電信技術規範
檢 驗 規 範

資通安全 0015 (IS0015-0)
定訂日期 101 年 2 月 29 日
通傳技字第 10043040220 號

路由交換器

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2月

目　次

圖　次

表　次

附　件

路由交換器資通安全檢測技術規範

1. 概說

路由交換器是一種同時具備網路封包路由及封包交換功能之網路設備，能處理路由協定、計算封包傳送的最佳路由及下一個傳送點，亦支援路由與交換相關網路管理與設定之功能。

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路由交換器，可支援開放系統介面 (OSI, Open System Interface) 之第一層至第三層，並依不同網路所屬之安全策略來處理網路封包。

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

基礎型設備安全功能測試項目包括安全管理、自動登出功能、路由認證、路由被動介面及封包阻擋規則等；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

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環路偵測與預防機制、網路用戶認證機制、備援管理及組態備援管理等；壓力測試項目包括吞吐量；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)

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。

5.7. **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. 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)。

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)	✓	✓
		2.範圍	應說明下列內容：	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			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) 使用者身份及鑑別資料。 (2) 被授權的系統角色。 (3) 輸入使用者密碼時，螢幕必須為暗碼。 (4) 使用者密碼資料在設定檔(configuration file)中必須加密。	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			(5) 可提供外部認證機制如：RADIUS/TACACS 等，統一控管所有使用者帳號資料。 (6) 近端管理 (console) 必須支援終止遠端管理連線功能。		
		3. 鑑別之時序	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。 (2) 完成使用者身分認證後，始可執行被授權的安全功能。	✓	✓
		4. 鑑別失敗處理	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。 (3) 需支援認證失敗告警(如：log 及 trap)。	✓	✓
		5. 資料流控制	安全功能應具備及設定以下資料流控制： (1) MAC 或 IPv4/v6 來源端位址或其他自行指定之來源格式。 (2) MAC 或 IPv4/v6 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) 使用者自行指定任意封包欄位。 (7) 其他 (自行指定)。	✓	✓
		6. 安全功能行為	安全功能應賦予被授權的管理者具備及設定以下安全功能行為的管理：	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		的管理	(1) 系統啟動與關閉。 (2) 針對路由交換器資料流控制規則進行新增、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) 允許或禁止所屬/外部網段的管理者/外部設備登入系統進行管理。 (5) 修改登入失敗次數的最大值。 (6) 恢復因登入失敗次數過多被停權的使用者。 (7) 允許或禁止外部設備登入系統進行管理。 (8) 修改系統日期或時間。 (9) 備份、建立、刪除、清空或審查稽核紀錄。 (10) 備份使用者安全屬性、路由交換器規則、稽核紀錄資料 (應由系統提供自動化備份工具)。 (11) 系統設定之還原。 (12) 當系統允許遠端管理時： A. 啟用或禁止透過所屬/外部網段進行管理。 B. 限制某外部網段位址可登入系統進行管理。 (13) 記錄所有命令輸入的使用者及時間資訊。 (14) 其他 (自行指定)。		
		7. 密碼操作	待測物應以密碼演算法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。	✓	✓
		8. 可信賴	待測物應具備可信賴之時戳 (Reliable	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		之時戳	Timestamp)，正確記錄稽核資料的日期及時間。		
		9. 稽核資料產生	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. 其他 (自行指定)。 (2) 每筆稽核紀錄至少包含下列資訊： A. 主體識別碼。 B. 事件日期及時間。 C. 事件類型。 D. 事件成功或失敗。	✓	✓
		10. 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) 儲存的稽核紀錄不允許任何使用者透過任何形式修改。 (3) 當系統發生稽核紀錄儲存空間已滿、故障或遭受攻擊時，設備安全功能應可維持儲存稽核紀錄之功能。	✓	✓
		11. 稽核資料漏失之預防	安全功能應具備當發生稽核紀錄儲存設備之空間用盡時，應維持儲存稽核紀錄之功能，並應至少提供下列一種處置方式： (1) 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。 (2) 刪除稽核紀錄：將不需要保存之稽核紀錄予	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
			以刪除。 (3) 覆蓋稽核紀錄：新增之稽核紀錄覆蓋最舊的稽核紀錄。		
		12. CPU 保護	安全功能應具備 CPU 保護機制，防止過量惡意 IP 與 ARP 封包造成 CPU 過於忙碌而無法處理來自於管理人員的管理封包。	✓	✓
		13. 系統備援	安全功能應具備以下系統備援： (1) 備援設備應保持對於主要設備之組態備份。 (2) 若主要設備故障，備援設備應立即取代，網路流量與管理立即回復正常。		✓
		14. 虛擬路由功能	安全功能應具備虛擬路由的各自互相獨立運作，網段號碼重疊互不影響。		✓
		15. 非生成樹 (STP) 的環路偵測與預防	安全功能應具備以下非生成樹 (STP) 的環路偵測與預防： (1) 偵測與阻斷同台機器上不同關閉 STP 的埠互聯所造成之環路。 (2) 具備迴路預防機制避免此種情況發生。		✓
		16. 網路用戶認證機制	安全功能應具備以下網路用戶認證機制： (1) 對於個人主機，支援使用者帳號密碼認證或 MAC 地址認證。 (2) 對於網路設備，支援 MAC 地址認證。		✓、

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	✓	✓

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	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：		✓

類別	項目	審查標準	基礎型	進階型
		(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	✓	✓

類別	項目	審查標準	基礎型	進階型
		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

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**	**進階**
安全功能測試	安全管理	依 6.4.1.1.2. 進行測試，應具備下列安全管理功能： 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。 3. 通行碼必須以暗碼顯示。 4. 設定檔具備加密功能。 5. 支援終止遠端管理連線功能。 6. 允許特定 IP 對待測物進行網管操作。	✓	✓

類別	項目	判定標準	基礎	進階
	自動登出功能	依 6.4.1.2.2. 進行測試，一段時間沒有操作待測物後，應自動登出管理介面。	✓	✓
	路由認證保護	依 6.4.1.3.2. 進行測試，只和通過認證保護的鄰近路由器交換 RIP 路由資訊。	✓	✓
	路由被動介面	依 6.4.1.4.2. 進行測試，應防止路由資訊被竊聽及禁止未授權之設備參與路由交換。	✓	✓
	封包過濾	依 6.4.1.5.2. 進行測試，可自訂 Access Control List (ACL)，並依 ACL 之內容，判斷其通過或阻擋與否。	✓	✓
	環路偵測與預防機制	依 6.4.1.6.2. 進行測試，當待測物偵測某埠之下游設備出現環路時，應自動關閉該埠。		✓
	網路用戶認證機制	依 6.4.1.7.2. 進行測試，應提供使用者帳號密碼驗證或 MAC 地址驗證之認證機制。		✓
	備援管理	依 6.4.1.8.2. 進行測試，備援待測物應於規定時間內接替失效之待測物。		✓
	組態備援功能	依 6.4.1.9.2. 進行測試，待測物之組態應正確回復至指定之備份組態。		✓
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。		✓
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。	✓	✓

類別	項目	判定標準	基礎	進階
	遠端管理異常流量	依 6.4.3.2.2.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 6.4.3.3.1.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。	✓	✓
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，應可持續 336 小時穩定運作。		✓

6.4.1. 安全功能檢測

6.4.1.1. 安全管理功能

6.4.1.1.1. 測試環境

(1) 測試平台：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、待測物及網際網路如圖 1。

(4) 開啟待測物之安全功能。

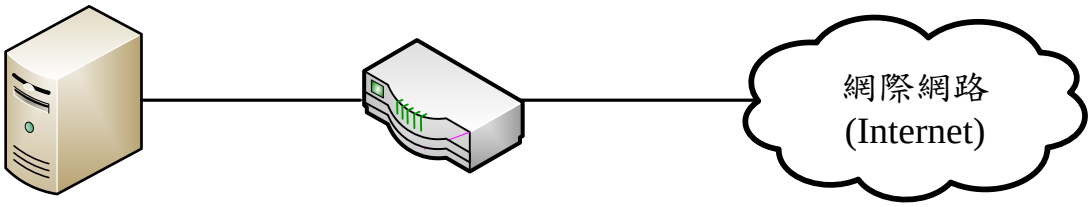

圖1　安全管理功能測試接續圖

6.4.1.1.2. 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。待測物應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。

(3) 輸入通行碼，應確認是否顯示為暗碼。

(4) 組態檔中的密碼資料必須加密。

(5) 建立遠端連線後，近端管理具備中止該遠端連線之功能。

(6) 允許特定 IP 之測試平台可對待測物進行網管操作。更改測試程平台之 IP 後，測試平台應無法對待測物進行管理。

6.4.1.2. 自動登出功能

6.4.1.2.1. 測試環境 同 6.4.1.1.1.。

6.4.1.2.2. 測試方法及標準：

(1) 合法使用者登入待測物之管理介面後，如不進行任何操作，當閒置時間超過設定值時，待測物應自動將此使用者登出，必須再次輸入帳號密碼才能管理待測物。

(2) 由測試平台模擬出 30 台連線之 PC，讓待測物新增這 30 台 PC 的 ARP Entry。 測試人員使用如 show arp 指令，確認待測物已新增 ARP Entry 後，停留在等待使用者輸入翻頁指令之畫面，不進行任何操作，待閒置時間超過設定值時，應自動登出。

6.4.1.3. 路由認證

6.4.1.3.1. 測試環境

(1) 路由器：處理網路封包路由 (Route) 之設備。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接路由器、待測物及網際網路如圖 2。

(4) 開啟待測物之 RIP 認證功能。

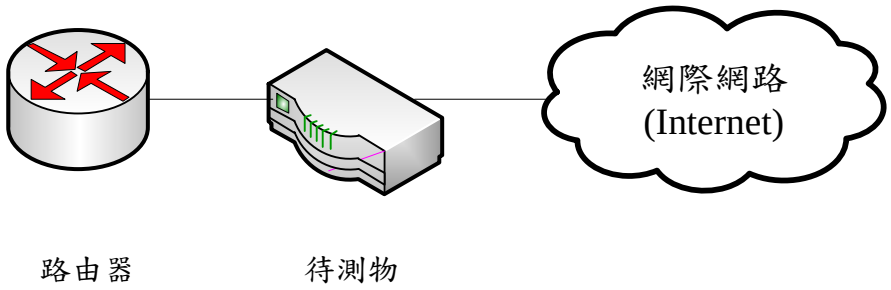

圖2　路由認證保護測試接續圖

6.4.1.3.2. 測試方法及標準

路由器必須設定與待測物相同之 RIP 認證碼，才能和待測物交換路由資訊。

6.4.1.4. 路由被動介面 (Passive Interface)

6.4.1.4.1. 測試環境

(1) 測試平台：測試儀器或程式。

(2) 路由器：處理網路封包路由之設備。

(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、路由器及網際網路如圖 3。

(5) 待測物之介面 A 及介面 B，都已經設定開啟 RIP 功能，且介面 A 設定為被動式介面 (Passive Interface)。

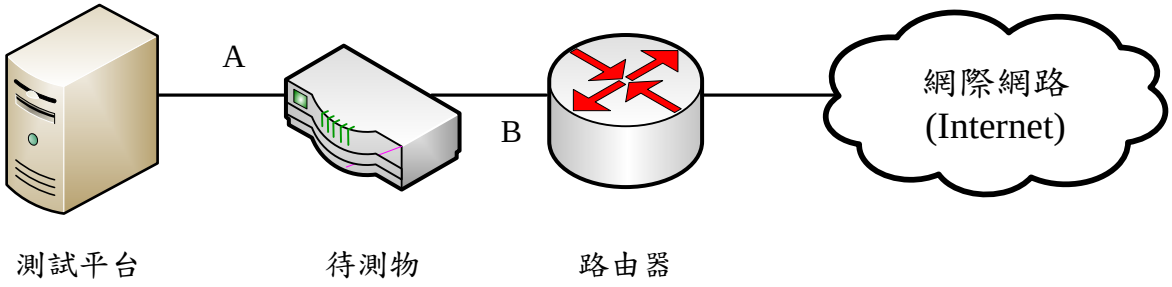

圖3　路由被動介面測試接續圖

6.4.1.4.2. 測試方法及標準

(1) 確認路由器可獲得介面 B 的路由資訊。

(2) 測試平台使用封包擷取軟體進行封包擷取，不可擷取到 RIP 封包。

6.4.1.5. 封包過濾

6.4.1.5.1. 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 4。
(6) 開啟待測物之封包過濾功能。
(7) 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。

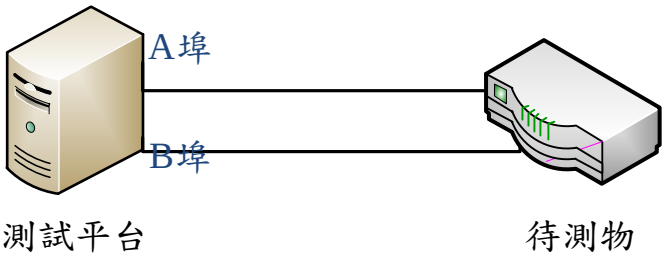

圖4 封包過濾測試接續圖

6.4.1.5.2. 測試方法及標準

(1) 待測物可自訂 Access Control List (ACL) 之安全規則屬性、辨識條件及安全策略。

(2) 待測物依 ACL 之內容，判斷其通過或阻擋與否。

6.4.1.6. 環路偵測與避免機制 (適用進階型)

6.4.1.6.1. 測試環境

(1) 測試平台：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。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接測試平台、待測物及交換集線器如圖 5。

(4) 開啟待測物之環路偵測與避免功能。

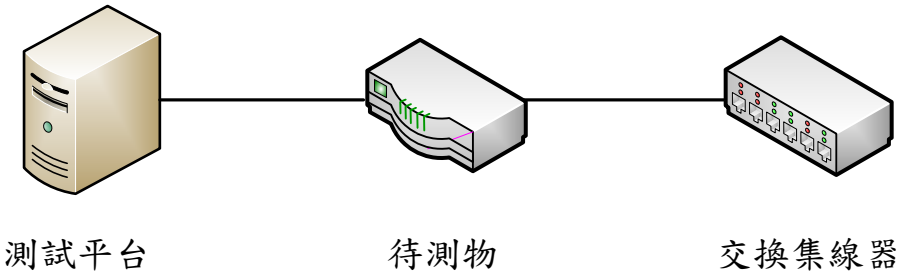

圖5　環路偵測與預防機制接續圖

6.4.1.6.2. 測試方法及標準

用網路連接線將下游的交換集線器之任意兩埠連接，使其產生環路，當待測物偵測某埠之下游設備出現環路時，應自動關閉該埠。

6.4.1.7. 網路用戶認證機制 (適用進階型)

6.4.1.7.1. 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) 網路連接線：乙太網路線或光纖纜線。

(3) 連接測試平台、待測物及網際網路如圖 1。

(4) 開啟待測物之網路用戶認證機制功能。

6.4.1.7.2. 測試方法及標準

待測物能對其連接之設備提供使用者帳號密碼驗證或 MAC 地址驗證，通過驗證之設備方可存取網際網路。

6.4.1.8. 備援管理 (適用進階型)

6.4.1.8.1. 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：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 6。

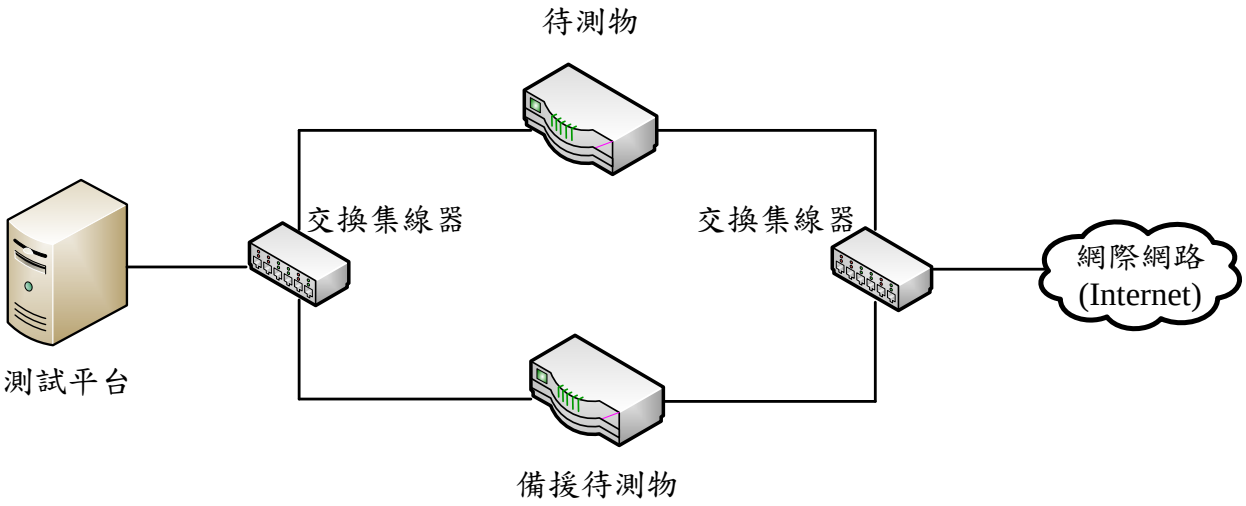

圖6 備援測試接續圖

6.4.1.8.2. 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 3 秒內自動接替待測物，確保網路流量仍可正常傳送至網際網路。

6.4.1.9. 組態備援功能 (適用進階型)

6.4.1.9.1. 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) 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 7。

(4) 開啟待測物之組態備援功能。

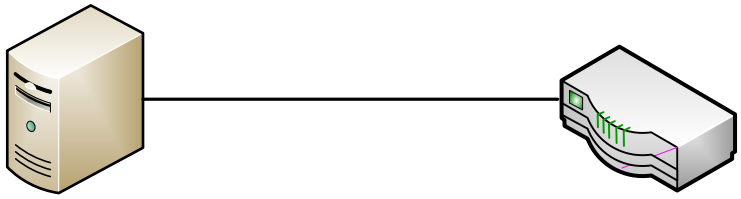

圖7　阻斷式攻擊測試接續圖

6.4.1.9.2. 測試方法及標準

啟用組態回復功能，待測物之組態必須正確回復至指定之備份組態。

6.4.2. 壓力測試

6.4.2.1. 吞吐量 (適用進階型)

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 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。

6.4.3. 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 7。
(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 7。
(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/協定異常流量產生程式 (若待測物提供 Web GUI 設定服務，則使用 HTTP 異常流量產生程式)，從外部網路對待測物施加各項服務/協定異常流量，測試過程待測物安全功能應保持正常運作。

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. 真實流量測試

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 8。

(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 9。

(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。

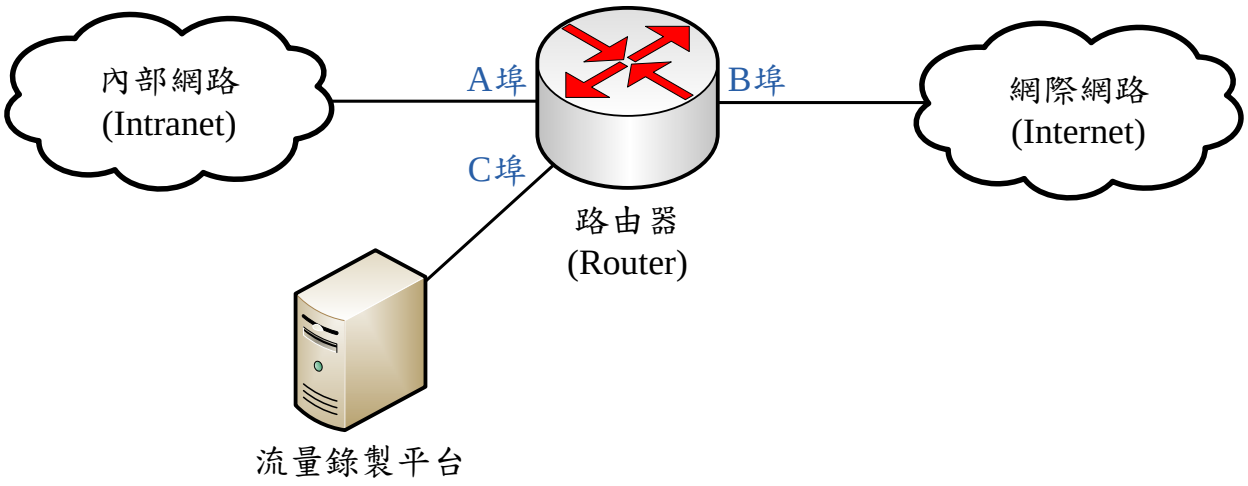

圖8　流量錄製接續圖

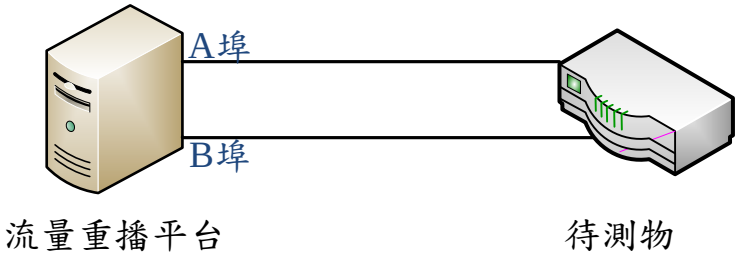

圖9　流量重播接續圖

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。

6.4.4.1.3. 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。*