 被授權的系統管理者 (3) 其他(自行列舉) 2. 設備安全功能(TSF)應可定義使用者與其安全角色之關聯
15.額外提供之安全技術	由廠商自行定義，如以下資訊流控制	設備安全功能實作之描述

項目	審查內容	判定標準
	功能： (1) 對每一個安全屬性實行資訊流控制。 (2) 實行額外資訊流控制。 (3) 消除非法資訊流。 (4) 非法資訊流監視。	

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	需提供附件 1 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。

等級	審查內容	判定標準
	面(TSFI)完整實現。	
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。	需提供附件 1 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	需提供附件 2 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。

審查內容	判定標準
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。	

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	需提供附件 3 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

審查內容	判定標準
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。	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	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

審查內容	判定標準
(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。 (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。	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
(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(如針對伺服器進行網路協定管制作業等) 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網路封包或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
----	----	------	----	----	----

類別	項目	判定標準	備註	基礎	進階
安全功能測試	病毒偵測	3.啟動預設規則下，應可偵測進出流量之封包。 4.啟動預設規則下： (1)對於 Mandatory 樣本不可有漏判。 (2)不可有誤判。 5.無論啟動何種協定之掃毒功能，管理介面皆要正常運作。	亦應符合附表 1-2-1、0 之項目 8	V	
		3.啟動預設規則下，應可偵測進出流量之封包。 4.啟動預設規則下： (1)對於 Mandatory 樣本不可有漏判，對於 Optional 樣本漏判率應小於 10%			V

類別	項目	判定標準	備註	基礎	進階
		(2) 不可有誤判。 5.無論啟動何種協定之掃毒功能，管理介面皆要正常運作。			
	線上更新	應可透過網路進行線上更新特徵碼資料。	亦應符合附表 1-2-1、0 之項目 10、13	V	V
	安全事件紀錄	應記錄病毒偵測之結果及處理方式(如隔離或刪除等)	亦應符合附表 1-2-1、0 之項目 1、2、7、9	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、0 之項目 10、13	V	V
	運作模式	具備可切換運作模式(路由	亦應符合附表		V

類別	項目	判定標準	備註	基礎	進階
	切換	模式或透通橋接模式)	1-2-1、0 之項目 13		
	惡意網址過濾	具備過濾惡意網址之功能	亦應符合附表 1-2-1、0 之項目 8		V
壓力測試	吞吐量	設備所負荷的吞吐量(Mbps 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。		V	V
	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

類別	項目	判定標準	備註	基礎	進階
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. 病毒偵測

6.4.1.1.1. 測試環境

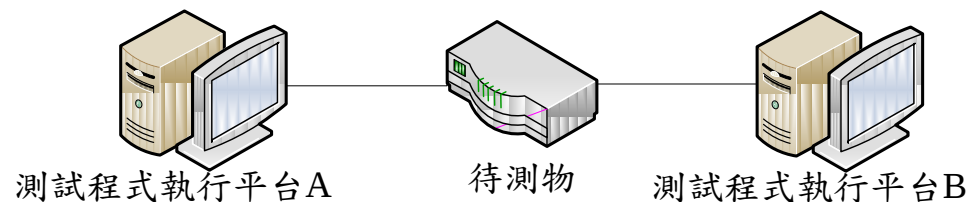


圖7 病毒偵測測試環境

6.4.1.1.2. 測試組態

(1) 連線至待測物設定掃毒功能，啟動支援之通訊協定掃毒功能。

(2) 參數設定

C.病毒 Mandatory 樣本：以 WildList 組織發布半年內之病毒資訊為樣本。

D.病毒 Optional 樣本：以 WildList 組織發布一年內之病毒資訊為樣本。

E.通訊協定：HTTP/FTP/SMTP/POP3/IMAP。

6.4.1.1.3. 測試方法及標準

(1)分別開啟 HTTP/FTP/SMTP/POP3/IMAP 通訊協定情況下，測試程式執行平台 A 模擬使用者經由待測物，連上測試程式執行平台 B，存取對應通訊協定之服務，下載病毒測試檔案。基礎等級對於 Mandatory 樣本之病

毒漏判率須為 0%；進階等級對於 Mandatory 樣本之病毒漏判率需為 0%，對於 Optional 樣本之病毒漏判率需小於 10%。

(2)分別開啟 HTTP/FTP/SMTP/POP3/IMAP 通訊協定情況下，測試程式執行平台 A 模擬使用者經由待測物，連上測試程式執行平台 B，存取對應通訊協定之服務，下載無毒測試檔案，不可有檔案被待測物判定為病毒。

(3)同時開啟 HTTP/FTP/SMTP/POP3/IMAP 通訊協定情況下，測試程式執行平台 A 模擬使用者經由待測物，連上測試程式執行平台 B，存取對應通訊協定之服務，下載病毒測試檔案。基礎等級對於 Mandatory 樣本之病毒漏判率須為 0%；進階等級對於 Mandatory 樣本之病毒漏判率需為 0%，對於 Optional 樣本之病毒漏判率需小於 10%。

(4)同時開啟 HTTP/FTP/SMTP/POP3/IMAP 通訊協定情況下，測試程式執行平台 A 模擬使用者經由待測物，連上測試程式執行平台 B，存取對應通訊協定之服務，下載無毒測試檔案，不可有檔案被待測物判定為病毒。

6.4.1.2. 線上更新

6.4.1.2.1. 測試環境

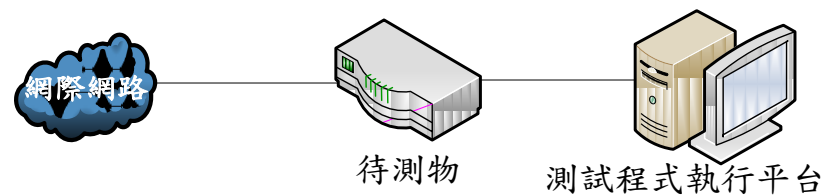


圖8 線上更新測試環境

6.4.1.2.2. 測試組態

(1) 啟用待測物線上更新功能。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，找到待測物線上更新功能的對應設定位置，將待測物線上更新功能開啟。

(2) 參數設定

更新方式：自動更新、手動更新

6.4.1.2.3. 測試方法及標準

(1) 由測試程式執行平台設定待測物，啟用自動更新功能，確認待測物可自動更新掃毒引擎與特徵碼。

(2) 由測試程式執行平台設定待測物，啟用手動更新功能，並設定每 5 分鐘更新，確認待測物可自動更新掃毒引擎與特徵碼。

(3) 由測試程式執行平台設定待測物，啟用手動更新功能，並設定每小時更新，確認待測物可自動更新掃毒引擎與特徵碼。

(4) 由測試程式執行平台設定待測物，啟用手動更新功能，並設定每周一、三、五凌晨 5 點更新，確認待測物可自動更新掃毒引擎與特徵碼。

6.4.1.3. 安全事件紀錄

6.4.1.3.1. 測試環境 同圖 8。

6.4.1.3.2. 測試組態

- (1) 啟用待測物掃毒功能，啟動支援之通訊協定掃毒功能。
- (2) 啟用待測物安全紀錄功能。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，找到待測物安全紀錄功能的對應設定位置，將待測物安全紀錄功能開啟。
- (3) 參數設定
 - A. 待測物參數：啟動支援之通訊協定掃毒功能。
 - B. 流量產生參數：測試程式執行平台 A 連線測試程式執行平台 B 之對應服務，下載病毒檔案。

6.4.1.3.3. 測試方法及標準

由測試程式執行平台 A 產生病毒流量通過待測物，待測物的安全事件紀錄資訊應正確紀錄違反安全事件發生的時間與內容，以及病毒處理之方式。

6.4.1.4. 安全管理功能

6.4.1.4.1. 測試環境

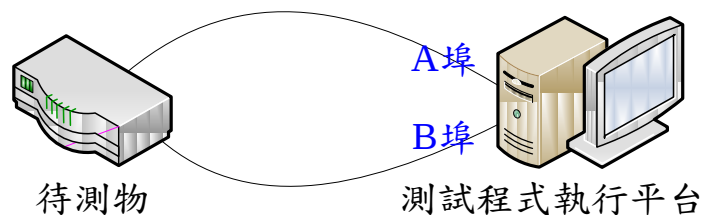


圖9 安全管理功能測試環境

6.4.1.4.2. 測試組態 無。

6.4.1.4.3. 測試方法及標準

- (1)由測試程式執行平台 A 連線至待測物，確認待測物是否需要密碼才可進行設定，待測物應須密碼才可進行管理設定。
- (2)嘗試輸入錯誤密碼，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一段時間，避免遭受攻擊。

6.4.1.5. 運作模式切換(進階等級)

6.4.1.5.1. 測試環境 同圖 83。

6.4.1.5.2. 測試組態

- (1) 由測試程式執行平台 A 連線至待測物，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，找到待測物運作模式切換功能的對應設定位置，切換待測物運作模式。

(2) 參數設定

將待測物運作模式切換成閘道模式或透通橋接模式。

6.4.1.5.3. 測試方法及標準

由測試程式執行平台 A 經由待測物連線測試程式執行平台 B，透過支援之通訊協定下載病毒檔案，待測物應正確偵測到病毒，且正確的阻擋或刪除檔案。

6.4.1.6. 惡意網址過濾(進階等級)

6.4.1.6.1. 測試環境 同圖 3。

6.4.1.6.2. 測試組態

(1) 啟用待測物惡意網址過濾功能。

(2) 參數設定

測試程式執行平台 A 透過 HTTP 通訊協定，瀏覽各類型惡意網址之網站。

6.4.1.6.3. 測試方法及標準

由測試程式執行平台 A 透過 HTTP 通訊協定，瀏覽各類型惡意網址之網站，待測物應阻擋使用者瀏覽惡意網址之

網頁內容，避免使用者遭受惡意網站內容之攻擊。

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 3。

(1) 開啟待測物之安全功能。

(2) 參數設定

封包大小：64~1518 位元組。

6.4.2.1.2. 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

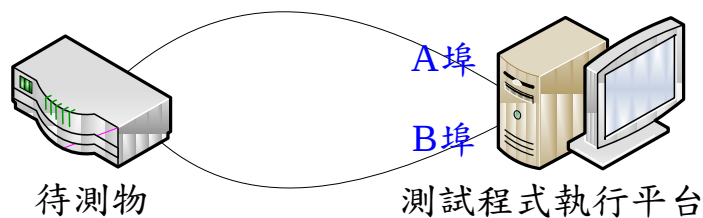


圖10 最大同時連線數測試環境

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. 最大連線速率

6.4.2.3.1. 測試環境 同圖 10。

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 同圖 10。

6.4.3.1.2. 測試組態

針對待測物提供服務的連接埠發動阻斷式攻擊。

6.4.3.1.3. 測試方法及標準

自測試程式執行平台產生各類阻斷式攻擊，攻擊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，等攻擊結束後待測物之病毒過濾功能應正常運作。

6.4.3.2. 惡意流量

6.4.3.2.1. 測試環境

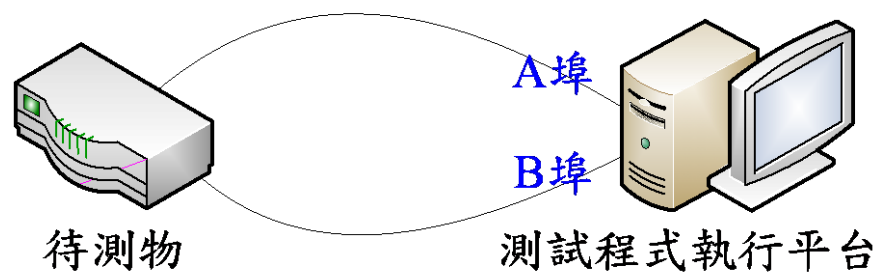


圖11 惡意流量防禦測試環境

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 buffer overflow)，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. 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

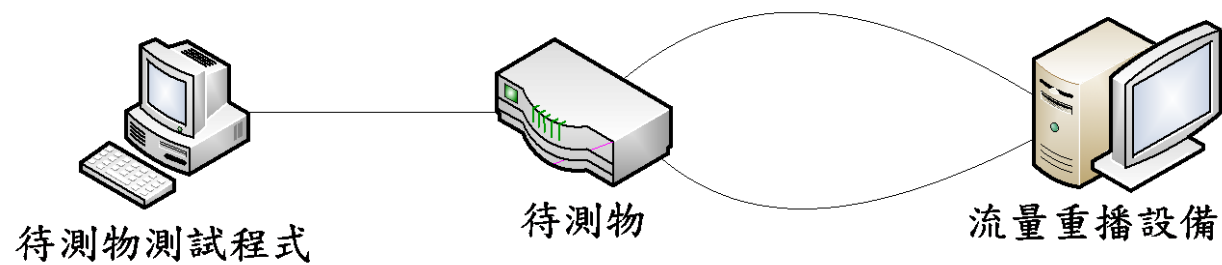


圖12 真實流量測試網路拓樸(重播方式)

6.4.4.1.2. 測試組態

- (1) 設定一組病毒過濾規則，過濾支援之通訊協定流量。
- (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 XXX		5. 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)向記憶體管理子系統要求一個記憶體區塊 (2)記憶體管理子系統回應所分配之記憶體起始位址

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	
	身分認證	
	資料安全管理	
	功能自我保護	
	用戶資料保護	
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。

項目	描述		
範例：	網路連接		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 Self-Protection	安全功能	與外部設備之介面	保護機制
	安全稽核		
	身分認證		
	密碼支援		
	資料安全管理		
	功能自我保護		
	用戶資料保護		
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

項目		描述	
範例：身分認證		以網路連結外部弱點資料庫、以TSFI_WEBGUI 介面進行身分認證	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
4.防止繞道攻擊 Bypass	安全功能	防護機制	
	安全稽核		
	身分認證		
	密碼支援		
	資料安全管理		
	功能自我保護		
	用戶資料保護		
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：身分認證		以實體封鎖方式，防止利用維護介面繞道身分認證程序。	