電信技術規範
檢 驗 規 範

資通安全 0014 (IS0014-0)
訂定日期 100 年 2 月 29 日
通傳技字第 10043040220 號

乙太網路交換器

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

乙太網路交換器資通安全檢測技術規範

1. 概說

乙太網路交換器 (Ethernet Switch，以下簡稱 Switch) 是用來連接網路區段的裝置，並負責導引資料封包，以確保它們可以到達正確的目的地。交換器可用來進行多重的連接亦可提升網路之效能。

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網路型乙太網路交換器，可支援開放系統介面 (OSI, Open System Interface) 網路架構。

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. 基礎型乙太網路交換器

基礎型設備安全功能測試項目包括安全稽核功能、資料流控制、使用者識別與鑑別功能、安全管理功能與可靠時戳；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. 進階型乙太網路交換器

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虛擬區網 (VLAN) 保護功能及組態備援管理等；壓力測試項目包括最大虛擬區網 (VLAN) 容量及最大 MAC 容量；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)

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)。

5.13. 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）。

5.14. 安全屬性 (Security Attribute)

指定義主體、使用者 (包括設備外部資訊產品) 、受體、資訊、對談 (Session) 或資源的一種特性，並根據其定義的特性 (值) 來執行安全功能。

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： 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

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. 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. 系統存取設備。 C. 系統資料存取。 D. 其他 (自行列舉)。 (2) 每筆稽核紀錄至少包含下列資訊： A. 事件日期及時間。 B. 事件類型。 C. 主體識別碼。 D. 事件成功或失敗。	✓	✓
		2. 稽核審查	安全功能應具備以下稽核紀錄之審查： (1) 可由被授權的管理者審核稽核紀錄。 (2) 稽核紀錄應以適合管理者理解之方式呈現。	✓	✓
		3. 稽核事件儲存	安全功能應具備以下稽核事件之儲存： (1) 應防止儲存的稽核紀錄被非授權使用者刪除或竄改。 (2) 承上，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。	✓	✓
		4. 密碼操作	安全功能應具備及設定以下密碼操作： (1) 密碼運算之密碼演算法及所屬標準。 (2) 密碼運算之金鑰長度。	✓	✓
		5. 資料流控制政	安全功能應具備及設定以下資料屬性之資料流控制政策：	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		策	(1) 主體識別 (如：網路卡介面、來源端網路設備、目的端網路設備、網路位址、通訊協定等)。 (2) 資訊 (如：IP 封包、非 IP 封包等)。 (3) 管制動作(如允許、拒絕、轉送)。		
		6. 資料流控制功能	安全功能應具備及設定以下資料流控制功能： (1) 待測物應能根據安全功能政策定義以下屬性： A. 主體屬性 (如：網路卡介面、來源端網路設備、目的端網路設備、網路位址、通訊協定等)。 B. 資訊屬性 (如：來源 IP 位址、埠、協定等)。 (2) 待測物應能依據安全功能政策允許被控制網路設備及其資訊和管制動作(如：適用)。 (3) 待測物應能依據安全功能政策認證後允許被控制網路設備及其資訊和管制動作(如：適用)。 (4) 待測物應能依據安全功能政策拒絕被控制網路設備及其資訊和管制動作(如：適用)。	✓	✓
		7. 身分鑑別	安全功能應具備以下身分鑑別： (1) 可執行的特定動作之前必須進行身分鑑別。 (2) 應提供多重使用者辨別機制 (自行列舉，如：密碼、數位簽章或 RADIUS 等)。	✓	✓
		8. 使用者識別	安全功能應具備可執行的特定動作之前必須進行使用者身分識別。	✓	✓
		9. 安全屬	安全功能應具備以下安全屬性管理：	✓	✓

類別	項目	子項目	審查標準	基礎型	進階型
		性管理	(1) 應提供預設規則 (值) 。 (2) 應需允許被授權的管理者選擇不同的預設規則 (值)。		
		10.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： (1) 應限制由被授權使用者角色執行以下功能： A. 查詢/新增系統資料與稽核資料。 B. 查詢/修改其他安全屬性資料。	✓	✓
		11.管理功能規格	待測物應具備管理功能，以管理設備安全功能(如：設定設備服務、設定密碼相關功能、設定更新等)。	✓	✓
		12. 安全管理角色	安全功能應具備以下安全管理角色： (1) 應維護以下安全角色： A. 被授權管理者。 B. 被授權的系統管理者。 C. 其他 (自行列舉)。 (2) 應可定義使用者與其安全角色之關聯。	✓	✓
		13.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。	✓	✓
		14.虛擬區網(VLAN) 保護功能	安全功能應具備及設定以下虛擬區網(VLAN) 保護功能： (1) 應可設定多個 VLAN。 (2) 不同 VLAN 的埠的廣播封包應不互通。		✓

類別	項目	子項目	審查標準	基礎型	進階型
		15.組態備援管理	安全功能應具備及設定以下組態備援管理： (1) 組態設定備份及回復功能。 (2) 可回復 (Rollback) 至指定之組態。		✓

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	✓	✓

類別	項目	審查標準	基礎型	進階型
		(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： (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：	✓	✓

類別	項目	審查標準	基礎型	進階型
		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) D. 連接安全 (如待測物與其他網路伺服器之連線		

類別	項目	審查標準	基礎型	進階型
		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

類別	項目	判定標準	基礎	進階
安全功能測試	安全稽核功能	依 6.4.1.1.2. 進行測試，應提供事件的稽核紀錄且可以防止或偵測非授權使用者之竄改行為。	✓	✓
	資料流控制	依 6.4.1.2.2. 進行測試，應可針對設定的資料屬性進行控制或過濾。	✓	✓
	使用者識別與鑑別功能	依 6.4.1.3.2. 進行測試，檢測系統是否能執行列舉之多重身分識別及鑑別機制，當執行特定動作前，須先進行身份識別與鑑別。	✓	✓
	安全管理功能	依 6.4.1.4.2. 進行測試，應能定義授權管理者的安全屬性與管理規則。	✓	✓
	可靠時戳	依 6.4.1.5.2. 進行測試，應提供可靠之時戳用於記錄稽核時間資訊。	✓	✓
	虛擬區域網路(VLAN)保護功能	依 6.4.1.6.2. 進行測試，應可設定多個 VLAN，不同 VLAN 的埠的廣播封包應不互通。		✓
	組態備援管理	依 6.4.1.7.2. 進行測試，組態設定備份及回復功能，應可回復 (Rollback) 至指定之組態。		✓
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。	✓	✓
	最大虛擬區域網路(VLAN)容量	依 6.4.2.2.2. 進行測試，所負荷的 VLAN 數量達到設備規格說明之最大量時，安全功能應正常運作。		✓

類別	項目	判定標準	基礎	進階
	最大MAC容量	依 6.4.2.3.2. 進行測試，所負荷的 MAC 數量達到設備規格說明之最大量時，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 6.4.3.2.3. 進行測試，待測物遠端管理介面對服務/協定異常流量應保持正常運作。		✓
	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. 安全稽核功能

6.4.1.1.1. 測試環境

(1) 測試平台：可產生攻擊測試樣本之測試儀器或程式。
(2) 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 1。
(4) 開啟待測物之安全稽核功能及預設的安全規則。

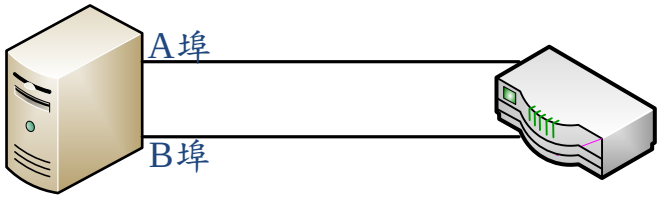

圖 1　安全稽核功能測試接續圖

6.4.1.1.2. 測試方法及標準

(1) 檢視是否依據功能定義之稽核事件產生稽核資料，並記錄於稽核資料庫。檢測設備之安全功能是否提供事件的稽核紀錄，每個稽核紀錄至少應具備下列資訊：

A. 事件日期及時間。

B. 事件型式。

C. 主體識別碼。

D. 事件內容（如：成功或失敗）。

(2) 測試待測物進行查核相關稽核紀錄之功能時，須對使用者進行識別及鑑別。設備之安全功能是否能有效防止已儲存的稽核紀錄被非授權者竄改、刪除或儲存，當稽核資料被非授權使用者竄改時能予以偵測。

6.4.1.2. 資料流控制

6.4.1.2.1. 測試環境

(1) 開啟待測物及設定管理規則。

(2) 連接測試平台及待測物如圖 1。

6.4.1.2.2. 測試方法及標準

(1) 檢測系統能根據以下資料屬性，對可管理的每項資料流進行控制、過濾等制定政策管理。

A. 主體識別 (網路卡介面、來源端網路設備、目的端網路設備、網路位址或通訊協定等)。

B. 資訊 (IP 封包或非 IP 封包等)。

C. 主體識別碼。

D. 管制動作 (允許、拒絕或轉送等)。

(2) 檢測系統是否能根據安全功能政策定義以下屬性

A. 主體屬性 (網路卡介面、來源端網路設備、目的端網路設備、網路位址或通訊協定等)。

B. 資訊屬性 (來源 IP 位址、埠或通訊協定等)。

(3) 檢測系統是否能依據安全功能政策允許被控制網路設備及其資訊。

(4) 檢測系統是否能依據安全功能政策認證後，允許被控制網路設備及其資訊。

(5) 檢測系統是否能依據安全功能政策拒絕被控制網路設備及其資訊。

6.4.1.3. 使用者識別與鑑別功能

6.4.1.3.1. 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) 連接測試平台、待測物及網際網路如圖 2。

(4) 開啟待測物之安全稽核功能及預設安全規則。

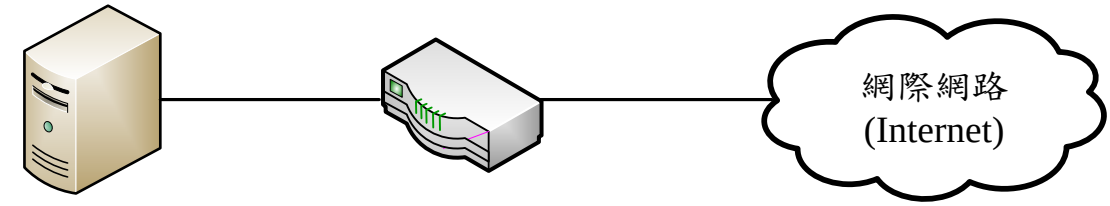

圖 2　安全管理功能測試接續圖

6.4.1.3.2. 測試方法及標準

(1) 檢測系統是否能在執行的特定動作之前，先執行身分識別機制。

(2) 檢測系統是否能執行其自行列舉之多重使用者辨別機制 (自行列舉之身分辨別機制，如：密碼、數位簽章或 RADIUS 等) 。

6.4.1.4. 安全管理功能

6.4.1.4.1. 測試環境

連接測試平台、待測物及網際網路如圖 2。

6.4.1.4.2. 測試方法及標準

(1) 檢測待測物是否能提供預設規則 (值)，且允許被授權的管理者，選擇不同的預設規則 (值)。

(2) 檢測系統安全功能 (TSF) 是否能限制由被授權使用者角色來執行以下功能：

A. 查詢/新增系統與稽核資料。

B. 查詢/修改其他安全屬性資料。

(3) 檢測待測物列舉之系統安全管理功能是否能正常運作 (如：設

定設備服務、設定密碼相關功能及設定更新等)。

(4) 檢測系統安全功是否能維護以下安全角色：

A. 被授權管理者。

B. 被授權的系統管理者。

C. 其他自行列舉之安全角色。

(5) 檢測系統安全功是否能定義使用者與其安全角色之關聯。

6.4.1.5. 安全功能防護功能

6.4.1.5.1. 測試環境

連接測試平台、待測物及網際網路如圖 2。

6.4.1.5.2. 測試方法及標準

(1) 檢測待測物提供可靠之時戳功能。

(2) 檢測待測物將可靠的時戳用於記錄稽核時間資訊。

6.4.1.6. 虛擬區域網路 (VLAN) 保護功能 (適用進階型)

6.4.1.6.1. 測試環境

(1) 連接測試平台及待測物如圖 1。

(2) 開啟待測物之預設安全規則。

6.4.1.6.2. 測試方法及標準

(1) 待測物可設定多個 VLAN。

(2) 由測試平台針對不同 VLAN 產生流量，並偵測不同 VLAN 的埠的廣播封包是否互通。

6.4.1.7. 組態備援功能 (適用進階型)

6.4.1.7.1. 測試環境

(1) 連接測試平台、待測物及網際網路如圖 2。

(2) 開啟待測物並設定不同安全規則。

6.4.1.7.2. 測試方法及標準

(1) 啟用待測物並設定組態備份功能，備份數組安全規則。

(2) 啟用待測物回復功能，用以測試待測物可組態設定及回復至指定之組態。

6.4.2. 壓力測試

6.4.2.1. 吞吐量測試

6.4.2.1.1. 測試環境

(1) 測試平台：可產生網路封包之測試儀器或程式。

(2) 測試平台 A 埠：模擬用戶端送收網路封包。

(3) 測試平台 B 埠：模擬伺服器端送收網路封包。

(4) 網路連接線：乙太網路線或光纖纜線。

(5) 連接測試平台及待測物如圖 3，其中乙太網路線或光纖線路連接數量依待測物運作模式 (如 Proxy 或 Transparent Mode) 決定。

(6) 代理模式 (Proxy Mode)：乙太網路線或光纖線路連接數量為一條，測試平台 A 埠及 B 埠為同一連接埠。

(7) 通透模式 (Transparent Mode)：乙太網路線或光纖線路連接數量為兩條，測試平台 A 埠及 B 埠為獨立的兩個連接埠。

(8) 開啟待測物之安全功能。

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

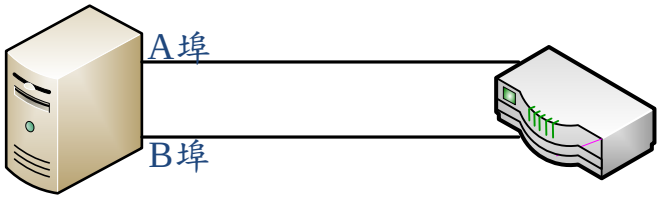

圖 3　吞吐量測試接續圖

6.4.2.1.2. 測試方法及標準

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

6.4.2.2. 最大虛擬區域網路 (VLAN) 容量

6.4.2.2.1. 測試環境

(1) 連接測試平台及待測物如圖 3。

(2) 開啟待測物之安全功能。

6.4.2.2.2. 測試方法及標準

當待測物所負荷的 VLAN 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 MAC 容量

6.4.2.3.1. 測試環境

(1) 連接測試平台及待測物如圖 3。

(2) 開啟待測物之安全功能。

6.4.2.3.2. 測試方法及標準

測試程式執行平台自 A 埠建立 MAC 數達到其規格說明之最大值時，其安全功能應保持正常運作。

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

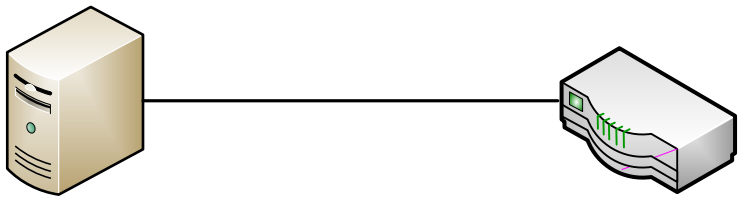

圖 4　阻斷式攻擊測試接續圖

(1) 測試平台：可產生大量網路流量之測試儀器或程式。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接測試平台及待測物如圖 4。

(4) 開啟待測物之安全功能。

(5) 測試平台針對待測物的服務連接埠，發動阻斷式攻擊。

6.4.3.1.2. 測試方法及標準

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

6.4.3.2. 遠端管理異常流量

6.4.3.2.1. 測試環境

(1) 測試平台：可產生大量網路流量之測試儀器或程式。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接測試平台及待測物如圖 4。

(4) 開啟待測物之安全功能。

(5) 透過待測物提供的終端管理介面進入待測物進行設定，開啟待測

物之遠端管理功能。

6.4.3.2.2. 測試樣本

以測試平台產生之服務或協定異常流量至少 10 種作為測試樣本。

6.4.3.2.3. 測試方法及標準

測試平台送出測試樣本至待測物，待測物之遠端管理功能應正常運作。

6.4.3.3. 非正常關機恢復

6.4.3.3.1. 測試方法及標準

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

6.4.4. 穩定測試

6.4.4.1. 真實流量

6.4.4.1.1. 測試環境

(1) 流量錄製平台：錄製網路封包。

(2) 網路連接線：乙太網路線或光纖纜線。

(3) 連接流量錄製平台、路由器、內部網路及網際網路如圖 5。

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

(5) 流量重播平台：將預先錄製之真實流量檔案還原成網路封包送至待測物。

(6) 連接流量重播平台與待測物如圖 6。

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

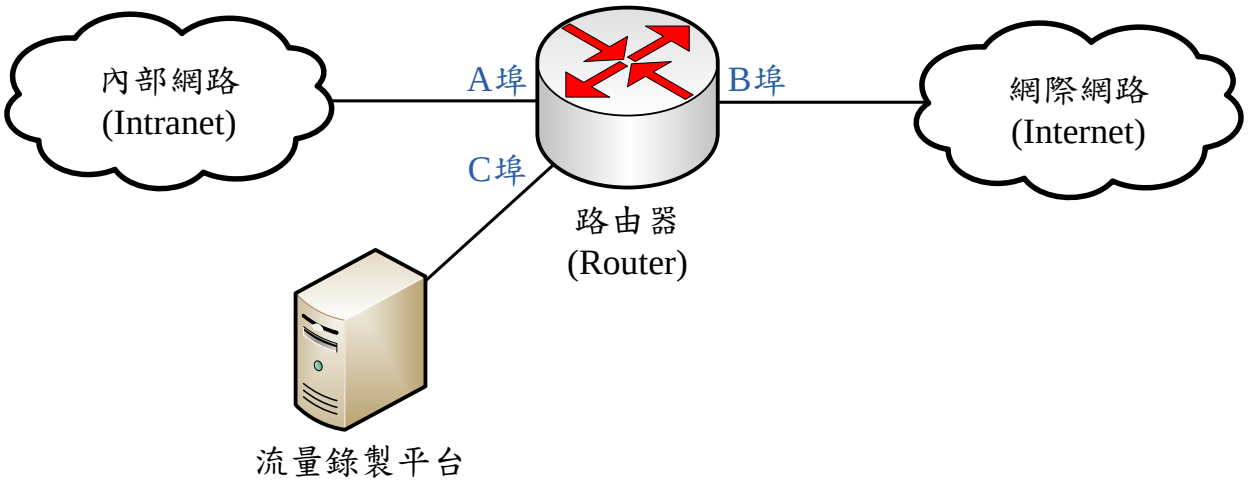

圖 5　流量錄製接續圖

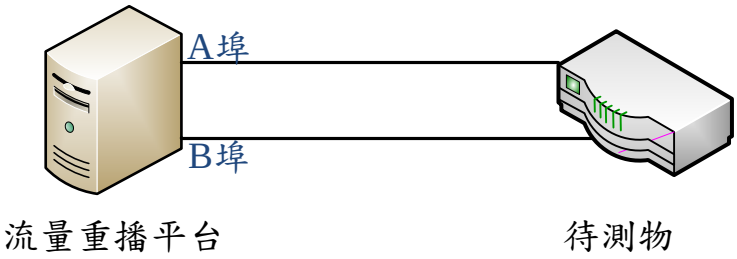

圖 6　流量重播接續圖

6.4.4.1.2. 測試樣本

測試樣本必須滿足以下要求：

(1) 應從真實網路環境錄製。

(2) 具備至少 100 位使用者同時上線之網路流量。

(3) 應為該待測物送測前 2 周內所錄製之網路流量。

(4) 須達該待測物規格說明之最大連線數 50% 以上。

(5) 須達該待測物規格說明之吞吐量最大值 50% 以上。

(6) 包含至少 10 種應用類型，每一種應用類型至少包括一個應用項

目，全部之應用項目須達 50 個以上。舉例如下：

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

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

C. File Transfer：ftp、flashget 及 smb。

D. Game：garena、facebook app 及 steam。

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

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

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

H. VoIP：skype 及 sip。

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

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

6.4.4.1.3. 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。*