



電信技術規範
檢驗規範

資通安全 0011 (IS0011-0)
訂定日期 101 年 3 月 30 日
通傳技字第 10143007090 號

網路型垃圾郵件過濾設備 資通安全檢測技術規範

國家通訊傳播委員會
中華民國101年3月

目 次

1. 概說	1
2. 適用範圍	1
3. 安全等級	1
4. 參考標準	1
5. 用語釋義	2
6. 技術要求	4
6.1. 書面審查類別	4
6.1.1. 安全標的	4
6.1.2. 安全功能設計	4
6.2. 書面審查類別之項目及判定標準	4
6.2.1. 安全標的	5
6.2.2. 安全功能設計	10
6.3. 實機測試類別	14
6.3.1. 安全功能測試	14
6.3.2. 壓力測試	14
6.3.3. 堅實測試	14
6.3.4. 穩定測試	14
6.4. 實機測試類別之項目及判定標準	15
6.4.1. 安全功能測試	16
6.4.2. 壓力測試	18
6.4.3. 堅實測試	20
6.4.4. 穩定測試	21

圖 次

圖 1	郵件內容反釣魚網址測試接續圖	17
圖 2	即時流量監控測試接續圖	17
圖 3	安全管理功能測試接續圖	18
圖 4	壓力測試接續圖	19
圖 5	流量錄製接續圖	22
圖 6	流量重播接續圖	22

表 次

表 1	書面審查之類別、項目及審查內容	5
表 2	實機測試之類別、項目及判定標準	15

附 件

附件一、 安全功能規格表.....	附件 1-1
附件二、 設計安全性表.....	附件 2-1
附件三、 安全架構表.....	附件 3-1

網路型垃圾郵件過濾設備資通安全檢測技術規範

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。

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)。

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

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。

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	附件一、安全功能規格表	✓	✓
	設計安全性	附表 1-4	附件二、設計安全性表		✓
	安全架構	附表 1-5	附件三、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. 設備類型說明

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）	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		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)。	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			(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。	✓	✓
		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	安全功能應具備以下資料流控制： (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. 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) 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	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			(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後，應具備避免殘餘資料外洩的功能。	✓	✓
		10.密碼操作	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。 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	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			(2) 稽核紀錄需可由人員辨讀		
		14.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) 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	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竊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。	✓	✓
		16.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，安全功能應具備以下稽核資料漏失之預防，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	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			警告		
		17.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，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		✓

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

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

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	✓	✓

類別	項目	審查標準	基礎型	進階型
		(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附件二、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		✓

6.2.2.3. 安全架構

本項書面審查內容依申請者提供之附件三、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	<p>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：</p> <p>(1) 待測物因執行安全功能所區隔的安全領域。</p> <p>(2) 安全功能的安全初始程序。</p> <p>(3) 安全功能的自我保護機制。</p> <p>(4) 安全功能執行如何避免被繞道。</p>		✓

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

類別	項目	審查標準	基礎型	進階型
安全功能設計	安全指引	<p>(1) 應定義每個使用者角色</p> <p>(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：</p> <ul style="list-style-type: none"> 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 <p>(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</p> <p>(4) 應列舉待測物操作時的所有運作模式</p> <p>(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</p> <p>(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</p> <p>(7) 應說明待測物操作的安全環境設置，應包括以下項目：</p> <ul style="list-style-type: none"> 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 	✓	✓

類別	項目	審查標準	基礎型	進階型
		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

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	郵件內容反釣魚網址過濾	依 6.4.1.1.2. 進行測試，應具備過濾釣魚網址之功能。	/	✓
	安全事件紀錄	依 6.4.1.2.2. 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 6.4.1.3.2. 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。	✓	✓
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。	/	✓
	最大建立連線速率	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	阻斷式攻	依 6.4.3.1.2. 進行測試，當攻擊流量低於或等於	✓	✓

類別	項目	判定標準	基礎型	進階型
測試	擊	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. 郵件內容反釣魚網址過濾 (適用進階型)

6.4.1.1.1. 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) 啟用待測物郵件內容反釣魚網址過濾功能。
- (6) 連接測試平台及待測物如圖 1。
- (7) 測試平台 A 透過 SMTP 通訊協定，寄出包含各類型惡意網址之

信件，此類信件通過待測物後應被阻擋或過濾掉。



圖 1 郵件內容反釣魚網址測試接續圖

6.4.1.1.2. 測試方法及標準

由測試平台 A 埠透過 SMTP 通訊協定接放含有釣魚網址的郵件，待測物應過濾含有釣魚網站連結之郵件，進而避免使用者因而洩漏個人資訊或造成其它安全危害。

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) 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) 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。
- (5) 開啟垃圾郵件過濾功能。
- (6) 使用測試程式執行平台寄送垃圾郵件。

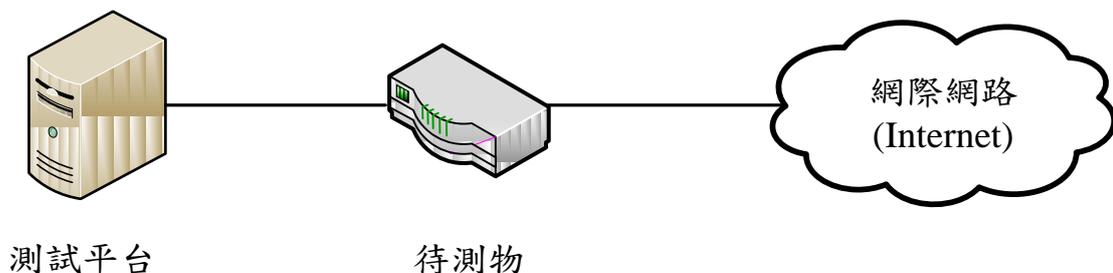


圖 2 安全事件管理測試接續圖

6.4.1.2.2. 測試方法及標準

以測試平台產生違反安全事件紀錄之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。

6.4.1.3. 安全管理

6.4.1.3.1. 測試環境

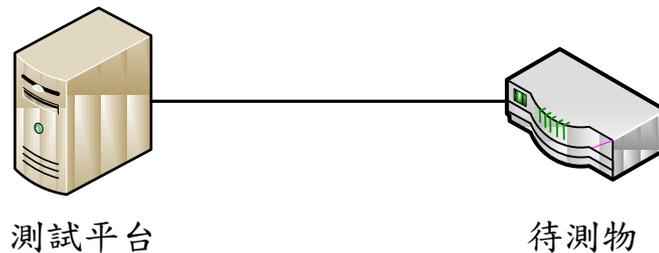


圖 3 安全管理功能測試接續圖

- (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。

6.4.1.3.2. 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。
- (2) 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。

6.4.2. 壓力測試

6.4.2.1. 吞吐量

6.4.2.1.1. 測試環境

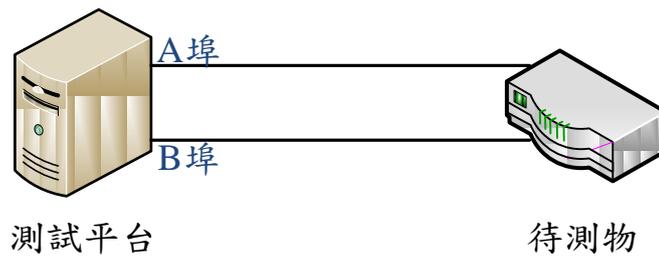


圖 4 壓力測試接續圖

- (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，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. 最大同時連線數 (適用進階型)

6.4.2.2.1. 測試環境 同 6.4.1.2.1。

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 (適用進階型)

6.4.2.3.1. 測試環境 同 6.4.1.2.1.。

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 (適用進階型)

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

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。

6.4.3.3. 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

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

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. 。

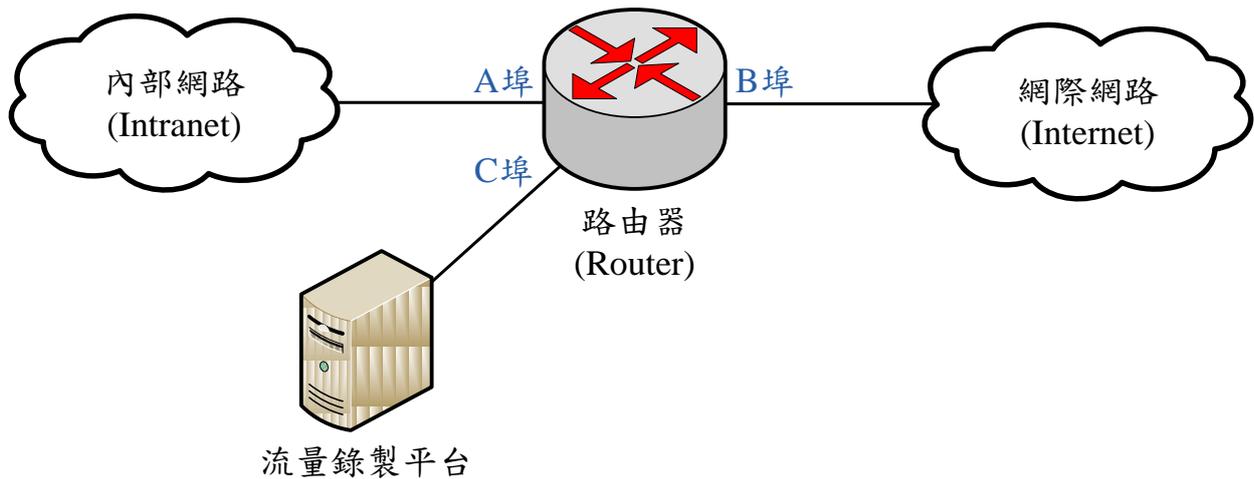


圖 5 流量錄製接續圖



圖 6 流量重播接續圖

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。

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値之 50% 以上。
- (4) 網路流量於測試期間必須達待測物吞吐量最大値之 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： <i>Subsystem_ssh</i>	範例： <i>提供 ssh 服務</i>	範例： <i>TSFI_CLI</i>	範例： (1) 提供 <i>TSFI_CLI</i> 命令列模式操作介面 (2) 與其他子系統之互動： (A) <i>Subsystem_auth</i> : 傳遞認證資訊給 <i>Subsystem_auth</i> ，並由回覆訊息確認認證是否成功 (B) <i>Subsystem_terminal</i> : ...

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： <i>TSFI_GUI:</i> <i>Domain_SecureLogAudit</i> <i>Domain_SecureConnection</i>	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 <i>TSFI_GUI</i> 來執行管理功能石，該 <i>TSFI</i> 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
	<p>列出各安全功能介面對應之自我保護機制</p> <p>範例：</p> <p><i>TSFI_WEB:</i></p> <p>自我保護 1:身分驗證</p> <p>自我保護 2:遠端連線加密</p>	<p>說明安全功能及其介面與外部設備之資料交換動作</p> <p>範例：</p> <p>遠端以瀏覽器連線待測物進行管理功能時，以 <i>TSFI_WEB GUI</i> 介面進行身分認證</p>	<p>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</p> <p>範例：</p> <ol style="list-style-type: none"> 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： <i>TSF_Authentication</i> 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。